CAHIERS DU SÉMINAIRE D'HISTOIRE DES MATHÉMATIQUES

EBERHARD BECKER

Sums of squares and quadratric forms in real algebraic geometry

Cahiers du séminaire d'histoire des mathématiques 2^e série, tome 1 (1991), p. 41-57

<http://www.numdam.org/item?id=CSHM_1991_2_1__41_0>

SUMS OF SQUARES AND QUADRATRIC FORMS IN REAL ALGEBRAIC GEOMETRY

Eberhard Becker
Univeristé de Dortmund

Introduction

This note wants to contribute to a description of the role of quadratic forms in real algebraic geometry. This latter theory is concerned, at least as a starting point, with the set of real solutions, i.e. $x \in \mathbb{R}^n$, of a system of polynomial equations

$$F_1(X) = 0, ..., F_r(X) = 0$$

where $F_1(X), ..., F_r(X) \in \mathbb{R}[X_1, ..., X_n]$. At a first glance, there seems to be no relation between algebraic geometry and quadratic form theory. However, that quadratic forms in fact play an important role in the study of systems of equations dates back at least to the days of Jacobi, Hermite and Sylvester. These great researchers discovered, by reflecting on Sturm's theorem, that in many cases the number of the real solutions of the above system can be counted by the signatures of associated quadratic forms.

These discoveries in the middle of the last century provide the starting point for this note. At the end we want to arrive at the modern results about the mapping $W(A) \longrightarrow C(\text{Sper } A, \mathbb{Z})$ where $W(A)$ denotes the Witt ring of the commutative ring A and the mapping goes into the ring of integer-valued continuous functions on the real spectrum of A. As to basic questions and concepts and seen from a today's point of view, there seems to be a natural road from Syvester's and Hermite's investigations to what is being studied at present. However, progress along this road went slow, ant it was only the development of the algebraic theory of quadratic forms and, slightly later, the foundation of a general real algebraic geometry that provided the necessary basis for a general understanding of what has been done more than hundred years ago. In this respect, the story of quadratic forms in real algebraic geometry represents one further example of the highly interesting and sometimes curious way mathematics actually evolves.

This note is not meant as a detailed report, it should rather display the general flavor. To see more about notions and results involved one should turn to the cited literature.

List of contents

1. The trace formula

In algebraic geometry one is concerned with sets defined by finitely many polynomial equations. Given polynomials $F_1(X), ..., F_r(X) \in \mathbb{R}[X, ..., X_n]$ where $X = (X_1, ..., X_n)$, one defines an affine algebraic variety by setting

$$V : F_1(X) = 0, ..., F_r(X) = 0 .$$

If K is any extension field of $\mathbb{R}$ we set

$$V(K) = \{x \in K^n \mid F_1(x) = F_2(x) = ... = F_r(x) = 0\} .$$

Real algebraic geometry deals primarily with $V(\mathbb{R})$. However, the "full" set of complex point $V(\mathbb{C})$ plays an important role even in the study of $V(\mathbb{R})$. In our situation we assume that

$$V(\mathbb{C}) \text{ is finite}$$

and ask for the

$$\text{cardinality of } V(\mathbb{R}) .$$

This number $\#V(\mathbb{R})$ can be obtained *via* quadratic forms, a method often referred to as the Hermite-Sylvester method. But also Borchardt and Jacobi should be mentioned in this context. The question of priority is a delicate one and will not be discussed here. But it seems that it was Hermite who was in the possesion of the most general and powerful method.

The original work of Borchardt, Jacobi, Hermite and Syvester can be found in [B1], [B2], [H1], [H2], [H3] and [S]. A very comprehensive account of the Hermite-Sylvester method, understood in a broad sense, gives the highly recommended paper of Krein-Naimark [Kr-N]. But one may also consult [G], [I] and [Ob]. Quite recently, our subject found a modern presentation in the book of Knebusch-Scheiderer [Kn-S], and it is also mentioned in the book of Benedetti-Risler [B-R, p. 17 ff].

We have to deal with quadratic forms over commutative ring A with 1 where 2 is invertible. For more general definitions than given here see [M-H],

[Ba] or [B-C-R, Ch. 15]. Quite basically, a quadratic form over a ring is nothing but a homogeneous polynomial of degree 2. For technical purposes we have to pass to a module theoretic approach. Let M be a free A-module of finite rank. A quadratic form φ on M is a map $\varphi : M \longrightarrow A$ subject to

(1) $\varphi(\alpha m) = \alpha^2 \varphi(m)$ for all $\alpha \in A$, $m \in M$,
(2) the mapping $\alpha(\ ,\ ) : M \times M \longrightarrow A$,
$$\varphi(x,y) = \frac{1}{2}(\varphi(x+y) - \varphi(x) - \varphi(y)), \text{ is } A\text{-bilinear.}$$

If φ admits an orthogonal basis $v_1, \ldots, v_n$, i.e. an A-basis of M with $\varphi(v_i, v_j) = 0$ whenever $i \neq j$, we set $\varphi = <\alpha_1, \ldots, \alpha_n>$ where $\alpha_i = \varphi(v_i, v_i) = \varphi(v_i)$.

In the case of $A = \mathbb{R}$, any quadratic form φ has an orthogonal basis : $\varphi = <\alpha_1, \ldots, \alpha_n>$. This allows to definie the signature

$$\operatorname{sgn}(\varphi) = \sum_1^n \operatorname{sgn}(\alpha_i) \in \mathbb{Z}$$

where $\operatorname{sgn}(\varphi) = 1, -1$ or 0 according to whether $\alpha > 0$, $\alpha < 0$ or $\alpha = 0$. That $\operatorname{sgn}(\varphi)$ is independant of the chosen orthogonal basis is exactly the content of Sylvester's law of inertia of 1853 [S].

