

Reducing inequalities with bounds

Jérôme Burési

Université d'Artois, Faculté Jean-Perrin, Rue Jean Souvraz
BP 18, F62307 LENS Cedex

Louis Mahé*

IRMAR, Université de Rennes 1, F35042 RENNES Cedex

Abstract

We show how an elementary and constructive proof of Bröcker-Scheiderer theorem can be used to keep control on the degrees of the polynomials involved in the process of reduction of systems of inequalities.

1 Introduction

Bröcker [Br2] and Scheiderer [Sch] have independently proved the now famous theorem that every system of simultaneous strict inequalities in a real variety of dimension d can be reduced to at most d such inequalities. In [Ma2], the second author of the present paper has announced another proof, somehow more "elementary" in the sense that it uses only classical techniques of Pfister forms. This proof is also more constructive and allows to consider explicit algorithmic reductions. For instance we may ask the following question: given a system of inequalities of n polynomials $f_1 > 0, \dots, f_n > 0$ in d variables of degree bounded by B , can we give a bound B' for the degree of an equivalent system of inequalities of d polynomials $g_1 > 0, \dots, g_d > 0$?

In sections 2 and 3, we present in full details the theoretical proof we use, in the general setting of the real spectrum of a ring, leaving intentionally aside the computational aspects and we end up section 3 by this reduction theorem:

*Partially supported by European Community contract CHRX-CT94-0506

Theorem 1.1 (Bröcker-Scheiderer) *Let A be any R -algebra of transcendence degree $d > 0$ over the real closed field R , then any system of strict inequalities $f_1 > 0, \dots, f_n > 0$ with $f_i \in A$, is equivalent to a system $g_1, \dots, g_{\max(d,1)}$ with $g_i \in A$.*

In that theorem, two systems of inequalities are said to be equivalent if the parts of the real spectrum $\text{Spec}_r A$ where they are satisfied are the same. As a corollary we get of course that any basic open semi-algebraic set in a real algebraic set V of dimension $d > 0$ is generated by d polynomial functions on V .

In section 4, we show how we can control the degree in the theorem of Tsen-Lang, which is the first tool in our proof. In section 5, we answer partially the question above: we give a bound B' for a system $g_1 > 0, \dots, g_d > 0$ "generically" equivalent to $f_1 > 0, \dots, f_n > 0$: the solution sets may differ by positive codimensional subsets. The explicit result we find for B' is $B' = ((3^d + 1)d(d + 1))^{n-d} B$. Eventually, in section 6, we give a complete answer in the 2-variable case (notice that the 1-variable case is rather trivial).

Before starting the proofs, let us recall some known facts and fix notations about quadratic forms on fields and rings. Notice that we deal here only with quadratic forms over free modules.

Definitions 1.2 Let A be any ring, a quadratic form of dimension n on A is a quadratic homogeneous polynomial map $\sum_{i,j=1}^n a_{ij}x_i x_j$ with coefficients $a_{ij} \in A$. A *diagonal* quadratic form has the shape $\sum_{i=1}^n a_i x_i^2$ and is denoted by $\langle a_1, \dots, a_n \rangle$. The form is said to be *regular* if the determinant $\prod a_i$ is a unit.

Two n -dimensional quadratic forms q_1 and q_2 are said to be isometric, and this will be denoted by $q_1 \simeq q_2$, if there is an automorphism f of A^n such that $\forall x \in A^n$ $q_1(f(x)) = q_2(x)$.

An r -fold Pfister form on A is a 2^r -dimensional quadratic form $\varphi = \langle 1, f_1 \rangle \otimes \dots \otimes \langle 1, f_r \rangle$. Once developed, it takes the shape $\langle 1 \rangle \perp \varphi'$, and φ' is called the *pure subform* of φ .

An element $h \in A$ is said to be *represented* by an n -dimensional form q over A if there exists $u \in A^n$ such that $h = q(u)$.

The element h is said to be *weakly represented* by q over A if there exist some $u_1, \dots, u_s \in A^n$ such that $h = q(u_1) + \dots + q(u_s)$. If $q = \langle a_1, \dots, a_n \rangle$, this is equivalent to $h = \sum_{i=1}^n a_i t_i$ with the t_i 's sums of s squares in A . As this means that h is represented by a multiple $s \times q$ of q , we will denote symbolically the fact by $h = s \times q(u)$.

For definitions and basic facts about real spectrum, we refer to [BCR]. Let us just say that a point γ of $\text{Spec}_r A$ may be thought as a homomorphism

from A to some real closed field, denoted by $k(\gamma)$. An element $a \in A$ is said to be positive at γ if the image of a in $k(\gamma)$ is positive, and totally positive if $a(\gamma) > 0$ for every $\gamma \in \text{Spec}_{\mathbb{R}} A$.

Given a form q and a point $\gamma \in \text{Spec}_{\mathbb{R}} A$, we can talk about the signature $\hat{q}(\gamma)$ of $q(\gamma) := q \otimes k(\gamma)$.

A constructible set in $\text{Spec}_{\mathbb{R}} A$ is a set defined by intersections, unions and complement of sets $\{x \in \text{Spec}_{\mathbb{R}} A : f(x) > 0\}$.

A basic open set in $\text{Spec}_{\mathbb{R}} A$ is a constructible set of the form

$$S_A(f_1, \dots, f_n) = \{x \in \text{Spec}_{\mathbb{R}} A : f_i(x) > 0 \text{ for } i = 1, \dots, n\}.$$

2 Generic reduction: the field case

If V is a real variety and $A = R[V]$ its coordinate ring, there is an isomorphism of boolean algebras between semi-algebraic subsets of $V(R)$ and constructible subsets of $\text{Spec}_{\mathbb{R}} A$. If K is the product of the function fields K_i of the irreducible components of V , there is an embedding of $\text{Spec}_{\mathbb{R}} K$ in $\text{Spec}_{\mathbb{R}} A$, and given two semi-algebraic subsets B and C of $V(R)$, they coincide up to positive codimensional subsets if and only if their traces on $\text{Spec}_{\mathbb{R}} K$ are equal. So, in order to make a "generic" reduction of the semi-algebraic set $\{x \in V(R) : f_1(x) > 0, \dots, f_n(x) > 0\}$, it is enough to make a true reduction at the level of $\text{Spec}_{\mathbb{R}} K$. We immediately see it is enough to consider the case V is irreducible and K is a field.

