Effective real Nullstellensatz and variants

HENRI LOMBARDI

Abstract. We give a constructive proof of the real Nullstellensatz. So we obtain, for every ordered field $\mathbf{K}$, a uniformly primitive recursive algorithm that computes, for the input "a system of generalized signs conditions (gsc) on polynomials of $\mathbf{K}[X_1, X_2, \ldots, X_n]$ impossible to satisfy in the real closure of $\mathbf{K}$, an algebraic identity that makes this impossibility evident. The main idea is to give an "algebraic identity version" of universal and existential axioms of the theory of real closed fields, and of the simplest deduction rules of this theory (as Modus Ponens). We apply this idea to the Hörmander algorithm, which is the conceptually simplest test for the impossibility of a gsc system in the real closure of an ordered field.

1) Introduction

This paper is the direct successor of [**LR**], where we develop the constructive elementary theory of ordered fields, in particular the constructive proof of the existence of the real closure of an ordered field $\mathbf{K}$ when one has a test for the sign of an element of $\mathbf{K}$.

Here, we give a constructive proof of the real Nullstellensatz and its variants.

The fundamental theorem from which one can deduce the real Nullstellensatz and its variants is the following (cf [**BCR**] theorem 4.4.2): let $\mathbf{R}$ be the real closure of an ordered field $\mathbf{K}$, $\mathbf{K}[\boldsymbol{X}]$ the ring $\mathbf{K}[X_1, X_2, \ldots, X_n]$, I a finitely generated ideal of $\mathbf{K}[\boldsymbol{X}]$, $\mathcal{P}$ a finitely generated cone of $\mathbf{K}[\boldsymbol{X}]$ (containing the positive elements of $\mathbf{K}$), $\mathcal{M}$ a finitely generated multiplicative monoid in $\mathbf{K}[\boldsymbol{X}]$; let us consider the semialgebraic subset S of $\mathbf{R}^n$ defined by:

$$S = \{x \in \mathbf{R}^n : f(x) = 0 \text{ for } f \in I,\ g(x) \geq 0 \text{ for } g \in \mathcal{P},\ h(x) \neq 0 \text{ for } h \in \mathcal{M}\};$$

then S is empty if and only if there exist $f \in I$, $g \in \mathcal{P}$, $h \in \mathcal{M}$ with $f + g + h^2 = 0$.

The general idea of our constructive proof is the following one. For an ordered field $\mathbf{K}$ there is an algorithm, conceptually very simple, for testing

if a system of *gsc* (generalized sign conditions) on polynomials in many variables is possible or impossible in the real closure of **K**. It is the Hörmander algorithm (cf. the proof of the Tarski-Seidenberg principle in [**BCR**] chap. 1), applied iteratively to diminish one at time the number of variables in the *gsc*. If one inspects the arguments on which the impossibility proof is based (in case of impossibility), one sees that there are essentially algebraic identities (corresponding to euclidean divisions), the mean value theorem and the existence of a root for a polynomial on an interval where it changes of sign. So the effective real ... -stellensatz will be obtained if one succeeds to "algebraicize" the basic arguments of the proof and the methods of deduction.

An important step has already been made with the algebraic version of the mean value theorem for polynomials (cf. [**LR**]). One can also verify that the purely universal axioms in the theory of ordered fields can be expressed in the form of *strong implications* (i.e. in an "algebraic identity" form, i.e. also in a "stellensatzised" form).

Another step consists in translating into a form of *constructions of strong implications* certain elementary methods of deduction (as: if $A \Longrightarrow B$ and $B \Longrightarrow C$ then $A \Longrightarrow C$). It is necessary moreover to find an "algebraic identity" version of existential axioms in the theory of real closed fields. This is made through the notion of *potential existence.*

Let us point out also that an important simplification in the construction of the real Nullstellensatz is obtained through an "algebraic identity" version of the Thom's lemma, given by what we call the mixed Taylor formulas.

Although we adopt a priori a constructive framework "à la Bishop", as developed in [**MRR**] concerning the theory of discrete fields, since we don't define the meaning of the words "effective" and "decidable", all the proofs can be read through glasses adapted to the philosophy or to the working framework of any particular mathematician.

If one accepts the "classical" point of view for example, the effective procedures in the initializing definitions can be considered as given by oracles. So, the proofs given provide a proof in the classical framework, and *without the axiom of choice*, of the real Nullstellensatz (and variants) in an arbitrary ordered field.

If one accepts the classical "recursive" theory point of view, the proofs given provide uniformly primitive recursive algorithms, "uniformly" understood in relation to an oracle giving the structure of the field of coefficients of the *gsc* system.

In Bishop's framework, we obtain the real Nullstellensatz and its variants for an arbitrary discrete ordered field.

In this paper we give the theorems, and some relevant proofs. Detailed proofs, and more constructive comments, can be found in [**Lom**].

2) Strong incompatibilities, evidence and implications

Strong incompatibilities (definitions).

We consider an ordered field $\mathbf{K}$, and $\boldsymbol{X}$ denotes a list of variables $X_1, X_2 \ldots, X_n$. We then denote by $\mathbf{K}[\boldsymbol{X}]$ the ring $\mathbf{K}[X_1, X_2, \ldots, X_n]$. If F is a finite subset of $\mathbf{K}[\boldsymbol{X}]$, we let F^{*2} be the set of squares of elements in F, $\mathcal{M}(F)$ be the *multiplicative monoid generated by* $F \cup \{1\}$, and we shall let $\mathcal{M}_2(F) := \mathcal{M}(F^{*2})$ and $\mathcal{M}_1(F)$ be the part of $\mathcal{M}(F)$ formed by products where each element of appears at most once.

$\mathcal{C}p(F)$ is the *positive cone generated by* F (the additive monoid generated by elements of type $p \cdot P \cdot Q^2$ where p is positive in $\mathbf{K}$, P is in $\mathcal{M}(F)$, Q is in $\mathbf{K}[\boldsymbol{X}]$).[1] We note that we may assume that P is in $\mathcal{M}_1(F)$.

Finally, let $I(F)$ be the ideal generated by F.

Definition: Consider 4 finite subsets of $\mathbf{K}[\boldsymbol{X}]$: $F_>, F_\geq, F_=, F_\neq$, containing polynomials for which we want respectively the sign conditions > 0, ≥ 0, $= 0$, $\neq 0$: we say that $\mathbf{F} = [F_>; F_\geq; F_=; F_\neq]$ is *strongly incompatible* in $\mathbf{K}$ if we have in $\mathbf{K}[\boldsymbol{X}]$ an equality of the following type:

$$(1) \quad S + P + Z = 0 \text{ with } S \in \mathcal{M}(F_> \cup F_\neq^{*2}), \quad P \in \mathcal{C}p(F_\geq \cup F_>),\ Z \in I(F_=)$$

Every strong incompatibility written in the form (1) can be rewritten as a strong incompatibility in the following form (2):

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

We can indeed multiply the first equality by a suitable element of $\mathcal{M}_1(F_>)$ to obtain each polynomial (in the first term S) with an even exponent.

It is clear that a strong incompatibility is a very strong form of incompatibility. In particular, it implies it is impossible to give the indicated signs to the polynomials, in any extension of $\mathbf{K}$. If one considers the real closure $\mathbf{R}$ of $\mathbf{K}$, the previous impossibility is testable by Hörmander's algorithm, for example. Moreover it is then constructively equivalent to its formulation in form of various implications: for example "$P = 0 \implies Q > 0$" is equivalent to "$P = 0, -Q \geq 0$ is impossible". We shall speak thus of *strong incompatibility*, *strong implication*, or *strong evidence*, meaning always implicitly a strong incompatibility.

---

[1] It would be more correct to denote $\mathcal{C}p(F, \mathbf{K}^+; \mathbf{K}[\boldsymbol{X}])$ in order to state: a) the positive elements of $\mathbf{K}$ are in the positive cone, and b) the positive cone is the one generated in $\mathbf{K}[\boldsymbol{X}]$.

Notation: We use the following notation for a strong implication:

$$^*([S_1 > 0, \ldots, S_i > 0, P_1 \geq 0, \ldots, P_j \geq 0, Z_1 = 0, \ldots, Z_k = 0, \\ N_1 \neq 0, \ldots, N_h \neq 0] \implies Q\,\tau\,0)^*$$

Note that if one takes $1 = 0$ in the right-hand side in the above strong implication, and applies the definitions, one obtains exactly the strong incompatibility for the left-hand side of the implication. Thus we can formulate any strong incompatibility in form of a strong implication.

Notation: Let us denote by the left-hand side in the preceding notation. Let us denote by $'$ a system of *gsc* : $Q_1\,\tau_1\,0, \ldots, Q_k\,\tau_k\,0$. We then write: $^*(\implies ')^*$ to mean

$$^*(\implies Q_1\,\tau_1\,0)^* \text{ and } \ldots \text{ and } ^*(\implies Q_k\,\tau_k\,0)^*$$

Remark: We could have an algebraic identity version for any quantifier free formula in the language of ordered rings with constants in **K**.

The Nullstellensatz and its variants.

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

Theorem. *Let* **K** *be an ordered field and* **R** *a real closed extension of* **K**. *The three following facts, concerning a gsc system on polynomials of* $\mathbf{K}[\boldsymbol{X}]$, *are equivalent:*

strong incompatibility in **K**
impossibility in **R**
impossibility in all the ordered extensions of **K**

This Nullstellensatz was first proved in 1974 ([**Ste**]). Less general variants were given by Krivine ([**Kri**]), Dubois ([**Du**]), Risler ([**Ris**]), Efroymson ([**Efr**]). All the proofs up to now used the axiom of choice. The first formulations were geometric: affirmation of the existence of an algebraic identity insuring that a given polynomial satisfied a given *gsc* on an algebraic or semialgebraic given set.

