The Positivstellensatz and small deduction rules for systems of inequalities

Henri Lombardi [1],
Nikolai Mnev [2],
Marie-Françoise Roy[3]

1 Introduction

Let $\mathbf{R}$ be any real closed field. A *set of sign conditions* $C = [C_=,\ C_{\geq}\ , C_>]$ is a list of three finite sets of polynomial in $\mathbb{Z}[X_1, \ldots, X_k]$. The *basic semi-algebraic set defined by* C , $\mathcal{S}(C) \subset \mathbf{R}^k$, is the set

$$\mathcal{S}(C) = \{x \in \mathbf{R}^k \mid \forall P \in C_=\ P(x) = 0,\ \forall Q \in C_{\geq}\ Q(x) \geq 0,\ \forall R \in C_>\ R(x) > 0\}$$

We shall prove a completeness theorem. We associate to the set of sign conditions C

- a geometric object: the ring $\mathcal{Q}(C)$ of quadratic functions over $\mathcal{S}(C)$, equipped with its set of nonnegative and positive functions
- a syntactic object, $\mathcal{R}(C)$, obtained as a quotient of the inductive limit of provable consequences of C under some simple deduction rules.

We will then prove the following theorem:

Theorem 1 *The ring $\mathcal{Q}(C)$ of quadratic functions is isomorphic to the ring $\mathcal{R}(C)$.*

Next we prove the following:

Theorem 2 *Two sets C_1 and C_2 of sign conditions are quadratic-ring equivalent (the rings $\mathcal{Q}(C_1)$ and $\mathcal{Q}(C_2)$ are isomorphic) if an only if they are logically equivalent that is, if they can be deduced from each other by using simple deduction rules.*

The key to these results is the link between algebra and geometry provided by Stengle's positivstellensatz ([3], [1]).

The next step in the future development of this theory (which originates from the ideas of the second author [2]) will consist in defining algebraic topological invariants associated to

[1] Laboratoire de Mathématique (URA CNRS 741), Université de Franche-Comté, 25030 Besançon CEDEX FRANCE
[2] Saint Petersburg's branch of Steklov Institute, 27 Fontanka, Saint-Petersburg, RUSSIA
[3] IRMAR (URA CNRS 305), Université de Rennes, Campus de Beaulieu 35042 Rennes cedex FRANCE
supported in part by the project ESPRIT-BRA 6846POSSO

nets of small sign conditions which are stable under the simple deduction rules. The fact that only small sign conditions are used, and that the simple deduction rules are local and can be performed by transforming a fixed number of small sign conditions without looking at the rest of the net, will be essential in the development of the algebraic topological aspects of the theory. As a consequence, if two sets of small sign conditions have different invariants, then the corresponding rings are not isomomorphic.

2 Quadratic functions associated to a basic semi-algebraic set

Definition 1 *The ring $\mathcal{Q}(C)$ is the ring generated by the coordinate functions $X_1, \ldots, X_k$ and finite compositions of the following operations:*

- *additions and multiplications,*
- *inversion of a function never vanishing within $\mathcal{S}(C)$,*
- *extraction of the nonnegative square root of nonnegative function on $\mathcal{S}(C)$.*

We immediately obtain the following properties:

- $f \in \mathcal{Q}(C)$ is nonnegative on $\mathcal{S}(C)$ if and only if it is a square in $\mathcal{Q}(C)$,
- $f \in \mathcal{Q}(C)$ is nonzero on $\mathcal{S}(C)$ if and only if it is invertible in $\mathcal{Q}(C)$.

So the subset of nonnegative functions and the subset of nonzero functions can be described via the ring structure of $\mathcal{Q}(C)$.

The ring of quadratic functions has nice algebraic properties since its elements can be described by finite algebraic information, but it also contains information about the geometry of the original basic semi-algebraic set. For example we can prove (using the notations in [1]):

Proposition 1 *The canonical morphism from $\mathbb{Z}[X_1, \ldots, X_k]$ to $\mathcal{Q}(C)$ induces a homeomorphism between the real spectrum of the ring $\mathcal{Q}(C)$ and the constructible set $\tilde{\mathcal{S}}(C) \subset Spec_r\mathbb{Z}[X_1, \ldots, X_k]$*

Proof : Given $\beta \in Spec_r\mathcal{Q}(C)$, the canonical ring homomorphism from $\mathcal{Q}(C)$ to $k(\beta)$ composed with the morphism from $\mathbb{Z}[X_1, \ldots, X_k]$ to $\mathcal{Q}(C)$ defines $\alpha \in \tilde{\mathcal{S}}(C)$ (since the defining sign conditions of C are automatically satisfied in $k(\beta)$).

Conversely, let $\alpha \in \tilde{\mathcal{S}}(C)$. It is clear that the canonical ring homomorphism from $\mathbb{Z}[X_1, \ldots, X_k]$ to $k(\alpha)$ such that $X(\alpha) = (X_1(\alpha), \ldots, X_k(\alpha)) \in \mathcal{S}(C)_{k(\alpha)}$ can be extended uniquely to a ring homomorphism from $\mathcal{Q}(C)$ to $k(\alpha)$, since $k(\alpha)$ is real closed, we thus obtain a $\beta \in Spec_r\mathcal{Q}(C)$.