Following the principle of the ideas of Hermite and Sylvester we will now attach a quadratic form ρ over $\mathbb{R}$ to the above system of equations resulting in the desired equality

$$\#V(\mathbb{R}) = \operatorname{sgn} \rho \ .$$

To this end, certain algebraic tools for treating general affine varieties - not assuming the above hypothesis on $V(\mathbb{C})$ - have to be introduced. Let $a = (F_1, \ldots, F_r)$ be the ideal of $\mathbb{R}[X_1, \ldots, X_n]$ generated by the given polynomials. Then form the ring $\mathbb{R}[V] = \mathbb{R}[X_1, \ldots, X_n] \,/\, a$, the coordinate ring of V. The elements of $\mathbb{R}[V]$ have a natural representation as functions on $V(\mathbb{R})$: an element $f+a$ gives rise to the function

$$\bar{f} = V(\mathbb{R}) \longrightarrow \mathbb{R}, \ x \longmapsto f(x) \ .$$

In the sequel, we will write f instead of $f+a$ and $f(x)$ instead of $\bar{f}(x)$.

Let $\varphi = <f_1, \ldots, f_n>$ be a quadratic form (with orthogonal basis) over $A = \mathbb{R}[V]$. For each $x \in V(\mathbb{R})$ we get the quadratic form

$$\varphi_x = <f_1(x), \ldots, f_n(x)> \text{ over } \mathbb{R} \ .$$

Each of these forms has a signature $\operatorname{sgn} \varphi_x \in \mathbb{Z}$. Putting all these signatures together we have constructed the total signature map

$$\operatorname{sign} : \begin{cases} QF(\mathbb{R}[V]) \longrightarrow \operatorname{Map}(V(\mathbb{R}),\mathbb{Z}) \\ \varphi \longmapsto (x \longmapsto \operatorname{sgn}(\varphi_x)) \end{cases}$$

where $QF(A)$ denotes the collection of all diagonalized quadratic forms over A, for any ring A.

We next turn to our special situation where $V(\mathbb{C})$ is finite, a fortiori : $V(\mathbb{R})$ finite. In this situation we have a further map

$\Sigma : \operatorname{Map}(V(\mathbb{R}),\mathbb{Z}) \longrightarrow \mathbb{Z}, g \longmapsto \sum_{x \in V(\mathbb{R})} g(x)$ which yields an incomplete diagram

$$\begin{array}{ccc} QF(\mathbb{R}[V]) & \xrightarrow{\operatorname{sgn}} & \operatorname{Map}(V(\mathbb{R}),\mathbb{Z}) \\ \vdots ? & & \downarrow \Sigma \\ QF(\mathbb{R}) & \xrightarrow{\operatorname{sgn}} & \mathbb{Z} \end{array}$$

It has really started with the investigation of Hermite and Sylvester that one knows how to remove the question mark and define a map $\operatorname{tr}^* : QF(\mathbb{R}[V]) \longrightarrow QF(\mathbb{R})$, the transfer or trace map, that renders the above diagram commutative. We record this as the main result in this section :

Theorem *(trace formula). There exists a transfer, $\varphi \longmapsto \operatorname{tr}^*\varphi$, of quadratic forms over $\mathbb{R}[V]$ to forms over $\mathbb{R}$ such the following formula holds :*

$$\operatorname{sgn}(\operatorname{tr}^*\varphi) = \sum_{x \in V(\mathbb{R})} \operatorname{sgn}(\varphi_x) .$$

Before entering the construction of the transfer and the sketch of the proof of the above result we want to list up some applications.

I) $\operatorname{sgn}(\operatorname{tr}^*\langle 1\rangle) = \#V(\mathbb{R})$.

This is obvious as $\langle 1\rangle_x = \langle 1\rangle$ for each $x \in V(\mathbb{R})$.

II) $\operatorname{sgn} \operatorname{tr}^*\langle f\rangle = \#\{x \in V(\mathbb{R}) \mid f(x) > 0\} - \#\{x \in V(\mathbb{R}) \mid f(x) < 0\}$.

To see this note $\langle f\rangle_x = \langle f(x)\rangle$.

III) For $g_1, \ldots, g_n \in \mathbb{R}[V]$ set $\varphi = \langle\langle g_1, \ldots, g_n\rangle\rangle = \langle \ldots, \prod_{i=1}^{n} g_i^{\varepsilon_i}, \ldots \rangle_{\varepsilon_1,\ldots,\varepsilon_n=0,1}$.

This form is usually referred to as the n-fold Pfister form of dimension 2^n. If $x \in V(\mathbb{R})$ then $\operatorname{sgn} \varphi_x = \prod_{i=1}^{n} (1 + \operatorname{sgn} g_i(x))$ whence

$$\operatorname{sgn} \operatorname{tr}^*\langle\langle g_1, \ldots, g_n \rangle\rangle = 2^n \cdot \#\{x \in V(\mathbb{R}) \mid g_1(x) > 0, \ldots, g_n(x) > 0\}$$

provided $g_i(x) \neq 0$ for all $i = 1, \ldots n$, $x \in V(\mathbb{R})$.
We will improve on this in the next section.
To define the transfer we first note that, on the hypothesis of "$V(\mathbb{C})$ finite", $\mathbb{R}[V]$ turns out to be a finite dimensional $\mathbb{R}$-algebra. We therefore have the $\mathbb{R}$-linear trace map

$$\operatorname{tr} : \mathbb{R}[V] \longrightarrow \mathbb{R}, \quad a \longmapsto \text{trace of } L(a)$$

where $L(a)$ is the left multiplication in $\mathbb{R}[V]$: $L(a)(b) = ab$. Now, given any quadratic form φ on a free $\mathbb{R}[V]$-module M of finite rank we first consider M as a $\mathbb{R}$-vectorspace $M_{\mathbb{R}}$, in fact of finite dimension, and then define $\operatorname{tr}^*(\varphi)$ $tr \circ \varphi : M_{\mathbb{R}} \longrightarrow \mathbb{R}$ as the transfer of φ. It is readily verified that $\operatorname{tr}^*(\varphi)$ is a quadratic form over $\mathbb{R}$.