One speaks of *Nullstellensatz* when one considers the condition for a polynomial to belong to the ideal of a given algebraic variety (i.e. an implication: "equalities to zero imply an equality to zero"); of weak *Nullstellensatz* when one considers the condition for a given algebraic variety to be empty (i.e. "equalities to zero are incompatible"), of *Positivestellensatz* when one considers the condition for a polynomial to be strictly positive on a given semi-algebraic variety (i.e. the general form of the incompatibility between *gsc*, seen as an implication, the conclusion of which is a strictly positive sign), of *Nichtnegativestellensatz* when one considers the condition for a polynomial to be nonnegative on a given semi-algebraic variety (i.e. the general form of the incompatibility between *gsc* seen as an implication the conclusion of which is a nonnegative sign). Let us for example give the general Positivestellensatz.

Theorem (Positivestellensatz). *Let* $\mathbf{K}$ *be an ordered field and* $\mathbf{R}$ *a real closed extension of* $\mathbf{K}$. *Let* A *be the semi algebraic set in* $\mathbf{R}^n$ *defined as:*

$$A = \{x \in \mathbf{R}^n : S_1(x) > 0, \ldots, S_i(x) > 0, P_1(x) \geq 0, \ldots, P_j(x) \geq 0, \\ Z_1(x) = 0, \ldots, Z_k(x) = 0, N_1(x) \neq 0, \ldots, N_h(x) \neq 0\}$$

Let Q *be a polynomial in* $\mathbf{K}[\boldsymbol{X}]$. *Then* Q *is positive at each point of* A *if and only if there is algebraic identity:* $Q \cdot P = S \cdot N^2 + R + Z$ *where:*
P *and* R *are in the positive cone of* $\mathbf{K}[\boldsymbol{X}]$*:* $\mathcal{C}p(S_1, \ldots, S_i, P_1, \ldots, P_j)$*;*
Z *is in the ideal of* $\mathbf{K}[\boldsymbol{X}]$*:* $I(Z_1, \ldots, Z_k)$*;*
S *is in the monoid* $\mathcal{M}(S_1, \ldots, S_i)$ *and*
N *is in the monoid* $\mathcal{M}(N_1, \ldots, N_h)$

Some trivial strong implications.

Proposition 2. *We have the following strong implications.*

$$\begin{aligned}
{}^*([U > 0, V > 0] &\implies [U + V > 0, U \cdot V > 0])^* \\
{}^*([U + V \geq 0, U \cdot V > 0] &\implies [U > 0, V > 0])^* \\
{}^*([U > 0, V \geq 0] &\implies U + V > 0)^* \\
{}^*([U \geq 0, U \cdot V > 0] &\implies V > 0)^* \\
{}^*(U \neq 0 &\implies U^2 > 0)^* \\
{}^*(U^2 > 0 &\implies U \neq 0)^* \\
{}^*(U = 0 &\implies U \cdot V = 0)^* \\
{}^*(U = V &\implies P(\boldsymbol{X}, U) = P(\boldsymbol{X}, V))^* \\
{}^*([U = V, V \,\tau\, 0] &\implies U \,\tau\, 0)^* \quad (\cdot \,\tau\, 0 \ \textit{is a} \ \textit{gsc}) \\
{}^*([W = 0, U = V + W \cdot Z] &\implies U = V)^* \\
{}^*([W = 0, U = V + W \cdot Z, V \,\tau\, 0] &\implies U \,\tau\, 0)^* \\
{}^*([\,] &\implies [1 + U^2 > U, 1 + U^2 > -U])^*
\end{aligned}$$

One proof: Let us prove the last but one strong implication when τ is $>$. We have to give a strong incompatibility between the following *gsc*:

$$W = 0, V + W \cdot Z - U = 0, V > 0, -U \geq 0$$

we can take:

$$V^2 + ((-U) \cdot V) + ((Z \cdot V) \cdot W + (-V) \cdot (V + W \cdot Z - U)) = 0$$

with

$$V^2 \in \mathcal{M}(F >^{*2} \cup F_{\neq}^{*2}), (-U) \cdot V \in \mathcal{C}p(F_{\geq} \cup F_{>}), \\ (Z \cdot V) \cdot W + (-V) \cdot (V + W \cdot Z - U) \in I(F_{=})$$

Q. E. D.

Proposition 3 (substitution principle). *If, in a strong implication, one replaces each occurrence of one variable by a fixed polynomial, one obtains again a strong implication.*

The proof is trivial. So, the strong implications of proposition 2, stated for variables U and V, are also valid for polynomials $U(\boldsymbol{X})$ and $V(\boldsymbol{X})$.

Constructions of strong implications.

Definition 4: We speak of construction of a strong implication from other strong implications when we have an algorithm that constructs the first from the others. So it is a logical implication in the constructive meaning. We denote it by the symbol: $\underset{\text{cons}}{\vdash}$ For example we give explicitly (theorem 8) the construction which proves:

$$[^*(\implies ')^* \text{ and } ^*(' \implies '')^*] \underset{\text{cons}}{\vdash} ^*(\implies '')^*$$

As another example, we can state the principle of substitution in the form:

$$^*((\boldsymbol{X}, W) \implies '(\boldsymbol{X}, W))^* \underset{\text{cons}}{\vdash} ^*((\boldsymbol{X}, P(\boldsymbol{X})) \implies '(\boldsymbol{X}, P(\boldsymbol{X})))^*$$

Lemma 5. *Let be a gsc system on polynomials of* $\mathbf{K}[\boldsymbol{X}]$, Q *an element of* $\mathbf{K}[\boldsymbol{X}]$. *Then each strong implication of the form* $^*(\implies Q\,\tau\,0)^*$ *(where* τ *is* $=, <$ *or* $>$*) can be interpreted as any "weaker" strong implication* $^*(\implies Q\,\tau'\,0)^*$. *For example, one has*

$$^*(\implies Q > 0)^* \underset{\text{cons}}{\vdash} ^*(\implies Q \geq 0)^*$$

Proposition 6. *Let be a gsc system on polynomials of* $\mathbf{K}[\boldsymbol{X}], Q$ *be an element of* $\mathbf{K}[\boldsymbol{X}]$, *then:*

$$[^*(\implies Q \leq 0)^* \text{ and } ^*(\implies Q \geq 0)^*] \underset{\text{cons}}{\vdash} ^*(\implies Q = 0)^*.$$

Likewise:

$$[^*(\implies Q \leq 0)^* \text{ and } ^*(\implies Q \neq 0)^*] \underset{\text{cons}}{\vdash} ^*(\implies Q < 0)^*$$

and

$$[^*(\implies Q = 0)^* \text{ and } ^*(\implies Q \neq 0)^*] \underset{\text{cons}}{\vdash} ^*(\implies 1 = 0)^*.$$

Proof: Let us give the first construction. Call $F_>$, $F_\geq$, $F_=$, $F_\neq$ the 4 finite subsets of $\mathbf{K}[\boldsymbol{X}]$ containing polynomials for which we have respectively the sign conditions > 0, ≥ 0, $= 0$, $\neq 0$ in the hypothesis .

The hypothesis $^*(\implies Q \leq 0)^*$ can be rewritten in the form $^*([, Q > 0] \implies 1 = 0)^*$ and means that we have an equality:

$$S + P + Z = 0$$

with

$$S \in \mathcal{M}(F_>^{*2} \cup F_\neq^{*2} \cup \{Q^2\}),\ P \in \mathcal{C}p(F_\geq \cup F_> \cup \{Q\}),\ Z \in I(F_=)$$

i.e. also:

$$Q^{2n} \cdot S_1 + Q \cdot P_1 + R_1 + Z_1 = 0$$

with

$$S_1 \in \mathcal{M}(F_>^{*2} \cup F_{\neq}^{*2}),\ P_1, R_1 \in \mathcal{C}p(F_{\geq} \cup F_>),\ Z_1 \in I(F_=)$$

Likewise the hypothesis $^*(\implies Q \geq 0)^*$ means we have an equality:

$$Q^{2m} \cdot S_2 - Q \cdot P_2 + R_2 + Z_2 = 0$$

with

$$S_2 \in \mathcal{M}(F_>^{*2} \cup F_{\neq}^{*2}),\ P_2, R_2 \in \mathcal{C}p(F_{\geq} \cup F_>),\ Z_2 \in I(F_=)$$

We rewrite the two equalities:

$$-Q \cdot P_1 = Q^{2n} \cdot S_1 + R_1 + Z1,\ Q \cdot P_2 = Q^{2m} \cdot S_2 + R_2 + Z_2$$

and we multiply: so

$$-Q^2 \cdot P_1 \cdot P_2 = Q^{2n+2m} \cdot S_1 \cdot S_2 + [Q^{2n} \cdot S_1 \cdot R_2 + Q^{2m} \cdot S_2 \cdot R_1 + R_1 \cdot R_2] + W$$

with $W \in I(F_=)$, so $Q^{2n+2m} \cdot S_1 \cdot S_2 + V + W = 0$ with:

$$S_1 \cdot S_2 \in \mathcal{M}(F_>^{*2} \cup F_{\neq}^{*2}),\ V \in \mathcal{C}p(F_{\geq} \cup F_>),\ W \in I(F_=)$$

and this is precisely a strong implication $^*(\implies Q = 0)^*$. Q. E. D.

The following theorem is a corollary of proposition 6.

Theorem 7 (proof by cases, according to the sign of a polynomial). *To show that is strongly incompatible, it is sufficient to construct a strong incompatibility for each of the 3 cases:* $Q > 0$, $Q < 0$, $Q = 0$.

Theorem 8 (transitivity of strong implications). *Let , ′, ″ be three gsc systems on polynomials of* $\mathbf{K}[\boldsymbol{X}]$.

Then: $[^*(\implies ')^*$ *and* $^*([,'] \implies '')^*] \underset{\text{cons}}{\vdash} {}^*(\implies '')^*$

Proof: It is sufficient to remove one after the other the hypothesis of $'$ in:

$$^*([,'] \implies '')^*.$$

Thus one may assume that $'$ contains a unique hypothesis $Q\,\tau\,0$.

