

Une preuve élémentaire (erronée) du Nullstellensatz réel effectif

Henri LOMBARDI
Besançon

Marie-Françoise ROY
Rennes

Résumé : Nous donnons dans cette note une preuve élémentaire du Nullstellensatz réel effectif (dans la version générale de Stengle). Les outils essentiels sont le théorème de Polya-Habicht et des trucs à la Rabinovitch.

Abstract : We give an elementary proof of the effective real Nullstellensatz, based on the Polya-Habicht theorem and on some tricks à la Rabinovitch.

Abridged English Version

Let \mathbf{K} be an ordered field and \mathbf{R} be its real closure. We denote by $\mathbf{K}[\mathbf{u}]$ the polynomial ring $\mathbf{K}[u_1, u_2, \dots, u_n]$. The Stengle real Nullstellensatz ([Ste]) is the following theorem :

Theorem : Let $[P_1 \geq 0, \dots, P_j \geq 0, Z_1 = 0, \dots, Z_k = 0, S_1 \neq 0, \dots, S_h \neq 0]$ be a system of signs conditions bearing on elements of $\mathbf{K}[\mathbf{u}]$. The two following assertions are equivalent :

- the system is impossible in \mathbf{R}^n
- there exists an algebraic identity in $\mathbf{K}[\mathbf{u}]$: $S^2 + P + Z = 0$, with S in the multiplicative monoid generated by S_1, \dots, S_h , P in the positive cone generated in $\mathbf{K}[\mathbf{u}]$ by $\mathbf{K}^+, P_1, \dots, P_j$ and Z in the ideal of $\mathbf{K}[\mathbf{u}]$ generated by Z_1, \dots, Z_k

Now we give the main steps of the constructive proof (effective Stengle real Nullstellensatz).

Definition and notation 1 : A system of signs conditions $[P_1 \geq 0, \dots, P_j \geq 0, Z_1 = 0, \dots, Z_k = 0, S_1 \neq 0, \dots, S_h \neq 0]$ is said to be *impossible* if it is impossible in \mathbf{R}^n and it is said to be *incompatible in \mathbf{K}* if we have a Stengle identity $S^2 + P + Z = 0$ for this system.

We shall use the following notation for an incompatibility:

$$\downarrow [P_1 \geq 0, \dots, P_j \geq 0, Z_1 = 0, \dots, Z_k = 0, S_1 \neq 0, \dots, S_h \neq 0] \downarrow$$

Notation 2 : The notation $(\downarrow \mathbb{H}_1 \downarrow \text{ and } \downarrow \mathbb{H}_2 \downarrow) \stackrel{\text{cons}}{\vdash} \downarrow \mathbb{H}_3 \downarrow$ means that we have an algorithm for constructing an incompatibility of type $\downarrow \mathbb{H}_3 \downarrow$ from incompatibilities of types $\downarrow \mathbb{H}_1 \downarrow$ and $\downarrow \mathbb{H}_2 \downarrow$

The two following propositions are tricks à la Rabinovitch.

Proposition 3 : ([Lom1]) Let $\mathbb{H}(\mathbf{u}, \mathbf{v})$ be a system of signs conditions, without the variable x , and $C(\mathbf{u})$ be a polynomial. Then :

$$\downarrow [C(\mathbf{u}) \cdot x = 1, \mathbb{H}(\mathbf{u}, \mathbf{v})] \downarrow \stackrel{\text{cons}}{\vdash} \downarrow [C(\mathbf{u}) \neq 0, \mathbb{H}(\mathbf{u}, \mathbf{v})] \downarrow$$

Proposition 4 : ([Lom1]) Let $\mathbb{H}(\mathbf{u}, \mathbf{v})$ be a system of signs conditions, without the variable x , and $C(\mathbf{u})$ be a polynomial. Then :

$$\downarrow [C(\mathbf{u}) = x^2, \mathbb{H}(\mathbf{u}, \mathbf{v})] \downarrow \stackrel{\text{cons}}{\vdash} \downarrow [C(\mathbf{u}) \geq 0, \mathbb{H}(\mathbf{u}, \mathbf{v})] \downarrow$$

Corollary 5 : ([Lom1]) Assume we know how to construct, for an ordered field \mathbf{K} , an

incompatibility $\downarrow H \downarrow$ for any impossible system H in which the only signs conditions are equalities. Then we have also an effective Stengle real nullstellensatz (for the field K)

Corollary 6 : Assume we know how to construct, for an ordered field K , an incompatibility $\downarrow P(u) = 0 \downarrow$, for any everywhere (in \mathbb{R}^n) positive polynomial. Then we have also an effective Stengle real nullstellensatz (for the field K)

Theorem 7 : (from *Polya-Habicht theorem*, [Hab], [HLP])

Let $P(u)$ be a polynomial in $\mathbb{Q}[u_1, \dots, u_n]$ bounded below by $a > 0$. Then we have an incompatibility in \mathbb{Q} : $\downarrow P(u) \leq 0 \downarrow$????????????????????.