The pillar of the proof is the following quadratic form result:

Theorem 2.1 *Let K be a field of transcendence degree d over a real closed field R and φ a regular n -fold Pfister form over K , with $n > \max(d, 1)$. Then 1 is represented over K by the pure subform φ' .*

Proof. If φ is isotropic, then φ' contains a subform of the type $\langle a, -a \rangle$ which represents 1 (recall $n \geq 2$). So, we may assume φ anisotropic. Thus, the field $K(i)$ has transcendence degree d over the algebraically closed field $R(i)$, and the form φ extended to $K(i)$ has degree 2, with $2^n > 2^d$ variables: By the theorem of Tsen-Lang [Lan], φ has a unimodular zero $u \in K(i)^{2^n}$. As φ is anisotropic over K , this shows in passing that $i \notin K$ and that $\{1, i\}$ is a basis of $K(i)$ over K . Denoting respectively by Ru and Iu the "real" and "imaginary" part of u , we get

$$\varphi(u) = \varphi(Ru) + 2i\langle Ru, Iu \rangle_{\varphi} - \varphi(Iu) = 0$$

(where $\langle \cdot, \cdot \rangle_{\varphi}$ denotes the polar form of φ). Thus we get the system

$$\varphi(Ru) = \varphi(Iu); \langle Ru, Iu \rangle_{\varphi} = 0.$$

Using the multiplicativity of Pfister forms [Pfi], one finds a vector z such that $\varphi(Ru)\varphi(Iu) = \varphi(Ru)^2 = \varphi(z)$; because φ is anisotropic and u is not zero, $\varphi(Ru) \neq 0$ and we may divide z by $\varphi(Ru)$ to get $1 = \varphi(\frac{z}{\varphi(Ru)})$. But by the same theorem of Pfister, φ being anisotropic, the first component of z is equal to $\langle Ru, Iu \rangle_\varphi = 0$, and so actually 1 has the form $\varphi'(z')$. \square

The next step is the following result which is a variant, a bit more efficient for our purpose, of [Lam, chap. 10, prop. 1.5]:

Theorem 2.2 *Let for $1 \leq i \leq r$, $\varphi_i = \ll f_1, \dots, f_i \gg$ be a regular Pfister form, u_i , $i = 1 \dots r-1$ elements in K represented by φ_i and u_0 a square in K . Define $\omega_i := \sum_{j=i+1}^r f_j u_{j-1}$. Then, if the ω_i 's are units, we have $\varphi_r \simeq \ll \omega_0, f_1 \omega_1, \dots, f_{r-1} \omega_{r-1} \gg$.*

Proof. Let us remind first the following:

if a, b and $a + b$ are units, then (1) $\ll a, b \gg \simeq \ll a + b, ab \gg$,

if b is represented by a regular Pfister form q , then (2) $q \otimes \ll a \gg \simeq q \otimes \ll ab \gg$.

Then we prove by descending induction on k , $0 \leq k < r$, that $\varphi_r \simeq \varphi_k \otimes \ll \omega_k, f_{k+1} \omega_{k+1}, \dots, f_{r-1} \omega_{r-1} \gg$ and the result will follow in putting $k = 0$. The only thing to show is that $\varphi_{k-1} \otimes \ll f_k, \omega_k \gg \simeq \varphi_{k-1} \otimes \ll \omega_{k-1}, f_k \omega_k \gg$. As we have $\omega_{k-1} = f_k u_{k-1} + \omega_k$, when u_{k-1} is a unit, it comes from the two reminders (1) and (2), and if $u_{k-1} = 0$, then $\omega_k = \omega_{k-1}$ and we have directly $\ll f_k, \omega_k \gg = \ll \omega_{k-1}, f_k \gg \simeq \ll \omega_{k-1}, f_k \omega_k \gg$ by (2). \square

We are now able to state the following:

Theorem 2.3 *Let K be a field of transcendence degree d over the real closed field R and f_1, \dots, f_n n elements of K with $n > \max(d, 1)$. Then there exist g_1, \dots, g_d in K such that $S_K(f_1, \dots, f_n) = S_K(g_1, \dots, g_{\max(d, 1)})$.*

Proof. It is easy to see that if $\varphi = \ll f_1, \dots, f_n \gg$, we get

$$S_K(f_1, \dots, f_n) = \{x \in \text{Spec}_r K : \hat{\varphi} > 0\} = \{x \in \text{Spec}_r K : \hat{\varphi} = 2^n\}.$$

By iteration, we may assume $n = d + 1$ if $d > 0$, and $n = 2$ if $d = 0$. So, by theorem 2.1, the element 1 is represented over K by φ' , meaning $1 = \omega_0 = \sum_{j=1}^n f_j u_{j-1}$ with notations of theorem 2.2. If one ω_r would be null, we would have $1 = \varphi'_r(u)$ for some u , reducing the problem to $n = r$. So we may assume $\omega_i \neq 0$ for $i = 0 \dots n - 1 = d$ and apply theorem 2.2 to get $\varphi \simeq \ll 1, f_1 \omega_1, \dots, f_d \omega_d \gg$ and finally $S_K(f_1, \dots, f_n) = S_K(g_1, \dots, g_d)$ for $g_i = f_i \omega_i$. \square

3 Extension to rings: actual reduction

We are going to extend to Regular Function Rings, a weakened version of the results of the preceding section.

Definition 3.1 A ring A will be called a *Regular Function Ring* (RFR in short) if it satisfies the following equivalent properties:

- i) all maximal ideals of A are real
- ii) the elements $1 + \sum x_i^2$ are units in A .

The standard examples are the rings of real regular functions over some real algebraic set (rational functions that vanish nowhere on this set), but there are many other examples (like any formally real field).

Theorem 3.2 *Let A be a RFR of transcendence degree d over a real closed field R and φ a regular n -fold Pfister form over A with $n > \max(d, 1)$. Then 1 is weakly represented by the pure subform φ' over A .*

Proof. We can first reduce to the case A itself is a reduced ring: if $1 = r \times \varphi'(\bar{u})$ in A_{red} for some r , we have $1 + i = r \times \varphi'(u)$ in A for some nilpotent element i . But then, $1 + i = s^2$ for some unit s and we can divide by that s to get $1 = r \times \varphi'(v)$ in A .