The proof of the trace formula can be sketched as follows. We first pass to the reduced algebra $\mathbb{R}[V]_{\text{red}} := \mathbb{R}[V]/\text{Nilradical}$. As the trace vanishes on the Nilradical the left hand side of the trace formula does not change if one passe to $\mathbb{R}[V]_{\text{red}}$. In the next step one observes

$$\mathbb{R}[V]_{\text{red}} \simeq \Big(\prod_{x \in V(\mathbb{R})} \mathbb{R}\Big) \times \mathbb{C}^s$$

which essentially yields the proof, cf. also [Kn-S].

2. Remarks on computations

It is the purpose of this section to show that the trace formula can be in fact used for computations. For each of the following computational tasks there exist implemented algorithms so that calculations can be carried out in practice, of course limited by the capacity of the computers used. We will refrain from discussing the efficiency of the methods ; those readers who are interested in complexity issues may consult the cited references.

Given the system of polynomial equations

$$V : F_1 = 0, \ldots, F_r = 0$$

with $F_i \in \mathbb{R}[X_1, \ldots, X_n]$ and $V(\mathbb{C})$ finite we passed in the last section to the $\mathbb{R}$-algebra $\mathbb{R}[V] = \mathbb{R}[X_1, \ldots, X_n] / a$. The signature of any form $\operatorname{tr}^*(\varphi)$ only

depends on $\mathrm{tr}^*(\bar{\varphi})$ where $\bar{\varphi}$ denotes the induced form over $\mathbb{R}[V]_{\mathrm{red}} = \mathbb{R}[X_1, ..., X_n] / \sqrt{a}$, $\sqrt{a}$ = the radical of a, and the transfer is defined by the trace map $\mathbb{R}[V]_{\mathrm{red}} \longrightarrow \mathbb{R}$. The first task is therefore to perform the calculation of the radical $\sqrt{a}$.

There exists an implementation of an algorithm based on Gröbner bases-techniques and using ideas of [GitrZ]. It works for arbitrary ideals in $\mathbb{R}[X_1, ..., X_n]$. Basic informations about Gröbner bases can be obtained e.g. from [Bu].

The assumption "$V(\mathbb{C})$ finite" is equivalent to the fact that $a \cap \mathbb{R}[X_i] = (\tilde{f}_i(X_i)) \neq 0$ for every $i = 1, ..., n$.
Set $f_i(X_i) = \tilde{f}_i / \gcd(\tilde{f}_i, \tilde{f}_i')$. According to Seidenberg [Se] one has

$$\sqrt{a} = (a, f_1, ..., f_n) .$$

The polynomial $\tilde{f}_i$ can be derived either by Gröbner base techniques or by Linera Algebra using bounds from an effective Nullstellensatz [CaGaHe].

Now, having the radical presented by some set of generators, one next proceeds to a distinguished one. This is the subject of the following lemma often referred to as the Shape Lemma, cf. [GiTrZ] :
The radical $\sqrt{a}$ can be generated by polynomial of the type

$$X_1 - g_1(X_n),\ X_2 - g_2(X_n), ..., X_{n-1} - g_{n-1}(X_n),\ f(X_n)$$

(possibly, only after a linear change of coordinates).

This set of generators is a Gröbner basis relative to a certain term ordering [GiTrZ].
Using the Shape Lemma we arrive at the following description of $\mathbb{R}[V]_{\mathrm{red}}$:

$$\mathbb{R}[V]_{\mathrm{red}} \simeq \mathbb{R}[T] / (f(T)) .$$

It is now much easier to compute the transfer from $\mathrm{tr}^*(\varphi) = \perp_{i=1}^{r} \mathrm{tr}^*\langle g_i \rangle$ if $\varphi = \langle g_1, ..., g_r \rangle$. Given $g \in \mathbb{R}[V]_{\mathrm{red}}$, $\mathrm{tr}^*\langle g \rangle$ is a deg f-dimensional form over $\mathbb{R}$. Relative to the basis $1, T, ..., T^{n-1}$, where $n = \deg f$, $\mathrm{tr}^*\langle g \rangle$ is described by the following symmetric matrix :

$$\mathrm{tr}^*\langle g \rangle \leftrightarrow (\alpha_{i+j-2})_{i,j=1,...,n} .$$

As one of various possibilities, the entries α_k can be obtained from the formal power series expansion

$$T\frac{g(T)f'(T)}{f(T)} = \sum_{k=0}^{\infty} \alpha_k T^{-k} .$$

To determine sgn tr*<g> one may use the above symmetric matrix, a socalled Hankel matrix [G], [I], [Kn-S]. Symmetric matrices of this type allow a more efficient way of calculating their signatures, e.g. by means of the theorem of Frobenius [l. cit.].

So far, it has been described how to calculate

$$\mathrm{tr}^*\langle g\rangle = \#\{x \in V(\mathbb{R}) \mid g(x) > 0\} - \#\{x \in V(\mathbb{R}) \mid g(x) < 0\}$$

by an efficient algorithm. However, if one turns to the third computational problem of § 1, i.e. the determination of

$$\#\{x \in V(\mathbb{R}) \mid g_1(x) > 0, \ldots, g_n(x) > 0\} = c(V, g_1, \ldots, g_n) ,$$

the above procedure would force us to deal with a symmetrix matrix with at least $2^n.\#V(\mathbb{R})$ rows. Even for n not too large, matrices of this size can hardly be handled. However, starting with the system (*), defining V, and the given $g_1, \ldots, g_n$ one can algorithmically produce a polynomial $h \in \mathbb{R}[X_1, \ldots, X_n]$ such that

$$c(V, g_1, \ldots, g_n) = c(V,h) .$$

Hence, one has to deal only with the transfer of the 2-dimensional form $\langle 1,h\rangle$ instead of $\langle\langle g_1, \ldots, g_n\rangle\rangle$ which has dimension 2^n .