It is thus sufficient to show that if one has two strong implications $^*(\implies Q\,\tau\,0)^*$, and $^*([, Q\,\tau\,0, A] \implies 1 = 0)^*$, then one can construct the strong implication: $^*([, A] \implies 1 = 0)^*$ (where A is a *gsc* on a polynomial). But this can be done by cases according to the sign of Q. Q. E. D.

Combining the transitivity of the strong implications and trivial strong implications, one obtains many corollaries, for example:

Corollary (example).

$$^*(\implies [P \cdot Q > 0, Q \geq 0])^* \underset{\text{cons}}{\vdash} {}^*(\implies P > 0)^*$$

Mixed Taylor formulas (strong evidence of Thom's lemma)

Let us at first recall Thom's lemma and the coding "à la Thom":

Thom's lemma. *Let* $\mathbf{R}$ *be a real closed field,* $P \in \mathbf{R}[T]$*, of degree* d*,* $\sigma_1, \sigma_2, \ldots, \sigma_d$ *a list of* $>$ *or* $<$*. The set*

$$\{t \in \mathbf{R} : P'(t)\,\sigma_1\,0, \ldots, P(i)(t)\,\sigma_i\,0, \ldots, P^{(d)}(t)\,\sigma_d\,0\}$$

is either empty or an open interval. In the latter case, its closure is obtained by weakening the signs σ_i*. In the same way, the set:* $\{\tau \in \mathbf{R} : P(t) = 0,$ $P'(t)\,\sigma_1\,0, \ldots, P^{(i)}(t)\,\sigma_i\,0, \ldots, P^{(d)}(U)\,\sigma_d\,0\}$ *is either empty or reduces to one point.*

Definition of the "coding à la Thom".

Let $\mathbf{K}$ be an ordered field, $\mathbf{R}$ its real closure. An element ζ of $\mathbf{R}$ is said to be *coded à la Thom* (in $\mathbf{K}$) if it is given as a root of a polynomial P of $\mathbf{K}[X]$, specifying the strict[2] signs of $P'(\zeta), P''(\zeta), etc\ldots$

An open unbounded interval of $\mathbf{R}$ is said to be *coded à la Thom* (in $\mathbf{K}$) if it is given as the set of elements ξ which give specified strict signs to a list of polynomials $[P, P', P''$, etc... $]$, the finite bound a of the interval being obtained for $P(a) = 0$.

A bounded open interval of $\mathbf{R}$ is said to be *coded à la Thom* (in $\mathbf{K}$) if it is given as the set of elements ξ which give specified strict signs to two lists of polynomials $[P, P', P''$, etc... $]$ and $[Q, Q', Q''$, etc...$]$, the bounds α and β of the interval being obtained for $P(\alpha) = 0$ and $Q(\beta) = 0$.

NB: Each point of $\mathbf{R}$, but only few open intervals of $\mathbf{R}$, can be coded à la Thom in $\mathbf{K}$. The important fact is that the minimal open intervals of Hörmander tableaux (cf. §4) are naturally coded à la Thom.

One considers now two variables U and V and one lets $\Delta : U - V$. One considers a polynomial P with coefficients in an ordered field $\mathbf{K}$ or more generally in a commutative ring A which is a -algebra.

If $\deg(P) \leq 3$, one has the following 4 mixed Taylor formulas:

$$\begin{aligned}
P(U) - P(V) =& \Delta \cdot P'(V) + (1/2) \cdot \Delta^2 \cdot P''(V) + (1/6) \cdot \Delta^3 \cdot P^{(3)} \\
P(U) - P(V) =& \Delta \cdot P'(V) + (1/2) \cdot \Delta^2 \cdot P''(U) - (1/3) \cdot \Delta^3 \cdot P^{(3)} \\
P(U) - P(V) =& \Delta \cdot P'(U) - (1/2) \cdot \Delta^2 \cdot P''(V) - (1/3) \cdot \Delta^3 \cdot P^{(3)} \\
P(U) - P(V) =& \Delta \cdot P'(U) - (1/2) \cdot \Delta^2 \cdot P''(U) + (1/6) \cdot \Delta^3 \cdot P^{(3)}
\end{aligned}$$

Assume now that U and V give the same strict sign σ to P', and the same strict sign σ'' to P''. Then, if we give a sign to Δ and $P^{(3)}$, one of the 4

[2]We say a sign to be strict when it is $+1$ or -1.

mixed Taylor formula is strong evidence showing that $P(U) - P(V)$ and $\Delta \cdot P'(U)$ have the same sign. For example, if $\sigma = +1, \sigma'' = -1$ and if $\Delta > 0, P^{(3)} < 0$, the third mixed Taylor formula can be reread:

$$P(U) - P(V) = \Delta \cdot (P'(U) - (1/3) \cdot \Delta^2 \cdot P^{(3)}) - (1/2) \cdot \Delta^2 \cdot P''(V)$$

Conversely these mixed Taylor formulas provide strong evidence in order to obtain the sign of Δ from the sign of $P(U) - P(V)$. In particular, they provide strong evidence that two roots of P coded à la Thom by the same sign sequence are equal. If $\deg(P) \leq 4$, one has the following 8 mixed Taylor formulas:

$$P(U) - P(V) =$$
$$\Delta \cdot P'(V) + (1/2) \cdot \Delta^2 \cdot P''(V) + (1/6) \cdot \Delta^3 \cdot P^{(3)}(V) + (1/24) \cdot \Delta^4 \cdot P^{(4)}$$
$$P(U) - P(V) =$$
$$\Delta \cdot P'(V) + (1/2) \cdot \Delta^2 \cdot P''(V) + (1/6) \cdot \Delta^3 \cdot P^{(3)}(U) - (1/8) \cdot \Delta^4 \cdot P^{(4)}$$
$$P(U) - P(V) =$$
$$\Delta \cdot P'(V) + (1/2) \cdot \Delta^2 \cdot P''(U) - (1/3) \cdot \Delta^3 \cdot P^{(3)}(V) - (5/24) \cdot \Delta^4 \cdot P^{(4)}$$
$$P(U) - P(V) =$$
$$\Delta \cdot P'(V) + (1/2) \cdot \Delta^2 \cdot P''(U) - (1/3) \cdot \Delta^3 \cdot P^{(3)}(U) + (1/8) \cdot \Delta^4 \cdot P^{(4)}$$
$$P(U) - P(V) =$$
$$\Delta \cdot P'(U) - (1/2) \cdot \Delta^2 \cdot P''(V) - (1/3) \cdot \Delta^3 \cdot P^{(3)}(V) - (1/8) \cdot \Delta^4 \cdot P^{(4)}$$
$$P(U) - P(V) =$$
$$\Delta \cdot P'(U) - (1/2) \cdot \Delta^2 \cdot P''(V) - (1/3) \cdot \Delta^3 \cdot P^{(3)}(U) + (5/24) \cdot \Delta^4 \cdot P^{(4)}$$
$$P(U) - P(V) =$$
$$\Delta \cdot P'(U) - (1/2) \cdot \Delta^2 \cdot P''(U) + (1/6) \cdot \Delta^3 \cdot P^{(3)}(V) + (1/8) \cdot \Delta^4 \cdot P^{(4)}$$
$$P(U) - P(V) =$$
$$\Delta \cdot P'(U) - (1/2) \cdot \Delta^2 \cdot P''(U) + (1/6) \cdot \Delta^3 \cdot P^{(3)}(U) - (1/24) \cdot \Delta^4 \cdot P^{(4)}$$

As all the possible sign combinations appear, one obtains: if U and V give the same sign sequence to the successive derivatives of a polynomial P of degree ≤ 4, then one has strong evidence that $P(U) - P(V)$ and $(U - V) \cdot P'(U)$ have the same sign. Likewise, if U and V don't give the same sign sequence to P and its successive derivatives (P of degree ≤ 4), one of the mixed Taylor formulas for P, P', P'', or $P^{(3)}$ provides strong evidence for the sign of Δ from the signs of $P^{(i)}(V)$ and $P^{(i)}(U)(i = 0, \ldots, 4)$.

Theorem 9 (mixed Taylor formula). *For each degree d, there are 2^{d-1} mixed Taylor formulas and all the possible sign combinations do appear.*

Proof: Linear algebra shows there is a mixed Taylor formula for each choice ($i \mapsto P^{(i)}(U)$ or $P^{(i)}(V), i = 1, \ldots, d-1$). The difficult point is

showing that all the possible sign combinations do appear. From the algebraic mean value theorem for polynomials, we can obtain the following result: if we choose $P^{(i)}(V)$ the signs of the coefficients of $P^{(i)}$ and $P^{(i+1)}$ are equal, and if we choose $P^{(i)}(U)$ the signs of the coefficients of $P^{(i)}$ and $P^{(i+1)}$ are opposite. Q. E. D.

Theorem 10 (strong evidence of Thom's lemma). *Let $P \in \mathbf{K}[\boldsymbol{X}][T]$, of degree d in T, $\sigma_1, \sigma_2, \ldots, \sigma_d$ a list of $>$ or $<$. Denote by $(\boldsymbol{X}, U)$ the gsc system: $P'(\boldsymbol{X}, U)\,\sigma_1\,0, \ldots, P^{(i)}(\boldsymbol{X}, U)\,\sigma_i\,0, \ldots, P^{(d)}(\boldsymbol{X}, U)\,\sigma_d\,0$, (derivatives with respect to T). Write (U) for $(\boldsymbol{X}, U)$, $P(U)$ for $P(\boldsymbol{X}, U)$ and so on: One has then the following strong evidence:*

$$(1) \qquad {}^*([(U),(V),P(U)=P(V)] \implies U=V)^*$$

$$(2) \quad {}^*([(U),(V)] \implies \operatorname{sign}((U-V)\cdot P'(U)) = \operatorname{sign}(P(U)-P(V)))^*$$

$$(3) \qquad {}^*([(U),(V),(W-U)\cdot(W-V)\leq 0] \implies (W))^*$$

$$(4) \qquad {}^*([(U),(V),P^{(i)}(W)\not\sigma_i\,0] \implies (W-U)\cdot(W-V)>0)^* \quad (i=1,\ldots,d)$$

Let $'$ be the gsc system obtained from by weakening all the sign conditions except those referring to $P^{(d)}$. One has then the following strong evidence:

$$(5) \qquad {}^*([{}'(U),{}'(V),U<W<V] \implies (W))^*$$

Note that (1) is one of the six strong implications written in the abbreviated form (2), and that the d strong incompatibities in (4) are the same as the ones in (3).