It is easy to verify that this defines an homeomorphims between the real spectrum of the ring $\mathcal{Q}(C)$ and the constructible set $\tilde{\mathcal{S}}(C)$. □

Definition 2 *Let C_1 and C_2 be two sets of sign conditions. The basic semi-algebraic sets $\mathcal{S}(C_1) \subset \mathbf{R}^n$ and $\mathcal{S}(C_2) \subset \mathbf{R}^m$ are* quadratically homeomorphic *if and only if there exist an n-tuple of quadratic functions $\psi = (\psi_1, \ldots, \psi_n) \in \mathcal{Q}(C_2)$ and an m-tuple of quadratic function $\phi = (\phi_1, \ldots, \phi_m) \in \mathcal{Q}(C_1)$ such that $\phi(\mathcal{S}(C_1)) \subset \mathcal{S}(C_2),\ \psi(\mathcal{S}(C_2)) \subset \mathcal{S}(C_1),\ \psi \circ \phi = Id_{\mathcal{S}(C_1)}$, and $\phi \circ \psi = Id_{\mathcal{S}(C_2)}$.*

Proposition 2 *Let C_1 and C_2 be two sets of sign conditions. The rings $\mathcal{Q}(C_1)$ and $\mathcal{Q}(C_2)$ are isomorphic if and only if the semi-algebraic sets $\mathcal{S}(C_1)$ and $\mathcal{S}(C_2)$ are quadratically homeomorphic.*

Proof : If $\mathcal{S}(C_1)$ and $\mathcal{S}(C_2)$ are quadratically homeomorphic, then the composition of elements of $\mathcal{Q}(C_2)$ with ϕ (resp. of $\mathcal{Q}(C_1)$) with ψ (resp. with ϕ) defines a ring isomorphism.

Conversely, let $\psi : \mathcal{Q}(C_1) \to \mathcal{Q}(C_2)$ and $\phi : \mathcal{Q}(C_2) \to \mathcal{Q}(C_1)$ be ring isomorphisms. Then $\phi = (\phi(Y_1), \ldots, \phi(Y_m))$ and $\psi = (\psi(X_1), \ldots, \psi(X_n))$ make $\mathcal{S}(C_1)$ and $\mathcal{S}(C_2)$ quadratically homeomorphic. □

3 Small sign conditions

Small sign conditions (equations or inequalities) are those which can be written in the following form, where a, b and c are 0, 1 or variables.

$$a + b = c,\ a \times b = c,\ a = b,\ a \geq 0,\ a > 0$$

A *net of small sign conditions* $[V, \Gamma]$ consists in a finite set of variables V and a finite set of small sign conditions Γ using only these variables and the constants 0 and 1.

To a set of sign conditions $C = [C_>, C_\geq, C_=] \subset \mathbb{Z}[X_1, \ldots, X_k]$, one associates a net of small sign conditions $\mathcal{D}(C) = [V(C), \Gamma(C)]$ as follows:

- start with the variables $X_1, \ldots, X_k$,
- construct the polynomials appearing in the defining inequalities $C_=,\ C_\geq,\ C_>$ by composing small equations, introducing as many variables as needed, in order to get, for any such polynomial P, a corresponding variable X_P,
- for every $P \in C_=$ (resp. $Q \in C_\geq,\ R \in C_>$), add $X_P = 0$ (resp. $X_Q \geq 0$, $X_R > 0$).

This construction is not unique. We shall extend the nets $\mathcal{D}(C)$ associated to C to a more invariant object: the inductive limit of its extensions under simple deduction rules.

Example 1 Let us consider $\mathcal{S}(C) \in \mathbf{R}^4$ defined by the equation $X_1^2 + X_2^2 + X_3^2 = 0$, i.e. the X_4 axis. There are two differents ways of putting brackets: $((X_1^2 + X_2^2) + X_3^2) = 0$ (1) and $(X_1^2 + (X_2^2 + X_3^2)) = 0$ (1').
One net of small sign conditions $[V_1, \Gamma_1]$ associated to $\mathcal{S}(C)$ is

$$[\{X_1, X_2, X_3, X_4, u, v, w, s, t\},$$
$$\{X_1 \times X_1 = u,\ X_2 \times X_2 = v,\ X_3 \times X_3 = w, u + v = s,\ s + w = t,\ t = 0\}]$$

while another net of small sign conditions associated to $\mathcal{S}(C)$, $[V_1', \Gamma_1']$, corresponding to (1') is

$$[\{X_1, X_2, X_3, X_4, u, v, w, s', t'\},$$
$$\{X_1 \times X_1 = u,\ X_2 \times X_2 = v,\ X_3 \times X_3 = w,\ v + w = s',\ u + s' = t',\ t' = 0\}]$$

Naturally, these two nets of small sign conditions are in some sense equivalent (through the associativity of addition). This is the notion we will make precise later.

4 Quadratic functions and the Positivstellensatz

To a quadratic function f in $\mathcal{Q}(C)$, one can also associate a net of small sign conditions $\mathcal{D}(f) = [V(f), \Gamma(f)]$:

- start with $\mathcal{D}(C)$,
- if f is the sum of two previously defined quadratic functions g and h represented by X_g and X_h, add X_f to the variables and $X_g + X_h = X_f$ to the small sign conditions,
- if f is the product of two previously defined quadratic functions g and h represented by X_g and X_h, add X_f to the variables and $X_g \times X_h = X_f$ to the small sign conditions,
- if f is the inverse of a previously defined quadratic function g represented by X_g, add X_f to the variables and $X_f \times X_g = 1$ to the small sign conditions,
- if f is the square root of a previously defined quadratic function g represented by X_g, add X_f to the variables and $X_f \times X_f = X_g,\ X_f \geq 0$ to the small sign conditions.

The proof of the completeness theorem we announced in the introduction uses as crucial tool the Positivstellensatz ([3], [1]). This theorem says that set theoretic facts concerning polynomial functions can be always certified by some algebraic identity.

Let us reformulate this result in the context of quadratic functions. Denote by X_f the variable representing f in $V(f)$ and $\mathcal{S}(f) \subset \mathbf{R}^m$ the realization set of $\Gamma(f)$.