Then we may assume A is noetherian: just work in $B = R[f_1, \dots, f_n]_{\Sigma}$ where $\Sigma = \{x \in R[f_1, \dots, f_n] : x \text{ is a unit in } A\}$. The ring B is a RFR (because A is so), is noetherian, has φ regular on itself and maps to A : a weak representation of 1 by φ' over B , will induce one over A .

Now, we will proceed by induction on d . If $d = 0$ and $n > 1$, A is a finite product of copies of R , and by theorem 2.1, the form φ' represents 1 over each factor and so over the product A . Let $d > 0$ and φ a $(d+1)$ -fold Pfister form, one can find (see for example [Ma1, lemme 2.3]) a non zero-divisor f such that A_f splits into a finite product of domains A_i , of transcendence degree $\leq d$. Call K_i their fraction field, theorem 2.1 says that $1 = \varphi'(u)$ over K_i and so over the product $\prod K_i$. Cancelling denominators, one finds some non zero-divisor g such that $g^2 = \varphi'(u)$ in $A_f = \prod A_i$ and $(f^r g)^2 = \varphi'(w)$ in A for some integer r .

If $f^r g$ is a unit in A , just divide by its square, otherwise go into $A/(f^r g)$: it is a RFR of transcendence degree $< d$ satisfying the induction hypothesis and we can write $1 = m \times \varphi'(\bar{x})$ in $A/(f^r g)$ for some integer m and some m -tuple of vectors x . Lifting this equation in A , we get $1 - m \times \varphi'(x) = \lambda f^r g$ for some $\lambda \in A$, and by squaring we get:

$$(1 - m \times \varphi'(x))^2 = (\lambda f^r g)^2 = \varphi'(\lambda w)$$

Expanding the lefthandside, this gives

$$1 + s^2 = m \times \varphi'(x\sqrt{2}) + \varphi'(\lambda\omega) = (m + 1) \times \varphi'(y)$$

Because $1 + s^2$ is a unit in A , we eventually obtain $1 = 2(m + 1) \times \varphi'(z)$ in A . \square

Let us now state an extension of theorem 2.2 to general rings.

Theorem 3.3 *Let A be a ring and f_1, \dots, f_r any r elements in A . Let, for $1 \leq i \leq r$ $\varphi_i = \ll f_1, \dots, f_i \gg$ be a (non necessarily regular) i -fold Pfister form, and u_i , $i = 1 \dots r - 1$ elements in A weakly represented by φ_i and u_0 a sum of squares in A . Define $\omega_i := \sum_{j=i+1}^r f_j u_{j-1}$. Then, if $\psi = \ll \omega_0, f_1 \omega_1, \dots, f_{r-1} \omega_{r-1} \gg$, we get $\hat{\varphi}_r(\gamma) = \hat{\psi}(\gamma)$ at the points γ at which both forms are regular.*

Proof. Just apply theorem 2.2 to $\varphi_r(\gamma)$ and $\psi(\gamma)$. \square

It is now easy to conclude in giving the proof of theorem 1.1.

Let A be a ring of transcendence degree d over a real closed field R , and f_1, \dots, f_n be any $n > \max(d, 1)$ elements of A . By iteration, we may assume that $n = d + 1$ if $d > 0$ and $n = 2$ if $d = 0$. Let $S = S(f_1, \dots, f_n) \subseteq \text{Spec}_r A$ and $B = A_{\Sigma_S}$ with $\Sigma_S = \{a \in A : \forall \gamma \in S \ a(\gamma) > 0\}$. The RFR B has transcendence degree $\leq d$ over R and the f_i 's are units in B . So, theorem 3.2 gives a weak representation of 1 by the pure subform φ' . With the notations of theorem 3.3, we have $1 = \omega_0$ and multiplying by the totally positive element $P^2 = (1 - f_n + f_n^2)^2$, we get a representation $P^2 = \omega'_0$ of the same shape. This can be written $(1 + f_n^2)^2 = \omega'_0 + 2f_n(1 + f_n^2) = \omega''_0$ with $\omega''_{n-1} = f_n(u'_{n-1} + 2(1 + f_n^2))$ for some u'_{n-1} weakly represented by φ_{n-1} . So, this ω''_{n-1} has the right shape and is totally positive on S , forcing all the ω''_i 's to be units in B . Cancelling denominators, we get $u = \omega'''_0$ in A for some u positive on S and by theorem 3.3, we get $\hat{\varphi}(\gamma) = \hat{\psi}(\gamma)$, with $\psi = \ll u \gg \otimes \chi$ and $\chi = \ll f_1 \omega'''_1, \dots, f_{n-1} \omega'''_{n-1} \gg$ at the points γ where both forms are regular.

Let $g_i = f_i \omega'''_i$ for $1 \leq i \leq n - 1$; the g_i 's are strictly positive on S and so $S \subseteq S_A(g_1, \dots, g_d)$; in the other hand, because each f_i divides $\prod_j g_j$, if $\gamma \in S_A(g_1, \dots, g_d)$, none of the f_i 's can be 0 at γ . But as $u = f_1 u'''_0 + \omega'''_1$ with u'''_0 a sum of squares, $u(\gamma) = 0$ implies $f_1 \omega'''_1 \leq 0$, and so for $\gamma \in S_A(g_1, \dots, g_d)$, we have $u(\gamma) \neq 0$ and ψ is regular at γ : by theorem 3.3 $\hat{\psi}(\gamma) = 2\hat{\chi}(\gamma) > 0$ and $\gamma \in S$. So we have $S = S_A(g_1, \dots, g_d)$. \square

4 Bounds in the theorem of Tseng-Lang

From now on, we take $A = R[X_1, \dots, X_d]$ with R a real closed field, we fix $n = d + 1$ polynomials f_1, \dots, f_n in A of degree bounded by B , and we want to find a bound B' such that we can assert that there exist g_1, \dots, g_d of degree at most B' in A such that $S_A(g_1, \dots, g_d) = S_A(f_1, \dots, f_n)$ up to positive codimensional subsets. We may always assume $S_A(f_1, \dots, f_n) \neq \emptyset$, or else we are already done.