Proof: (1) and (2) are obtained from mixed Taylor formulas as has been explained for degree 3. The d strong implications (3):

$${}^*([(U),(V),(W-U)\cdot(W-V)>0] \implies P^{(i)}(W)\,\sigma_i\,0)^*(i=1,\ldots,d)$$

are proved by steps, for i decreasing from d to 1, using at step $P^{(i)}$ a mixed Taylor formula for $P^{(i)}$, and applying transitivity for strong implications.

(5) is proved in the same way. Q. E. D.

Note that theorem 10 doesn't capture entirely Thom's lemma in form of strong evidence: statements concerning the bounds of the interval are missing. This gap is fulfilled in the section on the Hörmander tableaux, and requires the notion of potential existence.

3) Potential existence

Notations and definitions.

A strong implication $^*(\ \Longrightarrow\ ')^*$ is a strong form (in an algebraic identity form) for the corresponding *universal* implication: $\forall \boldsymbol{X}\ (\ \Longrightarrow\ ')$. But the theory of real closed fields has axioms which are not purely universal. So, we require a "stellensatzised" form for statements of the following type:

$$\forall \boldsymbol{X}\ \exists T\ (\boldsymbol{X}, T).$$

We should like to speak of potential existence when a *gsc* system is not strongly incompatible.

In fact, we want a little more. The non impossibility of the equation $P(\boldsymbol{X}) = T^2$ taken in isolation is not the same thing as the non impossibility of the equation $P(\boldsymbol{X})^2 = T^4$. Indeed, in the second case, contrarily to the first, whatever hypothesis is made on $\boldsymbol{X}$, adding the equation cannot introduce a contradiction. This distinction is translated in logic by an alternation of quantifiers:

$$\forall \boldsymbol{X}\ \exists T\ P(\boldsymbol{X})^2 = T^4.$$

A "direct translation" of this alternation in terms of strong implication would seem to be: for each not strongly incompatible specification à la Thom of the X_i, the system $(\boldsymbol{X}, T)$ is not strongly incompatible. But, in a general proof, a specification of the X_i may depend on values of parameters Y_j. So we are led to the following definition.

Definition 11: Let ${}_1(\boldsymbol{X})$ be a *gsc* system on polynomials of $\mathbf{K}[\boldsymbol{X}]$ and ${}_2(\boldsymbol{X}, \boldsymbol{T})$ a *gsc* system on polynomials of $\mathbf{K}[\boldsymbol{X}, T_1, T_2, \ldots, T_m] = \mathbf{K}[\boldsymbol{X}, \boldsymbol{T}]$. We shall say that *the hypothesis* ${}_1(\boldsymbol{X})$ *allow the existence of* T_i *satisfying* ${}_2(\boldsymbol{X}, \boldsymbol{T})$ when, for all *gsc* systems $(\boldsymbol{X}, \boldsymbol{Y})$ on polynomials of $\mathbf{K}[\boldsymbol{X}, \boldsymbol{Y}]$, one has the construction of the strong implication:

$$^*([{}_2(\boldsymbol{X}, \boldsymbol{T}), (\boldsymbol{X}, \boldsymbol{Y})]\ \Longrightarrow\ 1 = 0)^* \underset{\text{cons}}{\vdash} {}^*([{}_1(\boldsymbol{X}), (\boldsymbol{X}, \boldsymbol{Y})]\ \Longrightarrow\ 1 = 0)^*.$$

We shall speak also of the potential existence of T_i satisfying ${}_2$ under the hypothesis ${}_1$.

NB: The condition on is that no variable $T_1, T_2, \ldots, T_m$ is in it; but this is possible for other variables, distinct from $X_1, X_2, \ldots, X_n$, hence the $\mathbf{K}[\boldsymbol{X}, \boldsymbol{Y}]$.

Notation: We shall denote this potential existence by:

$$^*({}_1\ \Longrightarrow\ \exists \boldsymbol{T}\ {}_2)^*.$$

We can specify the variables in the *gsc* systems, we then write:

$$^*({}_1(\boldsymbol{X}) \implies \exists \boldsymbol{T}\ {}_2(\boldsymbol{X}, \boldsymbol{T}))^*.$$

When the system ${}_1$ is empty, we shall use the notation: $^*(\exists \boldsymbol{T}\ {}_2)^*$.

For example, we shall show:

$$^*(P(\boldsymbol{X}, U) \cdot P(\boldsymbol{X}, V) < 0 \implies \exists W P(\boldsymbol{X}, W) = 0)^*$$

Note that the substitution principle stated in the preceding paragraph can be rewritten in the form:

$$^*((\boldsymbol{X}, P(\boldsymbol{X})) \implies \exists W\ (\boldsymbol{X}, W))^*$$

Remarks:

1) At first, we insist on the constructive reading of the above definition: the construction of the strong implication is to be provided by a uniform algorithmic process.
2) The notation is to be read as a unit (contrarily to the notation concerning constructions of strong implications).
3) If **L** is a given ordered extension of **K** there is not any obvious a priori relation between a statement $^*({}_1(\boldsymbol{X}) \implies \exists \boldsymbol{T}\ {}_2(\boldsymbol{X}, \boldsymbol{T}))^*$ read in **K** and the same statement read in **L**. In fact, after the Nullstellensatz' proof, it is clear that the two statements are equivalent to the statement: $\forall \boldsymbol{x}({}_1(\boldsymbol{x}) \implies \exists \boldsymbol{t}\ {}_2(\boldsymbol{x}, \boldsymbol{t})\ )$ read in the real closure of **K**.

Some rules of manipulation for potential existence statements.

Among the following rules, only the substitution rule is not immediate.

Lemma 12. *Any potential existence* $^*({}_1(\boldsymbol{X}) \implies \exists \boldsymbol{T}\ {}_2(\boldsymbol{X}, \boldsymbol{T}))^*$ *remains true:*

a) if one weakens the conclusion,
b) if one strengthens the hypothesis, or
c) if one suppresses behind $\exists$ *some variables that are not in* ${}_2(\boldsymbol{X}, \boldsymbol{T})$.

Proposition 13. (simultaneous reinforcement of the hypothesis and the conclusion).

If

$$^*({}_1(\boldsymbol{X}) \implies \exists \boldsymbol{T}\ {}_2(\boldsymbol{X}, \boldsymbol{T}))^*$$

then

$$^*([{}_1(\boldsymbol{X}), {}_3(\boldsymbol{X})] \implies \exists \boldsymbol{T}\ [{}_2(\boldsymbol{X}, \boldsymbol{T}), {}_3(\boldsymbol{X})])^*$$

(recall of the hypothesis in the conclusion).

If

$$^*({}_1(\boldsymbol{X}) \implies \exists \boldsymbol{T}\ {}_2(\boldsymbol{X}, \boldsymbol{T}))^*$$

then

$$^*(_1(\boldsymbol{X}) \implies \exists \boldsymbol{T}\, [_2(\boldsymbol{X}, \boldsymbol{T}), _1(\boldsymbol{X})])^*$$

Proposition 14 (potential existence as a generalization of strong implication). *Assume that the gsc systems* $_1$ *and* $_2$ *act only on the variables* $\boldsymbol{X}$. *Then* $^*(_1(\boldsymbol{X}) \implies \exists \boldsymbol{T}\, _2(\boldsymbol{X}))^*$ *if and only if* $^*(_1(\boldsymbol{X}) \implies _2(\boldsymbol{X}))^*$.

Proposition 15 (rule of proof by cases). *Let* Q *be a polynomial of* $\mathbf{K}[\boldsymbol{X}]$. *In order to settle a potential existence:* $^*(_1(\boldsymbol{X}) \implies \exists \boldsymbol{T}\, _2(\boldsymbol{X}, \boldsymbol{T}))^*$ *it is sufficient to prove the potential existence*

$$^*([_1(\boldsymbol{X}), Q\, \sigma\, 0] \implies \exists \boldsymbol{T}\, _2(\boldsymbol{X}, \boldsymbol{T}))^*$$

for the three σ *possible.*

Proposition 16 (existence implies potential existence). *Let*

$$P_1, P_2, \ldots, P_m \in \mathbf{K}[\boldsymbol{X}]$$

and let us denote $\mathbf{P}(\boldsymbol{X})$ *for* $P_1(\boldsymbol{X}), \ldots, P_m(\boldsymbol{X})$.

If $^*(_1(\boldsymbol{X}) \implies _2(\boldsymbol{X}, \mathbf{P}(\boldsymbol{X})))^*$ *then* $^*(_1(\boldsymbol{X}) \implies \exists \boldsymbol{T}\, _2(\boldsymbol{X}, \boldsymbol{T}))^*$

Theorem 17 (transitivity of potential existence). *One considers variables* $X_1,\ X_2, \ldots, X_n,\ T_1,\ T_2, \ldots, T_m,\ U_1,\ U_2, \ldots, U_k$ *and gsc systems* $_1(\boldsymbol{X})$, $_2(\boldsymbol{X}, \boldsymbol{T})$ *and* $_3(\boldsymbol{X}, \boldsymbol{T}, \boldsymbol{U})$. *If one has*

$$^*(_1(\boldsymbol{X}) \implies \exists \boldsymbol{T}\, _2(\boldsymbol{X}, \boldsymbol{T}))^*$$

and

$$^*([_1(\boldsymbol{X}), _2(\boldsymbol{X}, \boldsymbol{T})] \implies \exists \boldsymbol{U}\, _3(\boldsymbol{X}, \boldsymbol{T}, \boldsymbol{U}))^*$$

then one has also

$$^*(_1(\boldsymbol{X}) \implies \exists \boldsymbol{T}, \boldsymbol{U}\, [_1(\boldsymbol{X}),\ _2(\boldsymbol{X}, \boldsymbol{T}),\ _3(\boldsymbol{X}, \boldsymbol{T}, \boldsymbol{U})])^*$$

Remark 4: Combining the preceding theorem and proposition 14, one obtains some variants. A strong implication followed by a potential existence gives a potential existence. A potential existence followed by a strong implication gives a potential existence. Note also that we may see proposition 14 as a particular case of lemma 12 c).