Proposition 3 *Let us consider the polynomial ring $\mathbb{Z}[V(f)]$. Given a finite set of polynomials $L \subset \mathbb{Z}[V(f)]$, denote by $\mathcal{M}(L)$ (resp. $\mathcal{P}(L)$, $\mathcal{I}(C)$) the multiplicative monoid (resp. positive cone, ideal) generated by L. Then we have the following equivalences:*

$$f \geq 0 \text{ on } \mathcal{S}(C) \quad (1)$$
$$\text{if and only if}$$
$$\exists\ a \in \mathcal{M}(\Gamma(f)_>)\ \exists\ b_1, b_2 \in \mathcal{P}(\Gamma(f)_> \cup \Gamma(f)_\geq)\ \exists c \in \mathcal{I}(\Gamma(f)_=)\ \exists m \in \mathbb{N}$$
$$X_f \times (aX_f^{2m} + b_1) = b_2 + c \quad (1\star)$$

$$f > 0 \text{ on } \mathcal{S}(C) \quad (2)$$
$$\text{if and only if}$$
$$\exists\ a \in \mathcal{M}(\Gamma(f)_>)\ \exists\ b_1, b_2 \in \mathcal{P}(\Gamma(f)_> \cup \Gamma(f)_\geq)\ \exists c \in \mathcal{I}(\Gamma(f)_=)$$
$$(X_f \times b_1) = a + b_2 + c \quad (2\star)$$

$$f = 0 \text{ on } \mathcal{S}(C) \quad (3)$$
$$\text{if and only if}$$
$$\exists\ a \in \mathcal{M}(\Gamma(f)_>)\ \exists\ b \in \mathcal{P}(\Gamma(f)_> \cup \Gamma(f)_\geq)\ \exists c \in \mathcal{I}(\Gamma(f)_=)\ \exists m \in \mathbb{N}$$
$$aX_f^{2m} + b + c = 0 \quad (3\star)$$

Proof : Let us prove the first item, the others having completely similar proofs. The fact that

$$f \geq 0 \text{ on } \mathcal{S}(C)\ (1)$$

is equivalent to

$$X_f \geq 0 \ \text{ on } \mathcal{S}(f) \quad (1 \text{ bis}).$$

By the Positivstellensatz ([3], [1]) the fact (1 bis) is equivalent to $(1\star)$. □

5 Simple deduction rules

We will now describe the syntactic part of this paper. The idea is to introduce simple deduction rules that will make possible to transform the algebraic certificates given by the Positivstellensatz into logical proofs .

To each algebraic rule (commutativity, associativity, etc), as well as to some less classical rules for sign manipulations, corresponds a simple deduction rule. Each simple deduction rule can be read in two ways: an *extension rule* corresponding to adding logically equivalent formulae, and a *contraction rule* which consists in forgetting part of the information, still keeping a logically equivalent situation.

In the following, $[V, \Gamma]$ will be a net of small sign conditions, $V^* = V \cup \{0, 1\}$. The expression

$$[V, \Gamma] \prec [V', \Gamma'] \ \text{ in case } \ a \in V^*,\ t \notin V,\ A \subset \Gamma$$

can be read in two ways and used in two directions

- "$[V, \Gamma]$ can be extended in $[V', \Gamma']$", if a is in V^* and the variable t is not in V, and if the net of small sign conditions of Γ contains A, and also
- "$[V', \Gamma']$ can be contracted in $[V, \Gamma]$" if a is in V^* and the variable t is not in V , and if the net of small sign conditions of Γ contains A.

The rules A allow renaming of variables, the rules B add and suppress variables and allow the construction of polynomial functions, the rules C allow the construction of quadratic functions, the rules D are the ordinary rules for equality, the rules E are called ring rules (they correspond to the ring theoretic properties), while the rules F are called direct order rules (they correspond to the simplest properties of nonnegative and positive elements), and the rules G are called simplification rules. These last rules are less obvious and are needed to use various forms of the Null and Positivstellensatz, thus connecting algebra, logic and geometry.

Except for the renaming rule which is global, all the rules are "small deduction rules", they are local in the sense that their size is fixed and they modify the net of small conditions only locally.

We did not try to have a minimal list of rules but rather to have a list of natural rules.

A. **Renaming**

For any bijection σ of the set V of variables of $[V, \Gamma]$ into another finite set of variables V', define Γ_σ as the small sign conditions obtained by replacing variables $x \in V$ by variables $\sigma(x) \in V'$

$$[V, \Gamma] \prec [V', \Gamma_\sigma]$$

B. **New polynomial variables**

(1) Introduction of a variable equal to a constant or to another variable

$$x = a$$
$$[V, \Gamma] \prec [V \cup \{x\}, \Gamma \cup \{x = a\}] \text{ in case } a \in V^*,\ x \notin V$$

(2) Introduction of the sum of two elements

$$x = a + b$$
$$[V, \Gamma] \prec [V \cup \{x\}, \Gamma \cup \{a + b = x\}] \text{ in case } a \in V^*,\ b \in V^*,\ x \notin V$$

(3) Introduction of the product of two elements

$$x = a \times b$$
$$[V, \Gamma] \prec [V \cup \{x\}, \Gamma \cup \{a \times b = x\}] \text{ in case } a \in V^*,\ b \in V^*,\ x \notin V$$

(4) Introduction of the opposite of an element

$$\exists x\ a + x = 0$$
$$[V, \Gamma] \prec [V \cup \{x\}, \Gamma \cup \{a + x = 0\}] \text{ in case } a \in V^*,\ x \notin V$$

C. **New quadratic variables**

(1) Introduction of the multiplicative inverse of a positive element

$$a > 0 \ \Rightarrow\ \exists x\ a \times x = 1$$
$$[V, \Gamma] \prec [V \cup \{x\}, \Gamma \cup \{a \times x = 1\}] \text{ in case } x \notin V,\ \{a > 0\} \subset \Gamma$$

(2) Introduction of the square root of a nonnegative element

$$a \geq 0 \ \Rightarrow\ \exists x\ (x \geq 0,\ x \times x = a)$$
$$[V, \Gamma] \prec [V \cup \{x\}, \Gamma \cup \{x \geq 0,\ x \times x = a\}] \text{ in case } x \notin V,\ \{a \geq 0\} \subset \Gamma$$

Remark 1 Note that all variables introduced by rules B and C represent functions that are algebraic over previously existing variables.