From the beginning of section 2, we see that the first thing to do is to keep track of degrees in the theorem of Tseng-Lang. In order to deal easily with Pfister forms, let us fix the following notation: for an integer k less than 2^n , let us call $\varepsilon_i(k)$ the i -th binary digit of k , i.e. $k = \sum_{i=0}^{n-1} \varepsilon_i(k) 2^i$.

Denoting $R(\sqrt{-1})$ by C , we may consider the equation with coefficients in $C[X_1, \dots, X_d]$

$$\sum_{k=0}^{2^{d+1}-1} u_k^2 \prod_{i=0}^d f_{i+1}^{\varepsilon_i(k)} = 0 \quad (1)$$

where the u_i 's are the unknowns. Call $\alpha_i := \deg f_i$ and $\alpha := \sum \alpha_i$, we get the following:

Theorem 4.1 *There exists a non zero 2^{d+1} -tuple satisfying (1) such that each summand of the lefthandside has degree $\leq d\alpha$.*

Proof. Suppose we look for a solution $(u_0, \dots, u_{2^{d+1}-1})$ such that each summand of the equation has a fixed degree A , then $2A_k := \deg u_k^2 \leq A - \sum_{i=0}^d \alpha_{i+1} \varepsilon_i(k)$. Displaying everything over C , we get a system of e equations in v variables over C , with e equal to the number of monomials of degree less or equal to A , i.e. $\binom{A+d}{d}$, and $v = \sum_{k=0}^{2^{d+1}-1} \binom{[A_k]+d}{d}$ where $[A_k]$ is the integral part of A_k . We know that we will get a non trivial solution to (1) as soon as we get more unknowns than equations, i.e. if $\sum_{k=0}^{2^{d+1}-1} \binom{[A_k]+d}{d} > \binom{A+d}{d}$. We then have to prove that the above inequality holds for the choice $A = d\alpha$.

Let us begin by the following lemmas:

Lemma 4.2 *Let $\beta_1, \dots, \beta_{d+1}, A$ be integers such that $A > \beta := \sum_{i=1}^{d+1} \beta_i$ and define $A_k = \frac{1}{2}(A - \sum_{i=0}^d \beta_{i+1} \varepsilon_i(k))$. Then*

- 1) $\sum_{k=0}^{2^{d+1}-1} A_k = 2^d A - 2^{d-1} \beta$
- 2) $\sum_{k=0}^{2^{d+1}-1} (A_k + 1)(A_k + 2) \dots (A_k + d) \geq 2 \prod_{i=1}^d (A - \beta/2 + 2i)$.
- 3) $\sum_{k=0}^{2^{d+1}-1} ([A_k] + 1)([A_k] + 2) \dots ([A_k] + d) \geq 2 \prod_{i=1}^d (A - \beta/2 - 1 + 2i)$.

Proof. For every i , the equality $\sum_{k=0}^{2^{d+1}-1} \varepsilon_i(k) = 2^d$ gives

$\sum_{k=0}^{2^{d+1}-1} \sum_{i=0}^d \beta_{i+1} \varepsilon_i(k) = 2^d \beta$ and then we get 1). For 2), the condition $A \geq \beta$ ensures $A_k \geq 0$ and the convexity for $x \geq 0$ of the function $f : x \mapsto (x+1)(x+2)\dots(x+d)$ gives $\sum_{k=0}^{2^{d+1}-1} \frac{1}{2^{d+1}} f(A_k) \geq f\left(\sum_{k=0}^{2^{d+1}-1} \frac{1}{2^{d+1}} A_k\right)$. Applying 1) to the righthandside gives the result.

Let us show 3): suppose the β_i 's are all even. If A is even, then all the A_k are integers and 3) comes readily from 2). If A is odd, we may apply 2) to $A - 1$ which is still $\geq \beta$: we get $(A - 1)_k = [A_k]$ and we can conclude. If one β_i is odd, changing $\varepsilon_i(k)$ changes the parity of $2A_k$, and so half of the A_k 's (i.e. 2^d) are integers, the others being half-integers and so $\sum_{k=0}^{2^{d+1}-1} [A_k] = 2^d A - 2^{d-1} \beta - 2^{d-1}$. The same proof as in 2), added to the fact that f is increasing gives $\sum_{k=0}^{2^{d+1}-1} ([A_k] + 1)([A_k] + 2)\dots([A_k] + d) \geq 2 \prod_{i=1}^d (A - \beta/2 - 1/2 + 2i) > 2 \prod_{i=1}^d (A - \beta/2 - 1 + 2i)$. \square

Lemma 4.3 For $d > 0$ and $U \geq (d+1)/2$ we get:

$$\prod_{i=1}^d (U - 1 + 2i) \geq \left(U + \frac{d+1}{2}\right)^d$$

Proof. If $d = 1$, we have equality. If $d \geq 2$, we may group symmetric terms in the lefthandside and write $(U - 1 + 2i)(U - 1 + 2(d+1-i)) - (U + \frac{d+1}{2})^2 = 2U - (d+1)^2/4 + (2i-1)(2d+1-2i)$. If $U \geq (d+1)/2$, this is strictly positive. If d is odd, the isolated middle term is $U + d > U + (d+1)/2$. It, is then easy to conclude. \square

The proof of the last one is left to the reader:

Lemma 4.4 For all $d \in \mathbf{N}^*$, and for all $\beta \geq 0$ we have :

$$\sqrt[d]{2}((2d-1)\beta + d + 1) > 2d\beta + d + 1.$$

Now, let's finish the proof of theorem 4.1:

We know $f_i \neq 0$ (because $S \neq \emptyset$). If $\alpha < d+1$ there is some f_i of degree 0, and there is an easy solution with $(\sqrt{-f_i})^2 + f_i = 0$. If $\alpha \geq d+1$, since $d \geq 1$ we have $(d-1/2)\alpha \geq (d+1)/2$ and we may apply the preceding lemmas with $\beta_i = \alpha_i$, $U = (d-1/2)\alpha$ and $A = d\alpha$. We get:

$$\begin{aligned} \sum_{k=0}^{2^{d+1}-1} \binom{A_k + d}{d} &\geq \frac{1}{d!} 2 \prod_{j=1}^d (d\alpha - \alpha/2 - 1 + 2j), \quad (\text{lemma 4.2}) \\ &\geq \frac{1}{d!} 2 (d\alpha - \alpha/2 + \frac{d+1}{2})^d, \quad (\text{lemma 4.3}) \\ &> \frac{1}{d!} (d\alpha + (d+1)/2)^d, \quad (\text{lemma 4.4}) \end{aligned}$$

and finally, the concavity of the Log function gives $\frac{1}{d!} (d\alpha + (d+1)/2)^d \geq \frac{1}{d!} (d\alpha + 1) \dots (d\alpha + d) = \binom{d\alpha + d}{d}$, and we have proved theorem 4.1. \square

5 Quantitative generic reduction

In this section, we prove degree-controlled versions of the representation theorem 2.1 and its corollary, the generic reduction theorem 2.3. Following the plan of the proof of theorem 2.1, we see that the next step to control after the theorem of Tsen-Lang is the behaviour of the degrees in Pfister's theorem on multiplicativity.