Theorem 8 : (*improved Habicht theorem*)

Let $P(u)$ be a polynomial in $\mathbb{Q}[u_1, \dots, u_n]$ everywhere positive. Then we have an incompatibility in \mathbb{Q} : $\downarrow P(u) \leq 0 \downarrow$.

proof : Remark only that for a good exponent q the polynomial $P(u) (1 + \sum_i u_i^2)^4$ verifies the hypothesis of theorem 7. \square

Theorem 9 : (*effective Stengle real Nullstellensatz for \mathbb{Q}*)

The real Nullstellensatz is effective in the general Stengle form, for the field \mathbb{Q} .

preuve > From theorem 8 and corollary 6. \square

Theorem 10 : (*effective Stengle real Nullstellensatz*)

The real Nullstellensatz is effective in the general Stengle form, for any effective ordered field in which there is an effective sign test.

proof : From theorem 9 by parametrization. \square

Remark also that complexity bounds for the algorithm we have sketched here should be computed and that they are elementary recursive: the number of arithmetical operations can be bounded by an elementary recursive function in the degrees, the number of variables and the number of signs conditions. This is better than the previous bounds given in [Lom2].

Version française

1) Introduction

Une version effective du Nullstellensatz réel sous sa forme générale est donnée ici en utilisant des méthodes de construction relativement simples. Le calcul des bornes de complexité pour l'algorithme correspondant n'est pas explicité, mais il donnerait pour résultat une borne, pour les degrés et pour le nombre d'opérations arithmétiques dans le corps de base, élémentairement récursive en le degré, le nombre de variables et le nombre de conditions de signes donnés de départ. Ce résultat est meilleur que celui obtenu dans [Lom2].

2) Quelques notions et outils de base

Soit un corps ordonné K , de clôture réelle \mathbb{R} . Nous notons $K[u]$ l'anneau des polynômes $K[u_1, u_2, \dots, u_n]$. Soit une partie finie F de $K[u]$:

- nous notons F^2 l'ensemble des carrés d'éléments de F .
- le *monoïde multiplicatif engendré* par F est l'ensemble des produits d'éléments de

- $F \cup \{1\}$, nous le noterons $\mathcal{M}(F)$.
- le *cone positif engendré* par F est l'ensemble des sommes d'éléments du type $p.P.Q^2$ où p est positif dans \mathbf{K} , P est dans $\mathcal{M}(F)$, Q est dans $\mathbf{K}[\mathbf{u}]$. Nous le noterons $\mathcal{C}(F)$.
 - enfin nous noterons $I(F)$ l'idéal engendré par F dans $\mathbf{K}[\mathbf{u}]$.

Une *condition de signe* portant sur un élément x est une des relations $x < 0$, $x \leq 0$, $x = 0$, $x > 0$, $x \geq 0$, $x \neq 0$. Dans la suite, nous utilisons, sans perte de généralité, uniquement les conditions de signes $x = 0$, $x \geq 0$, $x \neq 0$.

Définition et notation 2.1 : Étant données trois parties finies de $\mathbf{K}[\mathbf{u}]$: F_{\geq} , $F_{=}$, F_{\neq} , contenant des polynômes auxquels on souhaite imposer respectivement les conditions de signes ≥ 0 , $= 0$, $\neq 0$, on dira que $F = [F_{\geq}; F_{=}; F_{\neq}]$ est *incompatible* dans \mathbf{K} si on a une égalité dans $\mathbf{K}[\mathbf{u}]$ du type suivant :

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

Nous utiliserons la notation suivante pour une incompatibilité:

$$\downarrow [P_1 \geq 0, \dots, P_j \geq 0, Z_1 = 0, \dots, Z_k = 0, S_1 \neq 0, \dots, S_h \neq 0] \downarrow$$

Il est clair qu'une incompatibilité est une forme très forte d'impossibilité. En particulier, elle implique l'impossibilité d'attribuer les signes indiqués aux polynômes souhaités, dans *n'importe quelle* extension ordonnée de \mathbf{K} . Dans [Lom1], on appelait incompatibilité forte ce qui est ici appelé plus simplement incompatibilité.