In concluding this section, one has to mention that there are other methods to determine the value of $c(V, g_1, \ldots, g_n)$, a number very important for many algorithms in real algebraic geometry. The paper [GLRR], especially section 4, contains o lot of informations.

3. Higher dimensional varieties

In this section we drop the hypothesis that $V(\mathbb{C})$ is finite but still want to study the total signature map sgn : $QF(\mathbb{R}[V]) \longrightarrow \mathrm{Map}(V(\mathbb{R}),\mathbb{Z})$. Recall that $(\mathrm{sgn}\,\varphi)(x) = \sum \mathrm{sgn}\, g_i(x)$ if $\varphi = \langle g_1, \ldots, g_n\rangle$. In the sequel we will assume that the coefficient functions g_i have no zeros on $V(\mathbb{C})$. Two forms $\varphi = \langle g_1, \ldots, g_n\rangle$ and $\psi = \langle h_1, \ldots, h_n\rangle$ are said to be isometric, written $\varphi \simeq \psi$, if there is an invertible matrix $A \in \mathrm{GL}(n,\mathbb{R}[V])$ such that

$$A \begin{pmatrix} g_1 & & 0 \\ & \ddots & \\ 0 & & g_n \end{pmatrix} A^t = \begin{pmatrix} h_1 & & 0 \\ & \ddots & \\ 0 & & h_n \end{pmatrix}$$

holds. Hyperbolic forms are forms of the type
$\varphi \simeq r \times \langle 1,-1\rangle = \langle 1,-1,1,-1,\ldots,1,-1\rangle$. The following properties are readily checked :

1) $\varphi \simeq \psi \longrightarrow \operatorname{sgn}(\varphi) = \operatorname{sgn}(\psi)$
2) $\operatorname{sgn}(\varphi^{\perp}$ hyperbolic form$) = \operatorname{sgn}(\varphi)$,
3) $\operatorname{sgn}(\varphi)$ is locally constant, continuous on $V(\mathbb{R}) \subset \mathbb{R}^r$.

These properties allow tow define the total signature on the level of the Witt ring $\omega(\mathbb{R}[V])$ of $\mathbb{R}[V]$. To do it properly one should consult the cited literature, e.g. [B-C-R, Chap. 15] is a good reference for this and the subsequent section. However, basically one proceeds as folloxs. Two forms φ and ψ, not necessarily of the same dimension, are called equivalent if there are hyperlolic τ, σ such that $\varphi^{\perp}\tau \simeq \psi^{\perp}\sigma$. The equivalence classe $[\varphi]$ form a ring, theWitt ring, with compositions induced by the formation of the orthogonal sum and the tensor product. (This is okay for fields of characteristic not 2, for general rings this gives only the idea). From the above we therefore get an induced ring homomorphism

$$\operatorname{sgn} : W(\mathbb{R}[V]) \longrightarrow C(V(\mathbb{R}),\mathbb{Z}) .$$

Clearly, $\operatorname{sgn}([\varphi])$ is also a locally constant continuous function and therefore constant on each of the connected components of $V(\mathbb{R})$. It is a general result of Withney, cf. [B-C-R, Ch. 2], that $V(\mathbb{R})$ decomposes in only finitely many connected components of $V(\mathbb{R})$. Denoting by $\pi_0(V(\mathbb{R}))$ the set of the connected components of $V(\mathbb{R})$, we find that in fact $\operatorname{sgn}(\varphi) \in C(\pi_0(V(\mathbb{R})),\mathbb{Z}) \subset C(V(\mathbb{R}),\mathbb{Z})$. Note that we have $C(\pi_0(V(\mathbb{R})),\mathbb{Z}) = \operatorname{Map}(\pi_0(V(\mathbb{R})),\mathbb{Z})$. It was Mahé who proved in 1982, cf. [Ma1], the following important theorem.

Theorem. *The map* $W(\mathbb{R}[V]) \xrightarrow{\operatorname{sgn}} C(\pi_0(V(\mathbb{R})),\mathbb{Z})$ *has a 2-torsion cokernel.*

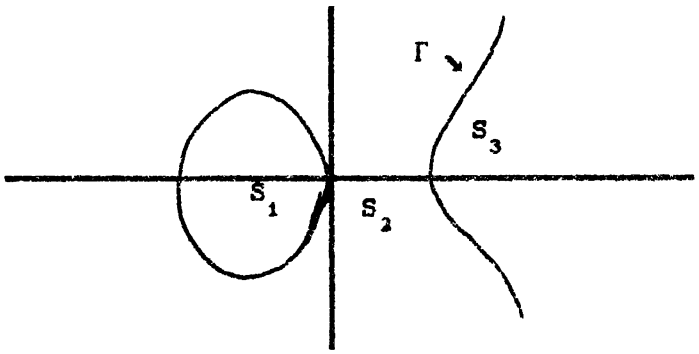
This result tell that the connected components of $V(\mathbb{R})$ can be separated by the signatures of quadratic forms. Namely, if C is one component we consider the characteristic function χ_C, i.e. $\chi_C(x) = 1$ or 0 according to whether $x \in C$ or not. By Mahé's theorem there is some power 2^k such that $2^k\chi_C = \operatorname{sgn}(\varphi)$. Obviously, $\operatorname{sgn}(\varphi_x) = 2^k$ if $x \in C$ and $\operatorname{sgn}(\varphi_x) = 0$ otherwise.