Let us fix some notations.

Notations 5.1 Let K be a commutative field, m an integer, $f_1, \dots, f_m \in K^*$. Call φ_m the Pfister form $\ll f_1, \dots, f_m \gg$ if $m > 0$ and $\varphi_0 := \langle 1 \rangle$. This form is represented by a matrix $A_m = \text{diag}(1, f_1, f_2, f_1 f_2, \dots, f_1 f_2 \dots f_m) =$

$$\begin{pmatrix} A_{m-1} & 0 \\ 0 & f_m A_{m-1} \end{pmatrix}, \text{ for } m > 0.$$

Let $x = x_0, \dots, x_{2^m-1}$ a 2^m -tuple of elements of K : we have $x = (u, \tilde{u})$ with u, \tilde{u} some 2^{m-1} -tuple for $m > 0$. Pfister defines a $2^m \times 2^m$ matrix T_x such that $\phi_m(x)\phi_m(y) = \phi_m(T_x(y))$ and T_x is inductively defined as follows: (cf. [Pfi] Satz 1, p. 231)

$T_x = u_0$, if $x \in R$ and for $m > 0$:

$$T_x = \begin{cases} \begin{pmatrix} T_u & 0 \\ 0 & T_u \end{pmatrix} & \text{if } \phi_{m-1}(\tilde{u}) = 0 \\ \begin{pmatrix} T_u & f_m T_{\tilde{u}} \\ -T_{\tilde{u}} & U_{m-1} \end{pmatrix} & \text{if } \phi_{m-1}(\tilde{u}) \neq 0 \end{cases}$$

$$\text{where } U_{m-1} = \frac{1}{\phi_{m-1}(\tilde{u})} T_{\tilde{u}} A_{m-1}^{-1} T_u' A_{m-1} T_{\tilde{u}}$$

The transposed of A is denoted by A' and $(T_x)_{kl}$ will denote the $(k+1, l+1)$ entry of T_x . For any integer k , we put $\lambda_k := \sum_{i=0}^{\infty} \varepsilon_i(k)$ (see last section for the definition of $\varepsilon_i(k)$).

From now on we assume $K = R(X_1, \dots, X_d)$ and the f_i 's polynomials. Then, the matrix A has the shape $\text{num } A / \text{den } A$ with $\text{num } A$ a matrix with polynomial entries and $\text{den } A$ a polynomial. In the sequel, $\text{num } A$ and $\text{den } A$ will always denote a possible "numerator" and denominator for A . An interesting feature of the matrices T_x is the following:

Proposition 5.2 *For any integer m and any vector $x \in K^{2^m}$ we have*

$$(A_m^{-1} T_x' A_m)_{k,l} = (-1)^{\lambda_k + \lambda_l} (T_x)_{k,l}.$$

Proof. By induction, considering the cases k and $l \leq 2^{m-1}$ or not.

As a consequence, we get that if $x = (u, \tilde{u})$, a possible denominator for T_x is given by $\phi_m(\tilde{u}) \text{den } T_u [\text{den } T_{\tilde{u}}]^2$.

Using this, it is now possible to control the degrees of numerator and denominator of T_x . Using the preceding notations, and with the convention that an empty sum is 0, we get the following:

Proposition 5.3 *Let $m \geq 1$ be an integer, $x \in R[X_1, \dots, X_d]^{2^m}$ and let $\alpha_1, \dots, \alpha_m, A$ be integers such that $A > \sum_{i=1}^m \alpha_i$. Assume that for every $0 \leq k \leq 2^m - 1$ we have $\deg(x_k) \leq \frac{1}{2} \left(A - \sum_{i=0}^{m-1} \varepsilon_i(k) \alpha_{i+1} \right)$, and define B_m as $\frac{3^{m-1}-1}{2} A - 3^{m-2} \sum_{i=1}^{m-1} \alpha_{i+1}$, then*

- 1) $\deg(\text{den } T_x) \leq B_m$
- 2) $\deg(\text{num } T_x)_{k,l} \leq \frac{1}{2} \left(A + \sum_{i=0}^{m-1} \alpha_{i+1} (\varepsilon_i(l) - \varepsilon_i(k)) \right) + B_m$.

Proof. Let us remark first that α_1 does not appear in B_m (it is not a mistake!). Let us prove 1) by induction on m : if $m = 1$, T_x needs no denominator and $B_1 = 0$. Then, we want to show step $m + 1$ from step m and so we assume $\deg(x_k) \leq \frac{1}{2} \left(A - \sum_{i=0}^m \varepsilon_i(k) \alpha_{i+1} \right)$ for every $k \in \{0, \dots, 2^{m+1} - 1\}$. Writing $x = (u, \tilde{u})$, we get for every $0 \leq k \leq 2^m - 1$ that $\deg(\tilde{u}_k) \leq \frac{1}{2} \left(A - \alpha_{m+1} - \sum_{i=0}^{m-1} \varepsilon_i(k) \alpha_{i+1} \right)$, and induction hypothesis applies to \tilde{u} with $A - \alpha_{m+1}$ and to u with A . We know from proposition 5.3 that a denominator for T_x is given by $(\text{den } T_u) (\text{den } T_{\tilde{u}})^2 \phi_m(\tilde{u})$ and so, writing $\tilde{B}_m = \frac{3^{m-1}-1}{2} (A - \alpha_{m+1}) - 3^{m-2} \sum_{i=1}^{m-1} \alpha_{i+1}$, induction hypothesis gives $\deg \text{den } T_x \leq B_m + 2\tilde{B}_m + A - \alpha_{m+1} = B_{m+1}$. The proof of 2) is similar, but long, and we skip the details. \square