Theorem 18 (substitution principle in potential existence). *One considers variables* $X_1, X_2, \ldots, X_n, Z_1, Z_2, \ldots, Z_k, T_1, T_2, \ldots, T_m$, *and polynomials* $P_1, P_2, \ldots, P_n$ *of* $\mathbf{K}[\boldsymbol{Z}]$. *Let us write* $\boldsymbol{P}(\boldsymbol{Z})$ *for* $P_1(\boldsymbol{Z}), \ldots, P_n(\boldsymbol{Z})$.

If one has

(a) $$^*(_1(\boldsymbol{X}) \implies \exists \boldsymbol{T}\, _2(\boldsymbol{X}, \boldsymbol{T}))^*$$

then one has also

(b) $$^*({}_1(\boldsymbol{P}(Z)) \implies \exists\ \boldsymbol{T}_2(\boldsymbol{P}(\boldsymbol{Z}), \boldsymbol{T}))^*$$

Proof: Assume

(1) $$^*([{}_2(\boldsymbol{P}(\boldsymbol{Z}), \boldsymbol{T}), (\boldsymbol{Z}, \boldsymbol{Y})] \implies 1 = 0)^*$$

We want to construct

(2) $$^*([{}_1(\boldsymbol{P}(\boldsymbol{Z})), (\boldsymbol{Z}, \boldsymbol{Y})] \implies 1 = 0)^*$$

But:

(3) $$^*([{}_2(\boldsymbol{X}, \boldsymbol{T}), (\boldsymbol{Z}, \boldsymbol{Y}), \boldsymbol{X} = \boldsymbol{P}(\boldsymbol{Z})] \implies [{}_2(\boldsymbol{P}(\boldsymbol{Z}), \boldsymbol{T}), (\boldsymbol{Z}, \boldsymbol{Y})])^*$$

Transitivity on (1) and (3) gives:

(4) $$^*([{}_2(\boldsymbol{X}, \boldsymbol{T}), (\boldsymbol{Z}, \boldsymbol{Y}), \boldsymbol{X} = \boldsymbol{P}(\boldsymbol{Z})] \implies 1 = 0)^*$$

The definition of potential existence gives:

(5) $$^*([{}_1(\boldsymbol{X}), (\boldsymbol{Z}, \boldsymbol{Y}), \boldsymbol{X} = \boldsymbol{P}(\boldsymbol{Z})] \implies 1 = 0)^*$$

We have also (trivial strong implications):

(6) $$^*([{}_1(\boldsymbol{P}(\boldsymbol{Z})), (\boldsymbol{Z}, \boldsymbol{Y}), \boldsymbol{X} = \boldsymbol{P}(\boldsymbol{Z})] \implies [{}_1(\boldsymbol{X}), (\boldsymbol{Z}, \boldsymbol{Y}), \boldsymbol{X} = \boldsymbol{P}(\boldsymbol{Z})])^*$$

Transitivity on (5) and (6) gives:

(7) $$^*([{}_1(\boldsymbol{P}(\boldsymbol{Z})), (\boldsymbol{Z}, \boldsymbol{Y}), \boldsymbol{X} = \boldsymbol{P}(\boldsymbol{Z})] \implies 1 = 0)^*$$

If we substitute $\boldsymbol{P}(\boldsymbol{Z})$ for $\boldsymbol{X}$ in (7), we obtain (2) Q. E. D.

Remark 5: The proofs of potential existence can generally be given directly in the form (b). Theorem 18 merely allows one to see more clearly the structure of theorems stating potential existence.

Remark 6: If one applies theorem 18 once again, one can substitute some X_j for some Z_i. One sees thus that the hypothesis that the X_j and the Z_i are distinct is in fact useless.

Fundamental potential existence

Theorem 19 (authorization to add the square root of a positive element).

$$^*(U \geq 0 \implies \exists T\ U = T^2)^*$$

Theorem 20. *(authorization to add the inverse of a nonzero element):*

$$^*(U \neq 0 \implies \exists T\ 1 = U \cdot T)^*$$

Proof: Assume without loss of generality that U is the variable X_n. Consider a *gsc* system $(\boldsymbol{X})$. Notation is as in the proof of proposition 6.

Let us write $\mathcal{C}p', I'$ when we consider the positive cone or the ideal generated in the polynomial ring with the extra variable T: $\mathbf{K}[\boldsymbol{X}, T] = \mathbf{K}[X_1, X_2, \ldots, X_n, T]$.

We want to give the construction:

$$^*([, 1 - U \cdot T = 0] \implies 1 = 0)^* \underset{\text{cons}}{\vdash} {}^*([, U \neq 0] \implies 1 = 0))^*.$$

The hypothesis is an algebraic identity:

$$S_1(\boldsymbol{X}) + P_1(\boldsymbol{X}, T) + (1 - U \cdot T) \cdot Y_1(\boldsymbol{X}, T) + Z_1(\boldsymbol{X}, T) = 0$$

where

$$S_1 \in \mathcal{M}(F_>^{*2} \cup F_{\neq}^{*2}), P_1 \in \mathcal{C}p'(F_{\geq} \cup F_>), Z_1 \in I'(F_=).$$

More precisely:

$$S_1(\boldsymbol{X}) + \sum_{i=1}^{h} Q_i(\boldsymbol{X}) \cdot V_i^2(\boldsymbol{X}, T)) + (1 - U \cdot T) \cdot Y_1(\boldsymbol{X}, T) + \sum_{j=1}^{r} N_j(\boldsymbol{X}) \cdot W_j(\boldsymbol{X}, T)) = 0$$

where $Q_i(\boldsymbol{X}) \in \mathcal{C}p(F_{\geq} \cup F_>)$ and $N_j(\boldsymbol{X}) \in F_=$. Informally: let us work modulo $(1 - U \cdot T)$. Replace everywhere in V_i and W_j, T by $1/U$ so that T disappears, then multiply by a suitable U^{2m} in order to suppress the denominator. More precisely: the same final result should be obtained if we first multiply by U^{2m} ($m \geq \deg_T(V_i)$ and $2m \geq \deg_T(W_j)$) and then replace each $U^k \cdot T^k$ in V_i and W_j by 1 modulo $(1 - U \cdot T)$.

One obtains thus an algebraic indentity:

$$S_1(\boldsymbol{X}) \cdot U^{2m} + \sum_{i=1}^{h} Q_i(\boldsymbol{X}) \cdot A_i^2(\boldsymbol{X}) + (1 - U \cdot T) \cdot Y_2(\boldsymbol{X}, T) + \sum_{j=1}^{r} N_j(\boldsymbol{X}) \cdot C_j(\boldsymbol{X}) = 0$$

One now has $Y_2(\boldsymbol{X}, T) = 0$ (otherwise consider in Y_2 the monomial of maximum degree in T). The remaining algebraic identity is a strong implication $^*([, U \neq 0] \implies 1 = 0))^*$:

$$S_1(\boldsymbol{X}) \cdot U^{2m} + \sum_{i=1}^{h} Q_i(\boldsymbol{X}) \cdot A_i^2(\boldsymbol{X}) + \sum_{j=1}^{r} N_j(\boldsymbol{X}) \cdot C_j(\boldsymbol{X}) = 0$$

Q. E. D.

Corollary 1 (authorization to add the inverse of the square root of a strictly positive element).

$$^*(U > 0 \implies \exists T \; 1 = U \cdot T^2)^*$$

Corollary 2 (the weak real Nullstellensatz implies the other real ... stellensatz). *Assume that for each natural number n and all systems of equalities to 0 on polynomials of* $\mathbf{K}[\boldsymbol{X}]$, *the impossibility in* $\mathbf{R}$ *(real closure of* $\mathbf{K}$*) implies the strong incompatibility in* $\mathbf{K}$. *Then, for all gsc systems on polynomials of* $\mathbf{K}[\boldsymbol{X}]$, *the impossibility in* $\mathbf{R}$ *implies the strong incompatibility in* $\mathbf{K}$.

Remarks 7: Theorems 19 and 20 "give the authorization" to add the root(s) of an equation of degree 1 or 2. Theorem 19 is also a consequence of theorem 21. Corollary 1 can be proved as in theorems 19 and 20. Corollary 2 is thus "directly" provable without the general theory of potential existence, as in the algebraically closed case.

Theorem 21 (authorization to add a root on an interval where a polynomial changes sign). *Denote by $P(U)$ a polynomial $P(\boldsymbol{X}, U)$. Then we have:*

$$^*([P(U) \cdot P(V) < 0, U < V] \implies \exists W[P(W) = 0, P(U) \cdot P(V) < 0, U < W < V])^*$$

Proof: Notation is as in the proof of proposition 6.

FIRST PART: We prove the potential existence

$$^*(P(U) \cdot P(V) \leq 0 \implies \exists W \; P(W) = 0)^*$$

We give a proof by induction[3] on the degree in T of $P(\boldsymbol{X}, T)$. When $\deg(P) = 0$ or -1, the result is easy.

[3]This proof "recopies" the classical proof of "if we have an ordered field and if $P(u) \cdot P(v) < 0$ with P irreducible, then the field $\mathbf{K}[W]/P(W)$ is real".