D. **Axioms of equality**

(1) Reflexivity and symmetry of equality

$$a = a, \quad (a = b \;\Rightarrow\; b = a)$$
$$[V, \Gamma] \prec [V, \Gamma \cup \{a = a\}] \text{ in case } a \in V^*$$
$$[V, \Gamma] \prec [V, \Gamma \cup \{b = a\}] \text{ in case } \{a = b\} \subset \Gamma$$

(2) Transitivity of equality

$$(a = b,\ b = c) \;\Rightarrow\; a = c$$
$$((a + b = d, c = d) \;\Rightarrow\; a + b = c), ((a + b = c,\ a + b = d) \;\Rightarrow\; c = d)$$
$$((a \times b = d, c = d) \;\Rightarrow\; a \times b = c), ((a \times b = c,\ a \times b = d) \;\Rightarrow\; c = d)$$
$$[V, \Gamma] \prec [V, \Gamma \cup \{a = c\}] \text{ in case } \{a = b,\ b = c\} \subset \Gamma$$
$$[V, \Gamma] \prec [V, \Gamma \cup \{a + b = c\}] \text{ in case } \{a + b = d,\ c = d\} \subset \Gamma$$
$$[V, \Gamma] \prec [V, \Gamma \cup \{c = d\}] \text{ in case } \{a + b = c,\ a + b = d\} \subset \Gamma$$
$$[V, \Gamma] \prec [V, \Gamma \cup \{a \times b = c\}] \text{ in case } \{a \times b = d,\ c = d\} \subset \Gamma$$
$$[V, \Gamma] \prec [V, \Gamma \cup \{c = d\}] \text{ in case } \{a \times b = c,\ a \times b = d\} \subset \Gamma$$

(3) Substitution of equal variables with $+$

$$(a = b,\ c = d \;\Rightarrow\; a + c = b + d$$
$$[V, \Gamma] \prec [V, \Gamma \cup \{e = f\}] \text{ in case } \{a = b,\ c = d,\ a + c = e,\ b + d = f\} \subset \Gamma$$

(4) Substitution of equal variables with $\times$

$$(a = b,\ c = d) \;\Rightarrow\; a \times c = b \times d$$
$$[V, \Gamma] \prec [V, \Gamma \cup \{e = f\}] \text{ in case } \{a = b,\ c = d,\ a \times c = e,\ b \times d = f\} \subset \Gamma$$

(5) Substitution of equal variables in inequalities

$$((a = b,\ a > 0) \Rightarrow b > 0), ((a = b,\ a \geq 0) \Rightarrow b \geq 0)$$
$$[V, \Gamma] \prec [V, \Gamma \cup \{b > 0\}] \text{ in case } \{a = b,\ a > 0\} \subset \Gamma$$
$$[V, \Gamma] \prec [V, \Gamma \cup \{b \geq 0\}] \text{ in case } \{a = b,\ a \geq 0\} \subset \Gamma$$

E. **Equational rules of rings**

(1) Associativity of $+$

$$a + (b + c) = (a + b) + c$$
$$[V, \Gamma] \prec [V, \Gamma \cup \{d = e\}] \text{ in case } \{a + b = f,\ f + c = d,\ b + c = g,\ a + g = e\} \subset \Gamma$$

(2) Commutativity of $+$

$$a + b = b + a$$
$$[V, \Gamma] \prec [V, \Gamma \cup \{c = d\}] \text{ in case } \{a + b = c,\ b + a = d\} \subset \Gamma$$

(3) Additive property of 0

$$a + 0 = a$$
$$[V, \Gamma] \prec [V, \Gamma \cup \{b = a\}] \text{ in case } \{a + 0 = b\} \subset \Gamma$$

(4) Multiplicative property of 0

$$a \times 0 = 0$$
$$[V, \Gamma] \prec [V, \Gamma \cup \{b = 0\}] \text{ in case } \{a \times 0 = b\} \subset \Gamma$$

(5) Associativity of multiplication

$$a \times (b \times c) = (a \times b) \times c$$
$$[V, \Gamma] \prec [V, \Gamma \cup \{d = e\}] \text{ in case } \{a \times b = f,\ f \times c = d,\ b \times c = g,\ a \times g = e\} \subset \Gamma$$

(6) Commutativity of multiplication

$$a \times b = b \times a$$
$$[V, \Gamma] \prec [V, \Gamma \cup \{c = d\}] \text{ in case } \{a \times b = c,\ b \times a = d\} \subset \Gamma$$

(7) Multiplicative property of 1

$$a \times 1 = a$$
$$[V, \Gamma] \prec [V, \Gamma \cup \{b = a\}] \text{ in case } \{a \times 1 = b\} \subset \Gamma$$

(8) Distributivity

$$(a + b) \times c = (a \times c) + (b \times c)$$
$$[V, \Gamma] \prec [V, \Gamma \cup \{e = h\}] \text{ in case } \{a+b = d,\ d \times c = e,\ a \times c = f,\ b \times c = g,\ f+g = h\} \subset \Gamma$$

Example 2 The two sets of small sign conditions $[V_1, \Gamma_1]$ and $[V_1', \Gamma_1']$ (defininig the subset $X_1^2 + X_2^2 + X_3^2 = 0$ in $\mathbf{R}^4$) we have seen in example 1 can be deduced one from each other, in the sense that they have a common extension constructed using correct rules. These are precisely the rule of associativity of addition E1 and the rules of symmetry and transitivity of equality D1 and D2. Notice that by chance we did not have to use the renaming rule for setting this equivalence.