Now let us come to the representation theorem: with the notations of theorem 2.1, we put $n = d+1$, $x = Ru$ and $y = Iu$. Calling $z = (0, z') = T_x \cdot y$, we get $\phi'(z') = \phi(x)\phi(y) = (\phi(x))^2$. Multiplying by $(\text{den } T_x)^2$ and putting $v = \text{den } T_x \cdot z'$, we get a polynomial P such that $P^2 = \varphi'(v)$. Concerning the degree of this P we have:

Proposition 5.4 *Let $\varphi = \ll f_1, \dots, f_{d+1} \gg$ be a $(d+1)$ -fold Pfister form, $f_i \in R[X_1, \dots, X_d]$, $\alpha_i = \deg f_i$ for each i and $\alpha = \sum_{i=1}^{d+1} \alpha_i$. Then there exist $P \in R[X_1, \dots, X_d]$ with P^2 of the shape $\varphi'(v)$ and*

$$\deg P \leq \frac{(3^d + 1)}{2} d\alpha - 3^{d-1}(\alpha - \alpha_1).$$

Proof. We have $P = \varphi(x) \text{den } T_x$, and by theorem 4.1, we may take x such that $\deg \varphi(x) \leq A = d\alpha$ and $\deg x_k$ satisfying hypotheses of proposition 5.3, so $\deg \text{den } T_x \leq B_{d+1}$, which gives $\deg P \leq A + B_{d+1}$. \square

Remark 5.5 Actually, it is not only P^2 which has degree bounded by $2(A + B_{d+1})$, but also each summand $v_k^2 \prod_{i=0}^d f_{i+1}^{\varepsilon_i(k)}$ of $\varphi'(z')$: we have $v_k = \sum_{l=0}^{2^{d+1}-1} (\text{num } T_x)_{k,l}(y)_l$, and by theorem 5.3 we know that

$\deg(\text{num } T_x)_{k,l}(y)_l \leq \frac{1}{2} \left[A + \sum_{i=0}^d \alpha_{i+1}(\varepsilon_i(l) - \varepsilon_i(k)) \right] + B_{d+1} + \frac{1}{2} \left[A - \sum_{i=0}^d \alpha_{i+1}(\varepsilon_i(l)) \right]$, that is $A - \frac{1}{2}(\sum_{i=0}^d \alpha_{i+1}\varepsilon_i(k)) + B_{d+1}$, for every $l < 2^{d+1}$. So, the same is true for v_k and we get the announced result.

As a corollary, we get:

Theorem 5.6 *Let $d > 1$, $f_1, \dots, f_{d+1} \in R[X_1, \dots, X_d]$, $K = R(X_1, \dots, X_d)$, $\alpha_i = \deg f_i$ and $\alpha = \sum_{i=1}^{d+1} \alpha_i$. There exist $g_1, \dots, g_d \in R[X_1, \dots, X_d]$ such that $\deg g_i \leq (3^d + 1)d\alpha$ and such that $S_K(f_1, \dots, f_{d+1}) = S_K(g_1, \dots, g_d)$.*

Proof. From the remark above, when P^2 is expressed in terms of ω_i 's, we have $\deg \omega_i \leq (3^d + 1)d\alpha - 2 \cdot 3^{d-1}(\alpha - \alpha_1)$. Renumbering the f_i 's if need be, we may assume that α_1 is the infimum of the α_i 's and so, by theorem 2.3, $\deg g_i = \deg \omega_i + \alpha_i \leq (3^d + 1)d\alpha + \alpha_i - 2 \cdot 3^{d-1}(\alpha - \alpha_1) < (3^d + 1)d\alpha$ by the choice of α_1 . \square

If we want to express this result in terms of a bound B for the degree of every f_i , we have the following:

Theorem 5.7 *Let $n > d > 1$, $f_1, \dots, f_n \in R[X_1, \dots, X_d]$, $K = R(X_1, \dots, X_d)$. Let B be such that $\alpha_i := \deg f_i \leq B$, then there exist $g_1, \dots, g_d \in R[X_1, \dots, X_d]$ such that $\deg g_i \leq B'$ with $B' = \left((1 + 3^d)(d(d+1))^{n-d} B \right)$ and $S_K(f_1, \dots, f_n) = S_K(g_1, \dots, g_d)$.*

Proof. There is just to remark that $\alpha \leq (d+1)B$ and iterate $n - d$ times. \square

Remark 5.8 As we will see next section, we have a better bound when $d = 2$ because of the multiplicativity of 3-fold Pfister forms in rings. In this case, $\alpha_i + 4\alpha$ (or $13B$) is enough.

6 Quantitative reduction in 2 variables

In the 2-variable case, we are able to make a complete reduction of systems of inequalities, keeping control on the degree of the final system. Precisely, putting $A = R[X, Y]$, we prove the following:

Theorem 6.1 *Given polynomials $f_1, f_2, f_3 \in A$, $\deg f_i = \alpha_i$, $\alpha = \sum \alpha_i$, there exist $g_1, g_2 \in A$ of degrees $\leq 112\alpha^2 + 26\alpha - 16$ such that $S_A(f_1, f_2, f_3) = S_A(g_1, g_2)$.*

Before starting the proof, let us fix some notations.

Notations 6.2 As usual, for $k = 0 \dots 7$, denote by $h_k = \prod_{j=0}^2 f_{j+1}^{\epsilon_j(k)}$, φ the Pfister form $\ll f_1, f_2, f_3 \gg$ and φ' the pure subform. Sums of squares will be denoted by s_i and elements weakly represented by φ' will be denoted by $\varphi'_{(i)}$, the subscript being used to identify them.

Proof. The proof will be divided in several steps.

(1) **A generic solution.** As in section 4, we apply the theorem of Tsen-Lang to φ in order to find a non zero vector $u \in C[X, Y]^8$ such that $\varphi(u) = \sum_{k=0}^7 h_k u_k^2 = 0$, and such that $\deg h_k u_k^2 \leq 2\alpha$. Calling x and y the real and imaginary part of u , we get $\varphi(x)^2 = \varphi(x)\varphi(y)$. But here φ is a 3-fold Pfister form and it is well known that such forms are multiplicative over any ring, meaning we can find $z \in R[X, Y]^8$ such that $\varphi(x)\varphi(y) = \varphi(z)$, and again, z may be chosen such that the first component z_0 is $\langle x, y \rangle_\varphi = 0$. So we have $P^2 = \sum_{k=1}^7 h_k z_k^2$ with $\deg P^2, \deg h_k z_k^2 \leq 4\alpha$ and we may find two polynomials g_1, g_2 of degree $\leq \alpha_i + 4\alpha, i = 1, 2$ (or $\leq 13B$) solving generically the reduction problem. Of course, dividing everything by a square if need be, we may assume that the z_k 's have no common factor.