This theorem and its companion [H-M] for projective varieties set the endpoint to a series of attempts to show that components can be separated by

the signature of quadratic forms ; it is very instructive to turn to the "note bibliographique" in [B-C-R, p. 347] for further informations. Also, a further paper of Mahé [Ma2] is recommended for a closer study of the above torsion exponents 2^k . For further study see [Schw].

The question may arise why, instead of using functions, one passes to quadratic forms to separate components. The answer is as easy as possible : in general, components cannot be separated by functions (which is however true for curves). The following example is taken from [B-C-R, p. 335 ff].

Let V be the complement in $\mathbb{R}^2$ of the elliptic curve $\Gamma : y^2 = x^3 - x$. It is an irreducible affine variety of dimension 2.



V consists of three components and setting $g = y^2 - x^3 + x$ we get $\mathbb{R}[V] = \{f.g^{-k} \mid f \in \mathbb{R}[X,Y],\ k \in \mathbb{N}\}$. If $fg^{-k} < 0$ on S_1 but > 0 on $S_2 \cup S_3$ one shows that $f = 0$ on Γ whence $g \mid f$ which finally yields the statement that in this case the components cannot be separated by a function.

The above separation of components by quadratic forms is based on the distinction of the three cases "$f(x) > 0$", "$f(x) < 0$" or "$f(x) = 0$" if $f \in \mathbb{R}[V]$, $x \in V(\mathbb{R})$ are given. Functions, everywhere non-negative on $V(\mathbb{R})$, can not be used for separation purposes. One is therefore led to study the following problem :

Characterize the function $f \in \mathbb{R}[V]$ *satisfying*
$f(x) > 0$ *for all* $x \in V(\mathbb{R})$.

This is the well known 17^{th} problem of Hilbert (at least a variant of it) posed in 1899, cf. e.g. [Be1]. It was Artin who provided in 1927 the solution ([A], [P]) :

if V is a irreducible affine variety of $\mathbb{R}$ and $f \in \mathbb{R}[V]$ then :
$f(x) \geq 0$ for all regular points $x \in V(\mathbb{R})$ iff f a sum of squares of rational functions.

The above applies to $\mathbb{R}^n$ and yields for any polynomial $f \in \mathbb{R}[X_1, ..., X_n]$:

$$f(x_1, ..., x_n) \geq 0 \text{ for all } (x_1, ..., x_n) \in \mathbb{R}^n \Leftrightarrow f = \sum_{i=1}^{N} \left(\frac{h_i}{g_i}\right)^2$$

where $h_i, g_i \in \mathbb{R}[X_1, ..., X_n]$, $g_i \neq 0$.

The chapter 6 of [B-C-R] contains a proof as well as many informations concerning generalizations to other rings of functions and also Pfister's result about the boun $N \leq 2^n$, valid for all $f \in \mathbb{R}[X_1, ..., X_n]$.

Artin's result can be read in two directions : it either presents a presentation of nowhere negative functions or it can be understood as a geometric characterization of sums of squares of rational functions. It is this second interpretation that motivated a corresponding study of sums of powers of rational functions with arbitrary even exponent, cf. the forthcoming paper [B-B-D-G]. Additionally, Pfister's bound has been extended to sums of $2n$-th powers [Be2].

4. The role of the real spectrum

The notion of the real spectrum of a ring is fundamental to real algebraic geometry. Clearly, the book [B-C-R] is the main reference. However other introductory papers on this subjects, providing special points of view, are also recommended, cf. e.g. [Kn], [L], [Be3].

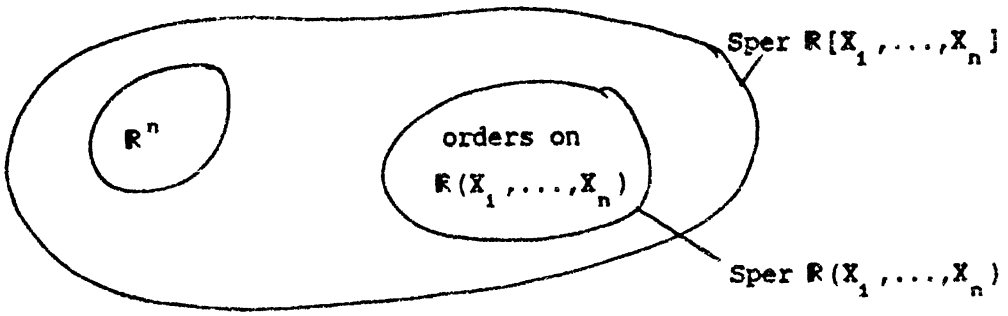
Interpreting Artin's proof in the light of the real spectrum may help to find a conceptual understanding. In the case of a positive function f on $\mathbb{R}^n$ one has to show that f is contained in every order P of the rational function field $\mathbb{R}(X_1, ..., X_n)$ since, by Artin, the intersection of all orders of a field is just the set of all sums of squares in this field. Thus we have to link points $x \in \mathbb{R}^n$ to orders P in $\mathbb{R}(X_1, ..., X_n)$. It is exactly the real spectrum of $\mathbb{R}[X_1, ..., X_n]$ which provides a compact topological space comprising points as well as orders.

Quite generally, if A is any commutative ring we set

$$\text{Sper } A = \{(\rho,P) \mid \rho \text{ a prime ideal, } P \text{ an order of quot}(A/\rho)\}.$$

On Sper A we impose a topology by taking the sets
$D(a) = \{(\rho,P) \in \text{Sper } A \mid a+\rho >_p 0\}$, $a \in A\tau$, as a subbasis. Sper A, endowed with this topology, is called the real spectrum of A. Note, there are other notations used : $\text{Spec}_r A$, $\mathcal{R}$-Spec A,... .