F. **Direct order rules**

(1) Nonnegative elements are stable under addition

$$(a \geq 0,\ b \geq 0) \ \Rightarrow\ a + b \geq 0$$
$$[V, \Gamma] \prec [V, \Gamma \cup \{c \geq 0\}] \text{ in case } \{a \geq 0,\ b \geq 0,\ a + b = c\} \subset \Gamma$$

(2) Nonnegative elements are stable under multiplication

$$(a \geq 0,\ b \geq 0) \ \Rightarrow\ a \times b \geq 0$$
$$[V, \Gamma] \prec [V, \Gamma \cup \{c \geq 0\}] \ \text{ in case } \ \{a \geq 0,\ b \geq 0,\ a \times b = c\} \subset \Gamma$$

(3) Positive elements are stable under addition

$$(a > 0,\ b > 0) \ \Rightarrow\ a + b > 0$$
$$[V, \Gamma] \prec [V, \Gamma \cup \{c > 0\}] \ \text{ in case } \ \{a > 0,\ b > 0,\ a + b = c\} \subset \Gamma$$

(4) Positive elements are stable under multiplication

$$(a > 0,\ b > 0) \ \Rightarrow\ a \times b > 0$$
$$[V, \Gamma] \prec [V, \Gamma \cup \{c > 0\}] \ \text{ in case } \ \{a > 0,\ b > 0,\ a \times b = c\} \subset \Gamma$$

(5) Squares are nonnegative

$$a^2 \geq 0$$
$$[V, \Gamma] \prec [V, \Gamma \cup \{b \geq 0\}] \ \text{ in case } \ \{a \times a = b\} \subset \Gamma$$

(6) 1 is positive

$$1 > 0$$
$$[V, \Gamma] \prec [V, \Gamma \cup \{1 > 0\}]$$

(7) The sum of a positive element and of a nonnegative element is positive

$$(a > 0,\ b \geq 0) \ \Rightarrow\ a + b > 0$$
$$V, \Gamma] \prec [V, \Gamma \cup \{c > 0\}] \ \text{ in case } \ \{a > 0,\ b \geq 0,\ a + b = c\} \subset \Gamma$$

(8) Positive elements are nonnegative

$$a > 0 \ \Rightarrow\ a \geq 0$$
$$[V, \Gamma] \prec [V, \Gamma \cup \{a \geq 0\}] \ \text{ in case } \ \{a > 0\} \subset \Gamma$$

(9) Zero elements are nonnegative

$$a = 0 \ \Rightarrow\ a \geq 0$$
$$[V, \Gamma] \prec [V, \Gamma \cup \{a \geq 0\}] \ \text{ in case } \ \{a = 0\} \subset \Gamma$$

G. **Simplification rules**

(1) Radical rule for equality

$$a^2 = 0 \ \Rightarrow\ a = 0$$
$$[V, \Gamma] \prec [V, \Gamma \cup \{a = 0\}] \ \text{ in case } \ \{a \times a = b,\ b = 0\} \subset \Gamma$$

(2) Nonnegative and nonpositive is zero

$$(a+b=0,\ a\geq 0,\ b\geq 0)\ \Rightarrow\ (a=0,\ b=0)$$
$$[V,\Gamma]\prec[V,\Gamma\cup\{a=0,\ b=0\}]\ \text{ in case }\ \{a+b=c,\ a\geq 0,\ b\geq 0,\ c=0\}\subset\Gamma$$

(3) Simplification rule for positive elements:

$$(a\times b>0,\ b\geq 0)\ \Rightarrow\ a>0$$
$$V,\Gamma]\prec[V,\Gamma\cup\{a>0\}]\ \text{ in case }\ \{b\geq 0,\ a\times b=c,\ c>0\}\subset\Gamma$$

(4) First simplification rule for nonegative elements:

$$(a\times b\geq 0,\ a>0)\ \Rightarrow\ b\geq 0$$
$$[V,\Gamma]\prec[V,\Gamma\cup\{b\geq 0\}]\ \text{ in case }\ \{a>0,\ a\times b=c,\ c\geq 0\}\subset\Gamma$$

(5) Second simplification rule for nonnegative elements:

$$(b\geq 0,\ a(a^2+b)\geq 0)\ \Rightarrow\ a\geq 0$$
$$[V,\Gamma]\prec[V,\Gamma\cup\{a\geq 0\}]\ \text{ in case }\ \{b\geq 0,\ a\times a=c,\ c+b=d,\ a\times d=e,\ e\geq 0\}\subset\Gamma$$

Remark 2 The rule $a^3\geq 0\ \Rightarrow\ a\geq 0$ can be easily deduced from the second simplification rule for nonnegative elements G5. In a similar way, we can prove the simplification rule $a^2\leq 0\Rightarrow a=0$ from G5 and G2.

Remark 3 Note that no new variables are introduced by rules D, E, F and G.

Definition 3 *Two sets* $[V_1,\Gamma_1]$ *and* $[V_2,\Gamma_2]$ *of small sign conditions are* logically equivalent *if there exists a net of small sign conditions* $[V,\Gamma]$ *such that* $[V,\Gamma]$ *can be deduced from both* $[V_1,\Gamma_1]$ *and* $[V_2,\Gamma_2]$ *using the extension rules.*

It is clear that two sets $[V_1,\Gamma_1]$ and $[V_2,\Gamma_2]$ of small sign conditions are logically equivalent if they can be deduced one from each other using the simple deduction rules above. This is a consequence of the symmetry between extension and contraction.