One may assume the variables U and V to be two variables X_i.[4] For any *gsc* system without the variable W we have to give a construction:

$$^*([, P(\boldsymbol{X}, W) = 0] \implies 1 = 0)^* \underset{\text{cons}}{\vdash} {}^*([, P(\boldsymbol{X}, U) \cdot P(\boldsymbol{X}, V) \leq 0] \implies 1 = 0)^*$$

which we may reread:

$$^*(\implies P(\boldsymbol{X}, W) \neq 0)^* \underset{\text{cons}}{\vdash} {}^*(\implies P(\boldsymbol{X}, U) \cdot P(\boldsymbol{X}, V) > 0)^*$$

Assume at first P is monic. The strong implication $^*(\implies P(\boldsymbol{X}, W) \neq 0)^*$ is written as an algebraic identity:

$$S_1(\boldsymbol{X}) + \sum_{i=1}^{h} Q_i(\boldsymbol{X}) \cdot B_i^2(\boldsymbol{X}, W) - P(\boldsymbol{X}, W) \cdot G(\boldsymbol{X}, W) + \sum_{j=1}^{r} N_j(\boldsymbol{X}) \cdot C_j(\boldsymbol{X}, W) = 0$$

with $Q_i(\boldsymbol{X}) \in \mathcal{C}p(F_{\geq} \cup F_{>})$ and $N_j(\boldsymbol{X}) \in F_{=}$. The polynomials $B_i(\boldsymbol{X}, W)$ and $C_j(\boldsymbol{X}, W)$ may be taken modulo P in W (because P is monic), and so $\deg_W(G) \leq \deg_W(P) - 2$. The same equality may be reinterpreted as various strong implications:

(1) $$^*(\implies G(\boldsymbol{X}, W) \neq 0)^*$$

(2) $$^*(\implies P(\boldsymbol{X}, W) \cdot G(\boldsymbol{X}, W) > 0)^*$$

Then, by substitution in (2),

$$^*(\implies P(\boldsymbol{X}, U) \cdot G(\boldsymbol{X}, U) > 0)^*, \ ^*(\implies P(\boldsymbol{X}, V) \cdot G(\boldsymbol{X}, V) > 0)^*$$

Hence,

$$^*(\implies P(\boldsymbol{X}, U) \cdot G(\boldsymbol{X}, U) \cdot P(\boldsymbol{X}, V) \cdot G(\boldsymbol{X}, V) > 0)^*$$

By the induction hypothesis, (1) implies that we can construct a strong implication:

$$^*(\implies G(\boldsymbol{X}, U) \cdot G(\boldsymbol{X}, V) > 0)^*.$$

But by trivial strong implications:

$$^*([P(\boldsymbol{X}, U) \cdot G(\boldsymbol{X}, U) \cdot P(\boldsymbol{X}, V) \cdot G(\boldsymbol{X}, V) > 0, \ G(\boldsymbol{X}, U) \cdot G(\boldsymbol{X}, V) > 0] \implies P(\boldsymbol{X}, U) \cdot P(\boldsymbol{X}, V) > 0)^*$$

We conclude the proof by transitivity of strong implications.

[4] According to the substitution principle for potential existence, we may actually assume we are in the generic case where U, V and the coefficients of P are all independent variables X_i.

Assume now P is not monic.

Let $C(\boldsymbol{X}) \cdot W^n$ be the leading monomial of $P(\boldsymbol{X}, W)$. Let $R(\boldsymbol{X}, W) = P(\boldsymbol{X}, W) - C(\boldsymbol{X}) \cdot W^n$. (so $\deg_W(R) < \deg_W(P)$). Consider a new variable T, and consider the polynomial $P_1(\boldsymbol{X}, T, W) = T \cdot R(\boldsymbol{X}, W) + W^n$. We give a proof of the potential existence by cases, according to the sign of $C(\boldsymbol{X})$.

1st case: $C(\boldsymbol{X}) = 0$. We have

$$^*([P(\boldsymbol{X}, U) \cdot P(\boldsymbol{X}, V) \leq 0, C(\boldsymbol{X}) = 0] \implies R(\boldsymbol{X}, U) \cdot R(\boldsymbol{X}, V) \leq 0)^*$$

and by the induction hypothesis

$$^*(R(\boldsymbol{X}, U) \cdot R(\boldsymbol{X}, V) \leq 0 \implies \exists W \; R(\boldsymbol{X}, W) = 0)^*$$

As

$$^*([R(\boldsymbol{X}, W) = 0, C(\boldsymbol{X}) = 0] \implies P(\boldsymbol{X}, W) = 0)^*$$

we conclude the proof by transitivity.

2nd case: $C(\boldsymbol{X}) \neq 0$. We have

$$^*(C(\boldsymbol{X}) \neq 0 \implies \exists T \; 1 = C(\boldsymbol{X}) \cdot T)^*,$$
$$^*(1 = C(\boldsymbol{X}) \cdot T \implies T \cdot P(\boldsymbol{X}, W) = P_1(\boldsymbol{X}, T, W))^*$$

and

$$^*(1 = C(\boldsymbol{X}) \cdot T \implies P(\boldsymbol{X}, W) = C(\boldsymbol{X}) \cdot P_1(\boldsymbol{X}, T, W))^*$$

so

$$^*([P(\boldsymbol{X}, U) \cdot P(\boldsymbol{X}, V) \leq 0, C(\boldsymbol{X}) \neq 0] \implies \exists T \; [1 = C(\boldsymbol{X}) \cdot T, P_1(\boldsymbol{X}, T, U) \cdot P_1(\boldsymbol{X}, T, V) \leq 0])^*$$

As P_1 is monic,

$$^*(P_1(\boldsymbol{X}, T, U) \cdot P_1(\boldsymbol{X}, T, V) \leq 0 \implies \exists W P_1(\boldsymbol{X}, T, W) = 0)^*$$

By transitivity,

$$^*([P(\boldsymbol{X}, U) \cdot P(\boldsymbol{X}, V) \leq 0, C(\boldsymbol{X}) \neq 0] \implies \exists T, W \; [1 = C(\boldsymbol{X}) \cdot T, P_1(\boldsymbol{X}, T, W) = 0])^*$$

Hence,

$$^*([P(\boldsymbol{X}, U) \cdot P(\boldsymbol{X}, V) \leq 0, C(\boldsymbol{X}) \neq 0] \implies \exists T, W \; P(\boldsymbol{X}, W) = 0)^*,$$

where we may remove T.

SECOND PART: Proof of the potential existence stated in the theorem.

We don't give the detailed proof. One may mimick the classical proof: if a root w of P is not between u and v, then we consider the polynomial $P(Z)/(Z - w)$, which also changes sign between u and v. So we may conclude by induction on $\deg(P)$. Q. E. D.

4) Strong evidence of the facts readable from a Hörmander tableau

Recall at first Hörmander's algorithm.

Proposition 22 (Hörmander tableau). *Let* $\mathbf{K}$ *be an ordered field, subfield of a real closed field* $\mathbf{R}$.

Let $L = [P_1, P_2, \ldots, P_k]$ *a list of polynomials of* $\mathbf{K}[\boldsymbol{X}]$.

Let $\mathcal{P}$ *be the polynomial family generated by the elements of* L *and by the operations* $P \mapsto P'$, *and* $(P, Q) \mapsto Rem(P, Q)$. *Then:*

1) $\mathcal{P}$ *is finite.*

2) One can set up the complete sign tableau for $\mathcal{P}$ *using only the following information:*

a) the degree of each polynomial in the family;

b) the diagrams of the operations $P \mapsto P'$, *and* $(P, Q) \mapsto Rem(P, Q)$ *(where* $\deg(P) \geq deg(Q)$*) in* $\mathcal{P}$ *; and*

c) the signs of the constants of $\mathcal{P}$.[5]

Proof: 1) is easy.

2) We number the polynomials in $\mathcal{P}$ in order of nondecreasing degree. Let $\mathcal{P}_n$ be the subfamily of $\mathcal{P}$ made of polynomials numbered 1 to n. Let us denote by $\mathcal{T}_n$ the Hörmander tableau corresponding to the family $\mathcal{P}_n$: i.e. the tableau where all the real roots of the polynomials of $\mathcal{P}_n$ are defined via a coding à la Thom, listed in increasing order, and where all the signs of the polynomials of $\mathcal{P}_n$ are indicated, at each root, and on each interval between two consecutive roots (or between $-\infty$ and the first root, or between the last root and $+\infty$).

Then by induction on n it is easy to prove that one can construct the tableau $\mathcal{T}_n$ from the allowed information. Q. E. D.

We are going to give a sufficiently faithful sketch for the proof of:

Theorem 23 (real Nullstellensatz in one variable). *Let* $\mathbf{K}$ *be an ordered field and* $\mathbf{R}$ *its real closure.*

Let $\mathcal{P}$ *be a family of polynomials of* $\mathbf{K}[X]$ *and* (X) *be a gsc system on elements of* $\mathcal{P}$.

Then:

either (x) *is impossible in* $\mathbf{R}$ *and then* $^*(\implies 1 = 0)^*$ *in* $\mathbf{K}$, *and thus* (x) *is impossible in any ordered extension of* $\mathbf{K}$.

or (x) *is possible in* $\mathbf{R}$ *and then* $^*(\exists X\ (X))^*$ *in* $\mathbf{K}$ *and in any ordered extension of* $\mathbf{K}$.

---

[5]Note that the constants in $\mathcal{P}$ are essentially the leading coefficients of polynomials in $\mathcal{P}$, and the values $P(\xi)$ where P is a polynomial in $\mathcal{P}$ and ξ a root of a degree one polynomial in $\mathcal{P}$.

One may assume that the family $\mathcal{P}$ is closed under the operations "remainder" and "derivation". The impossibility of (x) in $\mathbf{R}$ or the existence of x in $\mathbf{R}$ verifying (x) is directly readable from the Hörmander tableau of the family, and can be tested solely by computations in $\mathbf{K}$. We are going to show how the construction of the Hörmander tableau can be transformed, step by step, into strong evidence and potential existence which translate all the facts readable from the Hörmander tableau. If one now considers a given extension L of $\mathbf{K}$, one may apply to , L and its real closure, the results obtained for , $\mathbf{K}$ and $\mathbf{R}$: as the test is made solely by computations in $\mathbf{K}$ the possibility or the impossibility will be equivalent in the two cases.

When the field K is real closed.