Our case of Sper $\mathbb{R}[X_1,...,X_n]$ may be visualized as follows :



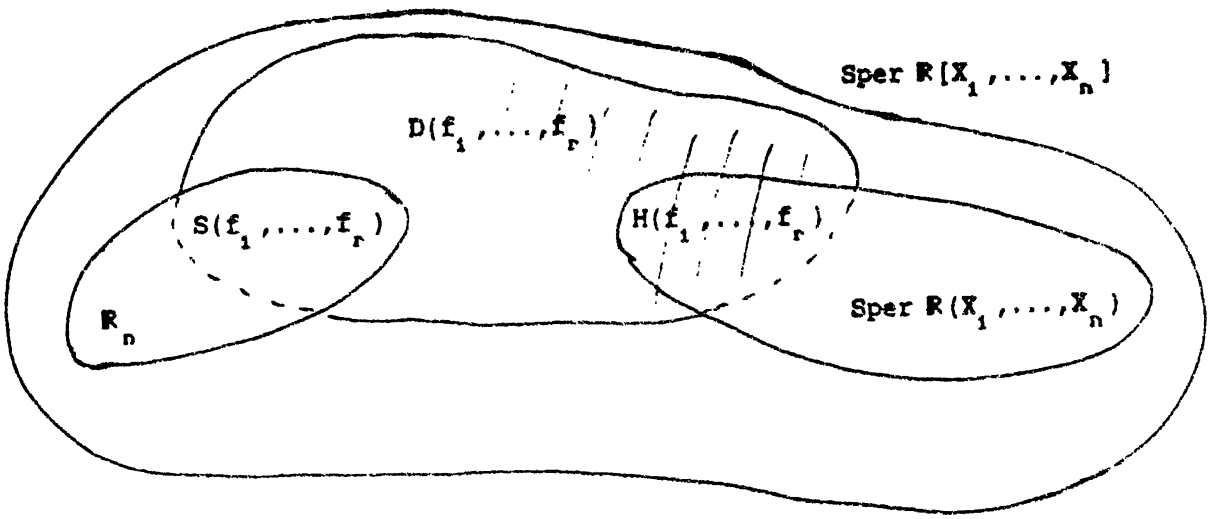
Here, $\mathbb{R}^n$ is identified with the set $\{(m_x, \mathbb{R}_+) \mid x \in \mathbb{R}^n\}$,
$m_x = \{f \in \mathbb{R}[X_1,...,X_n] \mid f(x) = 0\}$ and Sper $\mathbb{R}(X_1,...,X_n)$ = set of all orders on $\mathbb{R}(X_1,...,X_n)$ with $\{(0,P) \mid P \text{ order on } \mathbb{R}(X_1,...,X_n)\}$.

In contrast to the above graphical presentation, the sets $\mathbb{R}^n$ and Sper $\mathbb{R}(X_1,...,X_n)$ are dense subspaces of the topological space Sper $\mathbb{R}[X_1,...,X_n]$. More precisely, given $f_1,...,f_n \in \mathbb{R}[X_1,...,X_n] \setminus \{0\}$ we form the set $D(f_1,...,f_r) := \bigcap_i$ Sper $\mathbb{R}[X_1,...,X_n]$ and consider the intersections

$$S(f_1,...,f_r) := D(f_1,...,f_r) := \cap\, \mathbb{R}^n = \{x \in \mathbb{R}^n \mid f_1(x) > 0,...,f_r(x) > 0\}$$

and

$$H(f_1,...,f_r) := D(f_1,...,f_r) \cap \text{ Sper } \mathbb{R}(X_1,...,X_n) = \{P \mid f_1,...,f_r \in P\} .$$



It is the fundamental Artin-Lang theorem that states that

$$S(f_1,\ldots,f_r) \neq \phi \Leftrightarrow H(f_1,\ldots,f_r) \neq \phi \ .$$

In particular, if $f(x) \geq 0$ on $\mathbb{R}^n$ then $S(-f) = \phi$ implying that for all orders P, $-f \notin P$, i.e. for all such $P's$, $f \in P$, yielding that f is a sum of squares.

Mahé's result finds a natural interpretation in terms of the real spectrum for any commutative ring A. If $\alpha = (\rho,P) \in \mathrm{Sper}\, A$ and a quadratic form φ over A are given we set

$$\mathrm{sgn}_\alpha(\varphi) = \mathrm{sgn}_P(\varphi \otimes_A A/\rho)$$

to get, as in the previous case, a ring homomorphism

$$\mathrm{sgn} : \begin{cases} W(A) \longrightarrow C(\mathrm{Sper}\, A, \mathbb{Z}) \\ [\varphi] \longmapsto \{\alpha \longmapsto \mathrm{sgn}_\alpha \varphi\} \end{cases}$$

We then have the

***Theorem* (of Mahé in the general form)**

The cokernel of $\mathrm{sgn} : W(A) \longrightarrow C(\mathrm{Sper}\, A, \mathbb{Z})$ *is a 2-primary torsion group.*

G. Brumfiel [Br1, Br2] has found a K-theoretic refinement of Mahé's result by defining a K-group KO(Sper A) and a natural map $W(A) \longrightarrow$ KO(Sper A) which together with the dimension map KO(Sper A) $\longrightarrow C(\text{Sper } A, \mathbb{Z})$ gives a factorization :

$$\text{sgn} : W(A) \longrightarrow \text{KO(Sper } A) \longrightarrow C(\text{Sper } A, \mathbb{Z}) .$$