(2) **Digression.** This implies in particular that P cannot vanish on a 1-dimensional part of S , or else it would also be so for the z_k 's and they would have a common factor. So P has at most a finite number of zeros on S and this leads to the following remark: taking other identities $P_i^2 = \varphi'(z_{(i)})$ of same degree (we have infinitely many of them) and adding them, we get $s_0 = \varphi'_{(0)}$ with s_0 a sum of squares still of degree $\leq 4\alpha$ vanishing on S only at the common zeros of the P_i 's. It is very unlikely that all possible identities $P_i^2 = \varphi'(z_{(i)})$ of degree $\leq 4\alpha$ have a common zero on S (the opposite would be very strange), but we have not been able to prove it so far. So, although we think it is true, we cannot assert that an identity $s_0 = \varphi'_{(0)}$ of degree $\leq 4\alpha$ with $s_0(S) > 0$ exists, and we have to do more involved computations.

(3) **Working in A/P .** Taking inspiration in the proof of theorem 1.1, we try to find a sum of squares t such that $t = \varphi'_{(2)} \pmod{P}$ and t, P having no common factor. Actually we do a little less. Writing $P^2 = \sum_{k=1}^7 h_k z_k^2 = \varphi'_{(1)}$, it is possible that P and the $(h_k z_k)^2$ have a non trivial gcd Δ , but this Δ cannot vanish on S because each of its prime factors has to divide some h_k . We are going to find an equality $P^2 s_2 + t = \varphi'_{(2)}$, with s_2, t sums of squares multiple of Δ and $\tilde{P} := P/\Delta, \tilde{t} := t/\Delta$ without any common factor. This is obtained as follows:

for $k = 1 \dots 7$ define $\delta_k = 1 - n_k h_k + n_k^2 h_k^2$ for some positive constant n_k .

Then we get:

$$(P\delta_k)^2 = \left[(1 + n_k h_k + n_k^2 h_k^2)^2 - 4n_k h_k (1 + n_k^2 h_k^2) \right] h_k z_k^2 + \sum_{j \neq k} h_j (\delta_k z_j)^2$$

and so

$$(P\delta_k)^2 + 4n_k (1 + n_k^2 h_k^2) (h_k z_k)^2 = h_k [(1 + n_k h_k + n_k^2 h_k^2) z_k]^2 + \sum_{j \neq k} h_j (\delta_k z_j)^2$$

Adding these 7 equalities, we get

$$P^2 \sum_{k=1}^7 \delta_k^2 + 4 \sum_{k=1}^7 n_k (1 + (n_k h_k)^2) (h_k z_k)^2 = \varphi'_{(2)}.$$

Calling $t = 4 \sum_{k=1}^7 n_k (1 + (n_k h_k)^2) (h_k z_k)^2$, it is clear that Δ divides t , and we can choose the n_k 's in order to have \tilde{P} and \tilde{t} without any common factor. Calling $s_2 = \sum_{k=1}^7 \delta_k^2$, we have an equality $P^2 s_2 + t = \varphi'_{(2)}$ each summand of it being of degree $\leq 8\alpha$, and $\deg t \leq 7\alpha$.

(4) Down in dimension 0. Let us call R the resultant $\text{Res}_Y(\tilde{P}, \tilde{t})$ and call I the ideal generated by R and \tilde{P} . The ring A/I is zero dimensional and so it is clear by Hensel's lemma and Chinese Remainder Theorem, that we can solve for any element $f \in A$, the equation $\bar{f}u^2 = \bar{v}^2$ in A/I , in such a way that u and v are strictly positive at the real zeros of I where f is positive, and are null at the other real zeros of I .

(5) Back in A . Making $f = f_3$ and lifting this in A , we get an identity $f_3 u^2 - v^2 = w\tilde{P} + \lambda R$ and we know that u, v are strictly positive at the zeros of P inside S . As $R = U\tilde{P} + V\tilde{t}$, putting $\mu = w + \lambda U$, we get $f_3 u^2 - v^2 = \mu\tilde{P} + \lambda V\tilde{t}$. Multiplying by Δ , changing side and squaring, we have $((f_3 u^2 - v^2)\Delta - \mu P)^2 = (\lambda V t)^2$. From $t = \varphi'_{(2)} - s_2 P^2$, and because t is itself a sum of squares, we have $(\lambda V t)^2 = \varphi'_{(3)} - s_3$. After transformation, this equality rewrites:

$$(f_3 u^2 \Delta + v^2 \Delta - \mu P)^2 - 4\Delta^2 f_3 u^2 v^2 + s_3 - \varphi'_{(3)} = -4v^2 \Delta \mu P$$

Adding $0 = P^2 - \varphi'_{(1)} = P^2(1 + f_3 + f_3^2) - \varphi'_{(1)}(1 + f_3 - f_3^2) - 4f_3(1 + f_3^2)P^2$ to the lefthandside, we may write $-4v^2 \Delta \mu P = s_4 - \varphi'_4$ with $s_4 = (f_3 u^2 \Delta + v^2 \Delta - \mu P)^2 + s_3 + P^2(1 + f_3 + f_3^2)$ and $\varphi'_4 = 4\Delta^2 f_3 u^2 v^2 + \varphi'_3 + \varphi'_{(1)}(1 + f_3 - f_3^2) + 4f_3(1 + f_3^2)P^2$ strictly positive on S (because $\Delta^2 f_3 u^2 v^2$ doesn't vanish at the points of S at which P^2 vanishes, and $\varphi'_{(3)}, \varphi'_{(1)}$ are non negative on S).

Squaring again, we get $(s_4 - \varphi'_{(4)})^2 = (4\Delta \mu v^2)^2 P^2 = \varphi'_{(5)}$, which leads to $(s_4 + \varphi'_{(4)})^2 = 4s_4 \varphi'_{(4)} + \varphi'_{(5)} = \varphi'_{(6)}$ and $\varphi'_{(6)}$ is strictly positive on S .