Thus one has $\mathbf{R} = \mathbf{K}$. Let $\nu_1, \nu_2, \ldots, \nu_k$ be the finite list of points in the Hörmander tableau of the family $\mathcal{P}$. One can compute ν_0 and ν_{k+1} in $\mathbf{R}$ such that the strong evidence for the signs of all the $P \in \mathcal{P}$ is easy to state for $x \leq \nu_0$ and for $x \geq \nu_{k+1}$.

The possibility or otherwise in $\mathbf{R}$ for a given *gsc* system is immediately readable. Possibility occurs either for a ν_i, or for an $x = (\nu_i + \nu_{i+1})/2$ and this implies the potential existence. The incompatibility in $\mathbf{R}$ for a *gsc* system is also readable from the Hörmander tableau, but the strong incompatibility requires a new argument. One argues by cases, and it is sufficient to state the strong incompatibility for at least one *gsc* in : at each point ν_i on the one hand, on each open interval $]\nu_i, \nu_{i+1}[$ on the other hand, and finally for $X < \nu_0$ and for $X > \nu_{k+1}$. At a point ν_i the sign of each $P(\nu_i)$ is strongly evident in $\mathbf{R}$ (since $\nu_i \in \mathbf{R}$). On an interval $]\nu_i, \nu_{i+1}[$, the signs, constant and non zero, of the $P \in \mathcal{P}$ are all strongly evident from the signs at the end-points modulo a suitable mixed Taylor formula (cf. theorem 10(5)).

In the coefficients field.

We want to state, for all the facts readable from the Hörmander tableau, strong incompatibility and potential existence in $\mathbf{K}$. We have now to follow the Hörmander algorithm step by step, i.e. introducing the points in the Hörmander tableau one after the other. We begin by computing a and b in $\mathbf{K}$, such that for $x \leq a$ and for $x \geq b$, the signs of the polynomials in $\mathcal{P}$ are strongly evident. These 2 elements of $\mathbf{K}$ will replace $-\infty$ and $+\infty$ in the Hörmander tableau.

One first proves the lemma:

Lemma 24 (strong evidence and potential existence for the elementary facts readable from a Hörmander tableau). *Let* $\mathbf{K}$ *be an ordered field and* $\mathbf{R}$ *its real closure. Let* $\mathcal{P}$ *be a family of polynomials of* $\mathbf{K}[X]$ *closed under the operations "remainder" and "derivation", and let* $\mathcal{T}$ *be its Hörmander tableau.*

1) the points of the Hörmander tableau, defined à la Thom by their construction, satisfy the potential existence for their coding à la Thom.[6]
2) the comparison of 2 points of the tableau is strongly evident from their coding à la Thom.
3) at each point α in the tableau, the signs of all the polynomials in the family are strongly evident from the coding à la Thom for α.
4) at each point of a minimal open interval in the tableau, the signs of all the polynomials previously introduced are strongly evident either from the coding à la Thom for the interval bounds (if the interval is unbounded, only the finite bound is to be considered) and from the fact that the point is between the bounds, or also from the coding à la Thom for the interval.

Proof of the lemma: We prove the lemma for the family $\mathcal{P}_n$ and the tableau $\mathcal{T}_n$, by induction on n. The lemma is evident when all the polynomials are constants.

Let us go from n to $n+1$. If λ is a point of $\mathcal{T}_n$, we shall denote by $Q_\lambda(X)$ the first polynomial of which λ is a root, and ${}_\lambda(X)$ the *gsc* system which is its coding à la Thom (λ is the only point of $\mathbf{R}$ verifying ${}_\lambda(\lambda)$). Let now P be the polynomial numbered $n+1$, of degree $d \geq 1$.

In the following proof we examine only bounded open intervals. The modifications for the other case are easy.

For each point λ of $\mathcal{T}$, we introduce a new variable X_λ. In order to have a more readable proof, we shall write λ for X_λ.[7]

point 1): The only problematic points are roots of P. The sign of P at a point λ of $\mathcal{T}_n$ is strongly evident from the sign of $\mathrm{Rem}(P, Q_\lambda)(\lambda)$ and from the fact that $Q_\lambda(\lambda) = 0$; thus also, by the induction hypothesis (3), from ${}_\lambda(\lambda)$. Let ζ be a root of P on the minimal open interval $]\alpha, \beta[$ of $\mathcal{T}_n$. We have thus

$$^*({}_\alpha(\alpha) \implies P(\alpha) > 0)^* \text{ and } ^*({}_\beta(\beta) \implies P(\beta) < 0)^* \text{ or vice-versa.}$$

By the induction hypothesis (2) we have

$$^*([{}_\alpha(\alpha), {}_\beta(\beta)] \implies \alpha < \beta)^*$$

Theorem 21 and transitivity of potential existence give us

$$^*([{}_\alpha(\alpha), {}_\beta(\beta)] \implies \exists X[\alpha < X < \beta, P(X) = 0])^*$$

[6] A single point could be coded à la Thom via distinct polynomials. The coding we consider here is the first that appears in the tableau construction.
[7] The λ that we must read as X_λ are clear from the context.

Again by the induction hypothesis (3), there are $\tau_i \in \{<,>\}(i=1,\dots,d)$ such that, if we call τ'_i the sign $\leq$ or $\geq$ associated to τ_i, we have:[8]

$$^*({}_\alpha(\alpha) \implies [P^{(i)}(\alpha)\,\tau'_i\,0(i=1,\dots,d-1), P^{(d)}(\alpha)\,\tau_d\,0])^*$$
$$^*({}_\beta(\beta) \implies [P^{(i)}(\beta)\,\tau'_i\,0(i=1,\dots,d-1), P^{(d)}(\beta)\,\tau_d\,0])^*$$

Let us apply mixed Taylor formulas (theorem 10(5)) and transitivity:

$$^*([{}_\alpha(\alpha), {}_\beta(\beta)] \implies$$
$$\exists X[\alpha < X < \beta, P(X)=0, P^{(i)}(X)\,\tau_i\,0(i=1,\dots,d)])^*$$

We have previously

$$^*(\exists \alpha,\beta[{}_\alpha(\alpha), {}_\beta(\beta)])^*$$

By transitivity,

$$^*(\exists X[P(X)=0, P^{(i)}(X)\,\tau_i\,0(i=1,\dots,d)])^*$$

We rewrite this potential existence

$$^*(\exists\zeta\ {}_\zeta(\zeta))^*$$

point 2): We have already the strong implications

$$^*({}_\alpha(\alpha) \implies P^{(i)}(\alpha)\,\tau'_i\,0)^*, ^*({}_\alpha(\alpha) \implies P(\alpha)>0)^*$$

(or <0) and

$$^*({}_\alpha(\alpha) \implies P^{(d)}(\alpha)\,\tau_d\,0)^*,$$

So the sign of $\alpha-\zeta$ is strongly evident from the codings à la Thom of α and ζ via theorem 10 (2), (idem for $\beta-\zeta$):

$$^*([{}_\alpha(\alpha), {}_\zeta(\zeta)] \implies \alpha<\zeta)^*$$

Point 2) for $\mathcal{T}_{n+1}$ can then be deduced from point 2) for $\mathcal{T}_n$: if for example $\lambda \in \mathcal{T}_n$ with $\lambda < a$ the induction hypothesis shows:

$$^*([{}_\alpha(\alpha), {}_\lambda(\lambda)] \implies \lambda<\alpha)^*$$

Thus

$$^*([{}_\alpha(\alpha), {}_\lambda(\lambda), {}_\zeta(\zeta)] \implies \lambda<\alpha<\zeta)^*$$

But $(\exists\alpha\ {}_\alpha(\alpha))^*$, so

$$^*([{}_\lambda(\lambda), {}_\zeta(\zeta)] \implies \lambda<\zeta)^*$$

point 3): The sign of P at each point λ of $\mathcal{T}_n$ is already strongly evident from the coding à la Thom of λ. It remains to see that the sign of $Q \in \mathcal{P}_n$ at a new point (as ζ in 1)) is strongly evident from its coding à la Thom. From 2) we have:

$$^*([{}_\alpha(\alpha), {}_\beta(\beta), {}_\zeta(\zeta)] \implies \alpha<\zeta<\beta)^*$$

The induction hypothesis (3) shows that the sign of Q in α and β is strongly evident from ${}_\alpha(\alpha)$ and ${}_\beta(\beta)$.

Again by theorem 10 (5) and transitivity,

$$^*([{}_\alpha(\alpha), {}_\beta(\beta), {}_\zeta(\zeta)] \implies Q(\zeta)\,\tau\,0)^* \text{ with } \tau\in\{<,>\}$$

[8]The statements concerning $P^{(d)}(.)$ are trivial since $P^{(d)}$ is a constant, we give them here essentially for the rereading of this proof when the coefficients of P will depend on parameters.

But

$$^*(\exists\alpha,\beta\ [_\alpha(\alpha),\ _\beta(\beta)])^*$$

so we obtain

$$^*(_\zeta(\zeta)\implies Q(\zeta)\,\tau\,0)^* \quad \text{with} \quad \tau\in\{<,>\}$$

point 4): Let us denote by $_{\lambda,\mu}(X)$ the coding à la Thom for a minimal open interval of $\mathcal{T}_{n+1}$. It is obtained from $_\lambda(X)$, $_\mu(X)$ by replacing sign conditions $Q_\lambda(X)=0$ and $Q_\mu(X)=0$ by the suitable strict sign conditions. Applying theorem 10 (2) we obtain:

$$^*([_\mu(\mu),_\lambda(\lambda),_{\lambda,\mu}(X)]\implies \lambda<X<\mu)^*$$

If now Q is an arbitrary polynomial in $\mathcal{P}_{n+1}$ we argue as in 3) for the sign of Q in ζ and we obtain the strong evidence for the sign of $Q(X)$ under the hypothesis $_{\lambda,\mu}(X)$ Q. E. D.

To finish the proof of theorem 23, we can recopy (using lemma 24), with the usual cautions, all that we have done in the case of a real closed field. The disjunction of cases will be sound because of (2). The sign evaluation for a polynomial at a point of the tableau will be replaced by the strong evidence of the sign for this polynomial etc ... Q. E. D.