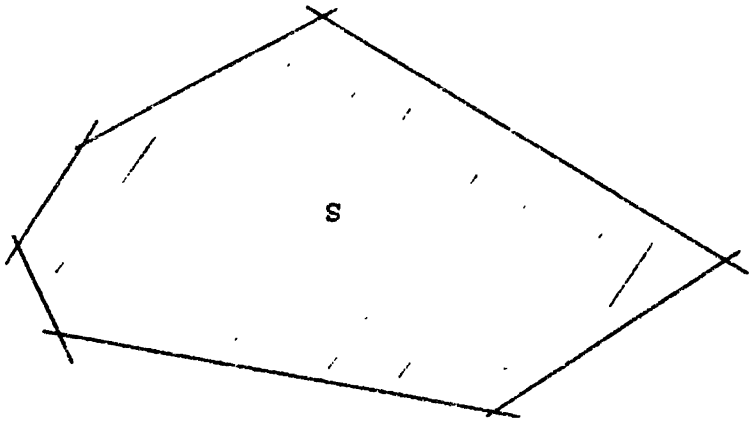
The above map $W(A) \longrightarrow$ KO(Sper A) is known from topology where one has the isomorphism $W(C(X,\mathbb{R})) \simeq KO(X)$ if X is any compact Haudsorff space, cf. e.g. [M-H,V]. The chapter 15 of [B-C-R] contains a very readable account of the relation between Witt rings and K-theory, not in the most general form as indicated above rather than concentrating on the concrete geometric situation $A = \mathbb{R}[V]$ and replacing Sper A by $V(\mathbb{R})$.

At the end of § 1 it was mentioned that in the case of "$V(\mathbb{C})$ finite", i.e. dim $V = 0$, the number $c(V; g_1, \ldots, g_n)$ can be computed by finding h such that $c(V; g_1, \ldots, g_n) = c(V; h)$. This is a consequence of a much more general and surprising result. To formulate it let V be any affine variety over $\mathbb{R}$ of dim $V = n$. Set $S(f_1, \ldots, f_r) = \{x \in V(\mathbb{R}) \mid f_1(x) > 0, \ldots, f_r(x) > 0\}$ where $f_1, \ldots, f_r \in \mathbb{R}[V]$. Assume further that $\mathbb{R}[V]$ is an integral domain with quotient field $\mathbb{R}(V)$. Under this hypothesis one has the following theorem of Bröcker and Scheiderer :

Theorem ([S]). *Given any number of regular function* $f_1, \ldots, f_r \in \mathbb{R}[V]$ *one can find* $g_1, \ldots, g_{\bar{n}} \in \mathbb{R}[V]$, $\bar{n} = \max\{1, n\}$, *such that*

$$S(f_1, \ldots, f_r) = S(g_1, \ldots, g_{\bar{n}}) .$$

This is an amazing theorem which at the moment resists any direct proof. It also seems to contradict our intuition in as much as even in simple cases one does not see how to construct the function $g_1, \ldots, g_{\bar{n}}$. In particular, consider this figure in the plane :



Clearly, $S = S(L_1, ..., L_7)$ where the L_i's are suitably closen linear forms. By the above theorem one should be able to find polynomials $g_1, g_2 \in \mathbb{R}[X,Y]$ satisfying $S = S(g_1,g_2)$. But how can this be done pratically ?

The proof of the theorem is an interesting blend of the theory of the real spectrum, quadratic form theory and general real algebraic geometry cf. also [A-B], [Brö]. It was exactly the notion of the real spectrum that tied together seemingly disparate methods and results. Consider the diagramm (associated to the real affine n-space $\mathbb{R}^n$, $X = (X_1, ..., X_n)$) :

$$\begin{array}{ccc} & \text{Sper } \mathbb{R}[X] & \\ \swarrow & & \searrow \\ \mathbb{R}^n & & \text{Sper } \mathbb{R}(X) \end{array}$$

and $S = S(f_1, ..., f_r)$. This latter set induces the characteristic function $\chi_S : \mathbb{R}^n \longrightarrow \mathbb{Z}$. Setting as above $D := D(f_1, ..., f_r) \subset \text{Sper } \mathbb{R}[X]$ we see that $\chi_S : \text{Sper } \mathbb{R}[X] \longrightarrow \mathbb{Z}$ extends χ_S. Neither χ_S nor χ_D are continuous in general. However the function $\chi_{D\,|\,\text{Sper } \mathbb{R}(X)} = \chi_H$, where $H(f_1, ..., f_r)$ as above, is in $C(\text{Sper } \mathbb{R}(X), \mathbb{Z})$. This ring is accessible by quadratic form theory, since, as a very special case of Mahé's theorem the natural map

$$W(\mathbb{R}(X)) \xrightarrow{\text{sgn}} C(\text{Sper } \mathbb{R}(X), \mathbb{Z})$$

has a 2-primary cokernel, in fact of exponent 2^n , as can be proved by additional arguments. One derives from this that $H(f_1, ..., f_r) = H(g_1, ..., g_n)$ holds for some $g_1, ..., g_n \in \mathbb{R}[X_1, ..., X_n]$. It is now the task of the proof to transfer this information from Sper $\mathbb{R}(X)$ via Sper $\mathbb{R}[X]$ finally back to $\mathbb{R}^n$ to prove the theorem.

Bibliography

[A] Artin E. : *Uber die Zerlegung definiter Funktionen in Quadrate.* Hamb. Abh. **5**, 100-115 (1927).

[A-B] Andradas C. and Becker E. : *Real stability index of rings and its application to semialgebraic geometry.* In : Séminaire sur les structures algébriques ordonnées (1984-1987), Publications mathématiques de l'Université de Paris VII **33**, 61-86 (1990).

[Ba] Baeza R. : *Quadratic forms over semi-local rings.* LN in Math. 655 (1978).

[Be1] Becker E. : *Valuations and real places in the theory of formally real fields.* In : Géométrie algébrique réelle et formes quadratiques, LN in Mathematics 959, 1-40 (1982).

[Be2] Becker E. : *The real holomorphy ring and sum of* 2n-th *power.* In : Géométrie algébrique réelle et formes quadratiques, LN in Mathematics 959, 139-181 (1982).