Example 3
Let us see that the net of small sign conditions

$$\mathcal{D}(C_1)=[\{X_1,X_2,X_3,X_4,t,u,v,w\},$$
$$\{X_1\times X_1=u,\ X_2\times X_2=v,\ X_3\times X_3=t,\ u+v=w,\ w+t=0\}]$$

associated to the subset $\mathcal{S}(C_1)$ defined by $X_1^2+X_2^2+X_3^2=0$ in $\mathbf{R}^4$, and the net of small sign conditions $\mathcal{D}(C_2)=[\{X_4\},\emptyset]$ associated to the line $\mathbf{R}$, are logically equivalent.

The net of small sign conditions $\mathcal{D}(C_1)$ can be extended to $[V,\Gamma]$ with

$$V=\{X_1,X_2,X_3,X_4,t,u,v,w\},$$
$$\Gamma=\{X_1\times X_1=u,\ X_2\times X_2=v,\ X_3\times X_3=t,\ u+v=w,\ w+t=0$$
$$u\geq 0,\ v\geq 0,\ t\geq 0,\ w\geq 0,\ w=0,\ t=0,\ u+v=0,\ u=0,\ v=0,$$
$$X_1\times X_1=0,\ X_2\times X_2=0,\ X_3\times X_3=0,\ X_1=0,\ X_2=0,\ X_3=0,\ 0\times 0=0,\ 0+0=0\}$$

using F5 three times, F1 four times, G2 twice, G1 three times and last D2.

On the other hand $\mathcal{D}(C_2)$ can also be extended to $[V,\Gamma]$ by introducing X_1, X_2, X_3 equal to 0 (by B1), then introducing u, v, t and a (by B3 and B2), and then applying E4, E3, and F9.

Let us also see that the net of small sign conditions

$$\mathcal{D}(C_1') = [\{X_1, X_2, u, v, w, \}, \{X_1 \times X_1 = u,\ X_2 \times X_2 = v,\ u + v = w,\ w + 1 = 0\}]$$

which is associated to the subset $\mathcal{S}(C_1')$ defined by $X_1^2 + X_2^2 + 1 = 0$ in $\mathbf{R}^2$, and $\mathcal{D}(C_2') = [\{X_1\}, \{1 = 0\}]$ which is associated to the empty set in $\mathbf{R}$, are also logically equivalent.

We first prove that $\mathcal{D}(C_1')$ can be extended to $[V,\Gamma]$ with

$$\begin{gathered} V = \{X_1, X_2, u, v, w\}, \\ \Gamma = \{X_1 \times X_1 = u,\ X_2 \times X_2 = v,\ u + v = w,\ w + 1 = 0, \\ u \geq 0,\ v \geq 0,\ w \geq 0,\ 1 \geq 0,\ 1 = 0,\ w = 0, u = 0,\ v = 0, \\ X_1 \times X_1 = 0,\ X_2 \times X_2 = 0,\ X_1 = 0,\ X_2 = 0,\ u + 0 = w, 0 = w,\ 0 \times 0 = 0,\ 0 + 1 = 0\} \end{gathered}$$

On the other hand $\mathcal{D}(C_2')$ can also be extended to $[V,\Gamma]$.

6 The inductive limit

We have to give a precise definition of the inductive limit of extensions of a net of small sign conditions. We consider a fixed infinite enumerable set Var of variables.

Given two nets of small sign conditions on Var, $[V,\Gamma]$ and $[V',\Gamma']$, $[V,\Gamma] \prec [V',\Gamma']$ means that $[V',\Gamma']$ is obtained from $[V,\Gamma]$ by applying one of the simple deduction rules. Note that when $[V,\Gamma] \prec [V',\Gamma']$ we can define an associated injection $\iota : V \to V'$. This is a bijection when the rule is the renaming rule, and a canonical injection in the other cases.

We denote $\prec\prec$ the transitive closure of $\prec$. More precisely, $[V,\Gamma] \prec\prec [V',\Gamma']$ defines an injection $\iota : V \to V'$: if

$$[V,\Gamma] = [V_1,\Gamma_1] \prec \ldots\ldots \prec [V_n,\Gamma_n] = [V',\Gamma']$$

ι is the composite of the associated injections $\iota_i : V_i \to V_{i+1}$. We remark that it is always possible to have the renaming rule only once, at the end.

One should be aware that there may exist more than one arrow ι between two fixed sets of small sign conditions $[V,\Gamma]$ and $[V',\Gamma']$.

An *extension* of $[V,\Gamma]$ is a pair $([V',\Gamma'],\iota)$ with $[V,\Gamma] \prec\prec [V',\Gamma']$ and $\iota : V \to V'$ the associated injection. We remark that this extension forgets a part of the information contained in the chain of elementary extensions. An *arrow* between two extensions $([V_1,\Gamma_1],\iota_1)$ and $([V_2,\Gamma_2],\iota_2)$ of $[V,\Gamma]$ is an extension of $[V_1,\Gamma_1]$ of the form $([V_2,\Gamma_2],\iota)$, with $\iota \circ \iota_1 = \iota_2$ the associated injection.

Let $\mathcal{S}(C)$ be a semialgebraic set and $\mathcal{D}(C) = [V(C),\Gamma(C)]$ a net of small sign conditions on Var describing $\mathcal{S}(C)$.

We denote $\mathcal{E}(C)$ the set of all the extensions $([V,\Gamma],\iota)$ of $\mathcal{D}(C)$. This family possesses an inductive limit which is $\mathcal{L}(C) = ([\mathcal{V}(C),\mathcal{C}(C)],\iota_C)$. The study of $\mathcal{L}(C)$ requires some lemmas.