5) Effective real Nullstellensanz and variants

When one has shown the "strong implication" version of the axioms and of the deduction rules in the formal theory of real closed fields with elements of $\mathbf{K}$ as constants, it is natural to wish to translate in form of strong implication every statement provable in this formal theory.

So to speak, the hardest part has been done with the validation of "proof by cases", the transitivity of strong implications and the authorization to add a root to a polynomial on an interval where it changes sign. In fact, as we have no "strong implication" version for statements with too many quantifier alternations, this is not completely straightforward.

The proof of the Nullstellensatz consists therefore of verifying that the algorithm for deciding a purely universal statement in the formal theory of real closed fields doesn't make use of logical arguments using statements with too many quantifier alternations.

Proposition 25 (parametrized Hörmander tableau). *Let* $\mathbf{K}$ *be an ordered field, subfield of a real closed field* $\mathbf{R}$. *Let* $L=[Q_1,Q_2,\ldots,Q_k]$ *a list of polynomials of* $\mathbf{K}[U_1,U_2,\ldots,U_n][X]$. *One can construct a finite family* $\mathcal{F}$ *of polynomials in* $\mathbf{K}[U_1,U_2,\ldots,U_n]$ *such that, for all* $u_1,u_2,\ldots,u_n$ *in* $\mathbf{K}$, *if we set* $P_i(X)=Q_i(u_1,u_2,\ldots,u_n;X)$, *the complete sign tableau for* $L=[P_1,P_2,\ldots,P_k]$ *is computable from the signs of the* $S(u_1,u_2,\ldots,u_n)$ *for* $S\in\mathcal{F}$.

Proof: The constants in the Hörmander algorithm (cf. proposition 22) are all obtained as rational fractions in the coefficients of polynomials of L. Otherwise, the computation of the family $\mathcal{P}$ is "uniform" except that a remainder computation, e.g. of $Rem(P,Q)$, depends on the degree of Q. As the Q coefficients are rational fractions in the coefficients of polynomials of L, the degree of Q, for a given specialization $u_1, u_2, \ldots, u_n$ of $U_1, U_2, \ldots, U_n$, depends on the vanishing of some polynomials in the coefficients of polynomials of L. Thus we include in the family $\mathcal{F}$ all the polynomials which appear in the numerator or the denominator of a coefficient of any polynomial of a family $\mathcal{P}$, for all the possible families $\mathcal{P}$. Q. E. D.

Theorem 26 (parametrized Hörmander tableau, strong implications and potential existence). *Let* $\mathbf{K}$ *be an ordered field, subfield of a real closed field* $\mathbf{R}$. *Let* $L = [Q_1, Q_2, \ldots, Q_k]$ *a list of polynomials of* $\mathbf{K}[U_1, U_2, \ldots, U_n][X]$. *One constructs the finite family* $\mathcal{F}$ *of polynomials in* $\mathbf{K}[U_1, U_2, \ldots, U_n]$ *as in proposition 25. Let* $(U_1, U_2, \ldots, U_n, X)$ *be a gsc system on polynomials in the list* L. *Let* $\sum = (\sigma_S)_{S\in\mathcal{F}}$ *in* $\{-1, 0, +1\}^{\mathcal{F}}$.

One denotes by $_\Sigma(U_1, U_2, \ldots, U_n)$ *the gsc system*

$$[S(U_1, U_2, \ldots, U_n) \equiv \sigma_S;\ S \in \mathcal{F}].$$

Assume that there exist $u_1, u_2, \ldots, u_n \in \mathbf{R}$ *satisfying* $_\Sigma(u_1, u_2, \ldots, u_n)$. *Then:*
either

$$\forall u_1, u_2, \ldots, u_n \in \mathbf{R}\ (_\Sigma(u_1, u_2, \ldots, u_n) \implies \exists x \in \mathbf{R}\ (u_1, u_2, \ldots, u_n, x))$$

and then

$$^*(_\Sigma(U_1, U_2, \ldots, U_n) \implies \exists X\ (U_1, U_2, \ldots, U_n, X))^*\ \textit{(read in } \mathbf{K})$$

or

$$\forall u_1, u_2, \ldots, u_n, x \in \mathbf{R}(_\Sigma(u_1, u_2, \ldots, u_n)\ \textit{and}\ (u_1, u_2, \ldots, u_n, x)) \implies 1 = 0$$

and then

$$^*([_\Sigma(U_1, U_2, \ldots, Un), (U_1, U_2, \ldots, U_n, X)] \implies 1 = 0)^*\ \textit{(in } \mathbf{K}).$$

Proof: The sign conditions $_\Sigma$ prescribe the degrees of the polynomials in the family (closed under remainder and derivation) generated by L, and also prescribe the Hörmander tableau of the family. We can then repeat with the usual cautions the reasonings in the proof of theorem 23, and we obtain theorem 23 "with parameters", i.e. theorem 26. Q. E. D.

The real effective Nullstellensatz is now easy.

Theorem 27 (Effective real Nullstellensatz, Positivestellensatz and Nichtnegativestellensatz). *Let* $\mathbf{K}$ *be an ordered field, subfield of a real closed field* $\mathbf{R}$. *Let* $(U_1, U_2, \ldots, U_n)$ *be a gsc system for a finite family of polynomials in* $\mathbf{K}[U_1, U_2, \ldots, U_n]$. *This system is impossible in* $\mathbf{R}$ *if and only if it is strongly incompatible in* $\mathbf{K}$.

In more formal terms:

If $\forall u_1, u_2, \ldots, u_n \in \mathbf{R}$ $(u_1, u_2, \ldots, u_n)$ *is absurd, then:*

$$^*((U_1, U_2, \ldots, U_n) \implies 1 = 0)^* \quad (\textit{in } \mathbf{K}\ ).$$

If

$$^*((U_1, U_2, \ldots, U_n) \implies 1 = 0)^* \quad (\textit{in } \mathbf{K}\ ),$$

then the gsc $(u_1, u_2, \ldots, u_n)$ *are impossible to realize in any ordered extension of* $\mathbf{K}$.

Proof: The "converse" part is evident. For the "forward" part, one argues by induction on the number of variables. For $n = 1$, this is theorem 23. Let us go from n to $n+1$. Let us call X the $(n+1)^{\text{st}}$ variable. In order to construct the strong implication, one argues case by case, according to the signs of the polynomials in the family $\mathcal{F}$ and one uses theorem 26.Q. E. D.

One has also immediately:

Theorem 28 (uniformly primitive recursive real Nullstellensatz and variants). *Let* $\mathbf{K}$ *be an ordered field, subfield of a real closed field* $\mathbf{R}$. *Let* $(U_1, U_2, \ldots, U_n)$ *be a gsc system for a finite family of polynomials in* $\mathbf{K}[U_1, U_2, \ldots, U_n]$. *Let* $(c_i)_{i \in I}$ *be the finite family of coefficients of polynomials in . Suppose that the structure of ordered field of* $Q((c_i)_{i \in I}$ *is given by an oracle that answers to the question: " what is the sign of* $P((c_i)_{i \in I})$*?", where the input is the polynomial* $P \in [(C_i)_{i \in I}]$. *There exists a uniformly primitive recursive algorithm that says wether is impossible in* $\mathbf{R}$ *and constructs, in the case of a positive answer, a strong implication* $^*(\implies 1 = 0)^*$ *(in* $\mathbf{K}$*).*

Remark 8: It would be easy to prove, by induction on the number of variables, an improvement of theorem 27, that should state: existence in $\mathbf{R}$ implies potential existence read in $\mathbf{K}$, and vice versa. In fact, the Nullstellensatz having been proved, one can deduce immediately the following interpretation for potential existence under conditions: Let $_1$ be a *gsc* system on polynomials of $\mathbf{K}[\boldsymbol{X}] = \mathbf{K}[X_1, X_2, \ldots, X_n]$, and $_2$ a *gsc* system on polynomials of $\mathbf{K}[\boldsymbol{X}, T_1, T_2, \ldots, T_m] = \mathbf{K}[\boldsymbol{X}, T]$. Then one has

$$^*(_1(\boldsymbol{X}) \implies \exists T\ _2(\boldsymbol{X}, \boldsymbol{T}))^* \quad \text{(read in } \mathbf{K})$$

if and only if

$$\forall \boldsymbol{x} \in \mathbf{R}^n (_1(\boldsymbol{x}) \implies \exists \boldsymbol{t} \in \mathbf{R}^m\ _2(\boldsymbol{x}, \boldsymbol{t}))$$

Remark 9: The same methods, simplified, could be applied in field theory (the only sign conditions are $= 0$ and $\neq 0$). One can thus obtain a direct constructive proof for the Hilbert Nullstellensatz, with a uniformly primitive recursive algorithm, (for the discrete case), without having to develop the constructive noetherian theory.

Acknowledgements: I thank Marie-Françoise Roy for her many comments and helpful suggestions.

REFERENCES

[BCR] Bochnak J., Coste M., Roy M.-F., "Géométrie Algébrique réelle," A series of Modern Surveys in Mathematics 11, Springer-Verlag, 1987.

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

[Efr] Efroymson, G., *Local reality on algebraic varieties*, J. of Algebra **29** (1974), 113–142.

[Kri] Krivine, J. L., *Anneaux préordonnés*, Journal d'analyse mathématique **12** (1964), 307–326.

[LR] Lombardi H., Roy M.-F., *Théorie constructive élémentaire des corps ordonnés*. English version in these proceedings

[Lom] Lombardi H., *Théorème des zéros réel effectif et variantes*, Publications Mathématiques de Besançon 88-89. Théorie des nombres. Fascicule 1.

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

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

[Ste] Stengle, G., *A Nullstellensatz and a Positivestellensatz in semialgebraic geometry*, Math. Ann. **207** (1974), 87–97.

Henri Lombardi
Laboratoire de Mathématiques.
UFR des Sciences et Techniques.
Université de Franche-Comté.
25 030 Besançon cédex
France