[Be3] Becker E. : *On the real spectrum of a ring and its application to semialgebraic geometry*, Bull. AMS 15,1 (1986), 19-60.

[B-B-D-G] Becker E., Berr R., Delon F., Gondard D. : *Hilbert's* 17^{th} *problem for sums of* 2n-th *powers.* Preprint (1990).

[B-R] Benedetti R., Risler J.-J. : *Real algebraic and semi-algebraic sets.* Hermann Editeurs, Paris (1990).

[B-C-R] Bochnak J., Coste M., Roy M.-F. : *Géométrie algébrique réelle.* Ergebn. der Math. 3 Folge Bd. 12, Springer-Verlag, Berlin-Heidelberg (1987).

[B1] Borchardt C. : *Développements sur l'équation à l'aide de laquelle on détermine les inégalités séculaires du mouvement des planètes.* J. Math. Pures Appl. **12**, 50-67 (5) (1847).

[B2] Borchardt C. : *Remarque relative à la note précédente.* J. Reine Angew. Math. **53**, 367-368 (1857).

[Br1] Brumfiel G.W. : *Witt rings and K-theory.* Rocky Mtn. J. Math. **14**, 733-765 (1984).

[Br2] Brumfiel G.W. : *The real spectrum of an ideal and KO-theory exact sequences. K*-theory 1 211-235 (1987).

[Brö] Bröcker L. : *Minimale Erzeugung von Positivbereichen.* Geom. Dedicata **16**, 335-350 (1984).

[Bu] Buchberger B. : *Gröbner bases : an algorithmic method in polynomial ideal theory.* In : Multidimensional Systems Theory (N.K. Bose ed.), D. Reidel Publishing Company, Dordrecht-Boston-Lancaster, 184-232 (1985).

[CaGaHe] Caniglia L., Galligo A., Heintz J. : *Some new effectivity bounds in computational geometry.* In : LN in Computer Science **357** (1988).

[G] Gantmacher F.R. : *Applications of the theory of matrices.* Interscience Publischers, New-York - London - Sidney (1959).

[GiTrZ] Gianni P., Trager B., Zacharias G. : *Gröbner bases and primary decomposition of polynomial ideals.* In : Computational aspects of commutative algebra (L. Robbiano ed.), Acad. Press London, 15-33 (1989).

[GLRR] Gonzalez L., Lombardi H., Recio T., Roy M.-F. : *Spécialisation de la suite de Sturm et sous-résultants.* Revue d'informatique théorique, to appear.

[H1] Hermite C. : *Sur l'extension du théorème de M. Sturm à un système d'équation simultanées.* C.R. Acad. Sci. Paris **35**, 52-54 (6,11,12,12) (1852).

[H2] Hermite C. : *Remarques sur le théorème de M. Sturm*, C.R. Acad. Sci. Paris **36** 294-297 (6,8,10) (1853).

[H3] Hermite C. : Extrait d'une lettre de Mr. Ch. Hermite de Paris à Mr. Borchardt de Berlin, *sur le nombre des racines d'une équation algébrique comprises entre les limites données.* J. Reine Angew. Math. **52**, 39-51 (6,7,17,20,24,27,27,32) (1856).

[H-M] Houdebine J., Mahé L. : *Séparations des composantes connexes réelles dans le cas des variétés projectives.* In : LN in Math. **959**, 358-370 (1982).

[K] Kohvidov I.S. : *Hankel and Toeplitz matrices and forms.* Birkhäuser-Verlag, Boston-Basel-Stuttgart (1982).

[Kn] Knebusch M. : *An invitation to real spectra.* In : 1983 Conference on quadratic forms and hermitian K-theory (C.R. Riehm, J. Hambleton ed.) Can. Math. Soc. Conf. Proc. **4** (1984).

[Kn-S] Knebusch M., Scheiderer C. : *Einfürhrung in die reelle Algebra.* Vieweg-Verlag, Braunschweig / Wiesbaden (1989).

[Kr-N] Krein M.G., Naimark M.A. : *The method of symmetric and hermitian forms in the theory of the separation of the roots of algebraic equations.* Linear and Multilinear Algebra **10**, 265-308 (1981).

[L] Lam T.Y. : *An introduction to real algebra.* Rocky Mtn. J. Math. **14**, 767-814 (1984).

[Ma1] Mahé L. : *Signatures et composantes connexes.* Math. Ann. **260**, 191-210 (1982).

[Ma2] Mahé L. : *Théorème de Pfister pour les variétés et anneaux de Witt réduits.* Invent. Math. **85**, 53-72 (1986).

[M-H] Milnor J., Husemoller D. : *Symmetric bilinear forms.* Ergebn. der Math. **73**, Springer-Verlag, Berlin-Heidelberg (1973).

[Ob] Obreschkoff N. : *Verteilung und Berechnung der Nulsstellen reeller Polynom.,* VEB Deutscher Verlagder Wissenschaften, Berlin (1963).

[P] Pfister A. : *Hilbert's seventeenth problem and related problem on definite forms.* In : Mathematical developments arising from Hilbert Problems, Proc. Symp. Pure Math. **28**, part 2, 483-489 (1976).

[Sch] Scheiderer C. : *Stability index of real varieties.* Invent. Math. **97**, 467-483 (1989).

[Se] Seidenberg A. : *Constructions in Algebra.* Trans AMS **197**, 273-313 (1974).

[S] Sylvester J. : *On a theory of the syzygetic relations of two rational integral functions, comprising an application to the theory of Sturm's functions, and that of the greatest Algebraical Common Measure.* Philos. Trans. Roy. Soc. London **143**, 407-548 (7,8,10,13,17,19) (1853).

[Schw] Schwartz N. : Der Raum der Zusammenhangskomponenten einer reellen Varietät, Geom. Dedicata 13 (1983), 361-397.