Now, $\varphi'_{(6)} = f_1 \sigma_0 + f_2 \sigma_1 + f_3 \sigma_2$ with σ_i weakly represented by φ_i ($\varphi_0 = \langle 1 \rangle$). We may observe that $\sigma_2 = 4s_4(4u^2 v^2 \Delta^2 + 4P^2(1 + f_3^2) + \dots)$ is strictly positive on S , forcing $\omega_2 = f_3 \sigma_2$ and $\omega_1 = f_2 \sigma_1 + \omega_2$ to be so. Now, putting $g_1 = f_1 \omega_1, g_2 = f_2 \omega_2$, we have $S = S_A(g_1, g_2)$ as shown in section 3.

(6) Counting degrees. We have to estimate the degree of g_i in terms of α . Having a close look at the computations above, we see that when we express $\varphi'_{(2)}$ and $\varphi'_{(3)}$ as $\sum h_k u_k$, for u_k sums of squares, then the degree of each summand $h_k u_k$ is not greater than the degree of the sum (this is because it is true for $\varphi'_{(1)}$, as shown in remark 5.5). As $\deg \varphi'_{(1)} \leq 4\alpha$, we have $\deg \varphi'_{(2)} \leq 8\alpha$ and $\deg \varphi'_{(3)} \leq 8\alpha + \deg t + 2 \deg \lambda V$. We have $\deg t \leq 7\alpha$; let us compute $\deg \lambda V$.

Up to a linear change of coordinates, we may always assume that P (and thus \tilde{P}) is monic as a Y -polynomial. So, in step (5), making the euclidean division of u, v, λ by \tilde{P} in Y , we may assume that u, v, λ have a degree in Y less than $\deg \tilde{P}$. forcing $\deg_Y w$ to be $\leq \deg_Y \tilde{P} + \deg_Y f_3 - 2$. Now, dividing the coefficients of u, v, w by R along X , we may also assume that $\deg_X u, \deg_X v, \deg_X w \leq \deg R - 1$ and $\deg_X \lambda \leq \deg R + \alpha_3 - 2$. This last operation does not modify the degree in Y of u, v, w , but does modify $\deg_Y \lambda$, which becomes only $\leq \deg_Y f_3 + 2 \deg_Y \tilde{P} - 2$. Adding the degrees in X and Y of everything, we get:

$$\begin{aligned} \deg u, v &\leq \deg R + \deg \tilde{P} - 2 \\ \deg w &\leq \deg R + \deg \tilde{P} - 3 + \deg f_3 \\ \deg \lambda &\leq \deg R + 2 \deg \tilde{P} - 4 + 2 \deg f_3. \end{aligned}$$

Knowing that $\deg V = \deg R - \deg \tilde{t} = \deg \tilde{t}(\deg \tilde{P} - 1)$, we have

$$\deg(\lambda V)^2 \leq 2(2 \deg R + 2 \deg \tilde{P} - \deg \tilde{t} - 4 + 2\alpha_3)$$

and as $\deg R = \deg \tilde{P} \deg \tilde{t}$ we have

$$\begin{aligned} \deg \varphi'_{(3)} &\leq \deg(\lambda V)^2 + 15\alpha \\ &\leq 4 \deg R + 4 \deg \tilde{P} - 2 \deg \tilde{t} - 8 + 4\alpha_3 + 15\alpha \\ &= 4 \deg \tilde{P} + 2 \deg \tilde{t}(2 \deg \tilde{P} - 1) - 8 + 4\alpha_3 + 15\alpha \end{aligned}$$

$\leq 8\alpha + 56\alpha^2 - 14\alpha - 8 + 4\alpha_3 + 15\alpha = 56\alpha^2 + 9\alpha - 8 + 4\alpha_3 =: N_1$. As this is also greater than the degree of $s_3, f_3(\Delta uv)^2, (f_3 u^2 \Delta + v^2 \Delta - \mu P)^2, P^2(1 \pm f_3 + f_3^2)^2$ and $f_3(1 + f_3^2)P^2$, N_1 is a bound for the degree of s_4 and any summand of $\varphi'_{(4)}$, showing that each summand of $\varphi'_{(6)}$ has degree less or equal to $2N_1$. At the end we have

$\deg g_2 \leq \deg f_2 + 2N_1 \leq 112\alpha^2 + 26\alpha - 16$ and this estimate works also for g_1 . Of course, there is a big gap between this bound and the bound 5α in the generic case, and there is probably much better to do. \square

In terms of B we have:

Corollary 6.3 *Given polynomials $f_1, f_2, f_3 \in A$, $\deg f_i \leq B$, there exist $g_1, g_2 \in A$ of degrees $\leq 1008B^2 + 63B - 16$ such that $S_A(f_1, \dots, f_n) = S_A(g_1, g_2)$.*

Proof. evident. \square

References

- [BCR] J. Bochnak, M. Coste, M.-F. Roy, *Géométrie Algébrique Réelle*, *Ergeb. der Math.* **3** 12, Springer Verlag, Berlin Heidelberg New-York, (1987)
- [Br1] L. Bröcker, *Spaces of orderings and semi-algebraic sets*, *Can. Math. Soc., Conf. Proc.* **4** (1984), 231-248.

- [Br2] L. Bröcker, *On basic semi-algebraic sets*, Expo. Math. **9** (1991), 289-334.
- [Lam] T. Y. Lam, *The Algebraic Theory of Quadratic forms*, Benjamin, Reading, (1973).
- [Lan] S. Lang, *On quasi algebraic closure*, Ann. Math. **55** (1952), 373-390.
- [Ma1] L. Mahé, *Théorème de Pfister pour les variétés et anneaux de Witt réduits*, Invent. Math. **85** (1986), 53-72.
- [Ma2] L. Mahé, *Une démonstration élémentaire du théorème de Bröcker-Scheiderer*, C.R. Acad. Sc. Paris, **309** (1989), Série I, 613-616.
- [Pfi] A. Pfister, *Zur Darstellung definiter Funktionen als Summe von Quadraten*, Invent. Math. **4** (1967), 229-237.
- [Sch] C. Scheiderer, *Stability index of real varieties*, Invent. Math. **97** (1989), 167-183.