Lemma 1 *Let x and y be two elements of V, where $[V,\Gamma]$ is an extension of $[V(C),\Gamma(C)]$. If x and y have the same image in $\mathcal{V}(C)$, then they are provably equal in some extension $[V',\Gamma']$ of $[V,\Gamma]$.*

Proof : We remark that by using the renaming rule we can always construct a common extension of two extensions of $[V(C),\Gamma(C)]$. So if x and y have the same image in $\mathcal{V}(C)$, then there exist an extension $[V_1,\Gamma_1]$ of $[V,\Gamma]$ and two distinct injections $\iota_1 : V \to V_1$ and $\iota_2 : V \to V_1$, each one defining $[V_1,\Gamma_1]$ as an extension of $[V,\Gamma]$, such that $\iota_1(x) = \iota_2(y)$. This implies that x and y play entirely symmetric roles in the net of small sign conditions Γ. This fact implies provable equality modulo the following lemma. □

Lemma 2 *Let x and y be variables in V (where $[V,\Gamma]$ is an extension of $[V(C),\Gamma(C)]$) introduced in the same way using rules B or C. Then they are provably equal in some extension of $[V,\Gamma]$.*

Proof: We have to verify in each case that there are corresponding small deduction rules. The only tricky proof is for two positive square roots x and y of the same nonegative element z. We get $(x-y)\times(x+y)=0$ with $x\geq 0$ and $y\geq 0$. We deduce $(x-y)\times(x+y)^2=0$, that is $(x-y)\times((x-y)^2+4xy)=0$ with $4xy\geq 0$. Next we use the second simplification rule for nonnegative elements G5 with $(x-y)=a$ and $4xy=b\geq 0$ and we get $(x-y)\geq 0$. Similarly we get $(y-x)\geq 0$ and we conclude with the simplification rule G2. □

Finally, we get the following description of the maps $V \to \mathcal{V}(C)$ given by the inductive limit construction :

Let x and y be distinct variables in V (where $[V,\Gamma]$ is an extension of $\mathcal{D}(C)$). They have the same image in $\mathcal{V}(C)$ exactly in the following case: x and y are not both images of variables in $V(C)$ and they are provably equal in some extension $[V',\Gamma']$ of $[V,\Gamma]$.

Using lemma 1 we see that we can define a ring $\mathcal{R}(C)$ by taking as elements of its basis set the equivalence classes of elements of $\mathcal{V}(C)$, i.e. "variables in $\mathcal{L}(C)$", under the equivalence relation of provable equality.

This set is naturally equipped with addition, multiplication, and nonnegative and positive elements, obtained from the small sign conditions in $\mathcal{C}(C)$. This clearly gives a partially ordered ring (more precisely an algebraic structure satisfying all the axioms corresponding to the small deduction rules).

It is clear that there is a canonical application from $\mathcal{E}(C)$ to $\mathcal{Q}(C)$ by taking as the image of an initial variable X_i the corresponding coordinate function in $\mathcal{Q}(C)$, and by following the renaming rule A and the introduction rules B and C.

7 The main result

It is clear from the preceeding paragraph that there is a canonical homomorphism from $\mathcal{R}(C)$ to $\mathcal{Q}(C)$.

Theorem 1 *Let C be a set of sign conditions. The ring $\mathcal{Q}(C)$ is isomorphic to the ring $\mathcal{R}(C)$ (by the canonical homomorphism).*

Proof : It is based on the Positivstellensatz we already quoted.

We have to see that

- If the variables X_f and X_g associated to the quadratic functions f and g are provably equal then f and g are equal. This is obvious. It means that the canonical homomorphism is a well defined function.
- If the variable X_f associated to a quadratic function f is provably ≥ 0 (resp. $= 0$, resp > 0) using the small deduction rules then f is ≥ 0 (resp. $= 0$, resp > 0) over $\mathcal{S}(C)$. This is obvious. It means that the canonical homomorphism preserve the partial order structure. In fact, it also means, arguing inductively, that the canonical application from $\mathcal{E}(C)$ to $\mathcal{Q}(C)$ is defined everywhere.
- If two quadratic functions f and g are equal then their associated variables X_f and X_g are provably equal . This implies the ring homomorphism is injective. The proof is a particular case of the following:
- If a quadratic function f is ≥ 0 (resp. $= 0$, resp > 0) over $\mathcal{S}(C)$, then the same facts are provable for its associated variable X_f . This implies (inductively) the ring homomorphism is onto.

Consider a quadratic function f on $\mathcal{S}(C)$ and its associated description $\mathcal{D}(f) = [V(f), \Gamma(f)]$ which is an extension of $\mathcal{D}(C)$.

The fact that

$$f \geq 0 \text{ on } \mathcal{S}(C)$$

is equivalent to

$$\exists\, a \in \mathcal{M}(\Gamma(f)_>)\ \exists\, b_1, b_2 \in \mathcal{P}(\Gamma(f)_> \cup \Gamma(f)_\geq)\ \exists c \in \mathcal{I}(\Gamma(f)_=)\ \exists m \in \mathbb{N}$$
$$X_f \times (a{X_f}^{2m} + b_1) = b_2 + c.$$

This algebraic identity will be proved somewhere in an extension of $\mathcal{D}(f)$ using the equational ring rules and the definition of f.

Let us prove that using only the small deduction rules we can deduce from this identity that $X_f \geq 0$ in the logical sense.

We can assume that m is odd by multiplying both sides of the identity by ${X_f}^2$ if necessary. We can then multiply by $a{X_f}^{m-1}$ which is nonnegative as the product of a nonnegative element and a power of a nonnegative element and apply rule G5 to $a{X_f}^m$ and get that $a{X_f}^m$ is nonnegative. Now we can deduce using G4 that ${X_f}^m$ is nonnegative. Finally we get that X_f itself is nonnegative by multiplying by ${X_f}^{2r} = ({X_f}^r)^2$ (with $m + 2r$ a power of 3) and using the rule $a^3 \geq 0 \ \Rightarrow\ a \geq 0$ several times.

The other cases can be proved in the same way. □

As a consequence we prove that:

Theorem 2 *Given two sets of sign conditions C_1 and C_2, the following properties are equivalent.*

- *(1)* $\mathcal{S}(C_1)$ *and* $\mathcal{S}(C_2)$ *are quadratically homeomorphic,*
- *(2)* $\mathcal{Q}(C_1)$ *and* $\mathcal{Q}(C_2)$ *are isomorphic,*
- *(3)* $\mathcal{D}(C_1)$ *and* $\mathcal{D}(C_2)$ *are logically equivalent*
- *(4)* $\mathcal{R}(C_1)$ *and* $\mathcal{R}(C_2)$ *are isomorphic.*

Proof : The equivalence of (1) and (2) has already been proved (proposition 2).

The equivalence of (2) and (4) comes from the previous theorem 2.

The implication (3) $\Rightarrow$ (4) is clear.

We shall prove that (1) implies (3).

Call the coordinate variables in $\mathcal{S}(C_1)$ (resp. $\mathcal{S}(C_2)$) $(X_1, \ldots, X_n)$ (resp. $(Y_1, \ldots, Y_m)$). Consider the two quadratic homeomorphisms ϕ and ψ from $\mathcal{S}(C_1)$ to $\mathcal{S}(C_2)$. We can associate to ϕ an extension $\mathcal{D}(\phi) = \mathcal{D}(\phi_1, \ldots, \phi_m)$ of $\mathcal{D}(C_1)$, and to ψ an extension $\mathcal{D}(\psi) = \mathcal{D}(\psi_1, \ldots, \psi_n)$ of $\mathcal{D}(C_2)$. Assume w.l.o.g. that all variables in these two extensions are distinct.

It is clear from $\phi(\mathcal{S}(C_1)) \subset \mathcal{S}(C_2)$ that the variables corresponding to the coordinates ϕ_i of ϕ satissfy the defining inequalities of $\mathcal{S}(C_2)$ under the hypotheses in $\mathcal{D}(\phi)$. So we can prove these set-theoretic facts in an extension of $\mathcal{D}(\phi)$, with no variable in $\mathcal{D}(\psi)$. Then, we create in this extension the variables Y_i by putting $Y_i = \phi_i$. Then by the rules of equality, we deduce all the sign conditions in $\mathcal{D}(C_2)$. Finally, we can also add the sign conditions defining $\psi_1, \ldots, \psi_n$ (we find these sign conditions in $\mathcal{D}(\psi)$).

In this way, we get an extension $[V_1, \Gamma_1]$ of $\mathcal{D}(\phi_1, \ldots, \phi_m)$ 'containing' $\mathcal{D}(\psi_1, \ldots, \psi_n)$.

It remains to construct an extension of $[V_1, \Gamma_1]$ which is also an extension of $\mathcal{D}(\psi)$ (and, a fortiori, of $\mathcal{D}(C_2)$).

The fact that $\psi \circ \phi = Id_{\mathcal{S}(C_1)}$ means that we can (set theoretically and thus by small deduction rules) prove the equations $X_j = \psi_j$ from the system $[V_1, \Gamma_1]$. Make the corresponding extension.

Make also the extension corresponding to a proof by small deduction rules of the fact $\psi(\mathcal{S}(C_2)) \subset \mathcal{S}(C_1)$, using only the sign conditions of $\mathcal{D}(\psi)$.

Construct finally the extension corresponding to a proof by small deduction rules of the set theoretical fact $\phi \circ \psi = Id_{\mathcal{S}(C_2)}$, this means the equations $Y_i = \phi_i$, by using only the sign conditions of $\mathcal{D}(\psi)$.

In this way, we have constructed an extension $[V_2, \Gamma_2]$ of $\mathcal{D}(\phi)$, where all facts are proven twice, the first time from $\mathcal{D}(\phi)$ and the second one from $\mathcal{D}(\psi)$. So the extension $[V_2, \Gamma_2]$ is also an extension of $\mathcal{D}(C_2)$, since the situation is now perfectly symmetric in $\mathcal{S}(C_1)$ and $\mathcal{S}(C_2)$. □

Corollary 1 *If two sets of sign conditions* C_1 *and* C_2 *are such that* $\mathcal{D}(C_1)$ *and* $\mathcal{D}(C_2)$ *are logically equivalent,* $\mathcal{S}(C_1)$ *and* $\mathcal{S}(C_2)$ *have the same dimension and the same number of connected components.*

Proof: The assertion about dimension is clear by the preceeding theorem. The assertion about connected components is a consequence of the preceeding theorem and of Proposition 1 using classical properties of the real spectrum (see [1]). □

8 Remarks

1) It seems quite probable to us that the fact that twogiven basic semi-algebraic sets are quadratic-ring equivalent in the preceeding sense is undecidable, but do not know a proof of this assertion.

On the other hand, the fact that the ring of quadratic functions on a basic semi-algebraic set is isomorphic to the trivial ring is decidable: this is the case if and only if the semi-algebraic set is empty.

2) Other similar statements can be proved in similar situations by similar methods ([2]).

For example we can consider the two following rings

- the quotient of the ring $\mathbb{Z}[X_1, \ldots, X_n]$ by an ideal $\mathcal{I}$
- the quotient of the ring $\mathbb{Z}[X_1, \ldots, X_n]$ by the radical $\mathcal{J}$ of the ideal $\mathcal{I}$

and the sets of rules adapted to these situations (rules involving only equalities, without the radical rule in the first case).

References

[1] J. Bochnak, M. Coste, M.-F. Roy: Géométrie algébrique réelle. Springer-Verlag (1987).

[2] N. Mnev: Lecture in Rennes (june 1993).

[3] G. Stengle: A Nullstellensatz and Positivstellensatz in semi-algebraic geometry. Math. Ann. 207, 87-97 (1974).