Le théorème des zéros réels et ses variantes

Les différentes variantes du théorème des zéros réel sont conséquence du théorème général suivant :

Théorème : (*Nullstellensatz réel sous forme générale*)

Soit \mathbf{K} un corps ordonné et \mathbf{R} la clôture réelle de \mathbf{K} . Les trois faits suivants, concernant un système de conditions de signes portant sur des polynômes de $\mathbf{K}[\mathbf{u}]$, sont équivalents :

l'incompatibilité dans \mathbf{K}

l'impossibilité dans \mathbf{R}^n

l'impossibilité dans toutes les extensions ordonnées de \mathbf{K}

Ce théorème remonte à 1974 ([Ste]). Des variantes plus faibles ont été établies par Krivine ([Kri]), Dubois ([Du]), Risler ([Ris]), Efroymsou ([Efr]). Toutes les preuves jusqu'à ([Lom1]) utilisaient des méthodes non constructives.

Constructions d'incompatibilités

Notation 2.2 : La notation

$$(\downarrow \mathbb{H}_1 \downarrow \text{ et } \downarrow \mathbb{H}_2 \downarrow) \stackrel{\text{cons}}{\vdash} \downarrow \mathbb{H}_3 \downarrow$$

signifie qu'on a un algorithme de construction d'une incompatibilité de type $\downarrow \mathbb{H}_3 \downarrow$ à partir d'incompatibilités de types $\downarrow \mathbb{H}_1 \downarrow$ et $\downarrow \mathbb{H}_2 \downarrow$

Dans cette note, nous utiliserons les constructions élémentaires suivantes:

Proposition 2.3 : ([Lom1]) Soit \mathbb{H} un système de conditions de signes portant sur des polynômes de $\mathbf{K}[\mathbf{u}]$, Q un élément de $\mathbf{K}[\mathbf{u}]$, alors:

$$[\downarrow (\mathbb{H}, Q \leq 0) \downarrow \text{ et } \downarrow (\mathbb{H}, Q \geq 0) \downarrow] \stackrel{\text{cons}}{\vdash} \downarrow \mathbb{H} \downarrow$$

preuve> Notons : F_{\geq} , $F_{=}$, F_{\neq} les trois parties finies de $\mathbf{K}[\mathbf{u}]$ contenant des polynomes auxquels sont attribués les conditions de signes correspondantes dans l'hypothèse \mathbb{H} .

L'hypothèse $\downarrow[\mathbb{H}, Q \geq 0] \downarrow$ signifie qu'on a une égalité :

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

c.-à-d. encore :

$$S_1 + Q.P_1 + R_1 + Z_1 = 0 \quad \text{avec } S_1 \in \mathcal{M}(F_{\neq}^2), P_1, R_1 \in \mathcal{C}(F_{\geq}), Z_1 \in I(F_{=})$$

De même l'hypothèse $\downarrow[\mathbb{H}, Q \leq 0] \downarrow$ signifie qu'on a une égalité :

$$S_2 - Q.P_2 + R_2 + Z_2 = 0 \quad \text{avec } S_2 \in \mathcal{M}(F_{\neq}^2), P_2, R_2 \in \mathcal{C}(F_{\geq}), Z_2 \in I(F_{=})$$

On réécrit les 2 égalités obtenues sous forme :

$$-Q.P_1 = S_1 + R_1 + Z_1 \quad \text{et} \quad Q.P_2 = S_2 + R_2 + Z_2 \quad \text{et on les multiplie :}$$

d'où $S_1.S_2 + [S_1.R_2 + S_2.R_1 + R_1.R_2 + Q^2.P_1.P_2] + W = 0$ avec $W \in I(F_{=})$

ce qui est précisément une incompatibilité $\downarrow \mathbb{H} \downarrow$. \square

Proposition 2.4 : (*autorisation de rajouter l'inverse d'un non nul*) ([Lom1])

Soit un système de conditions de signes $\mathbb{H}(\mathbf{u}, \mathbf{v})$, sans la variable x , et $C(\mathbf{u})$ un polynome. Alors on a la construction d'incompatibilités :

$$\downarrow [C(\mathbf{u}).x = 1, \mathbb{H}(\mathbf{u}, \mathbf{v})] \downarrow \downarrow_{\text{cons}} \downarrow [C(\mathbf{u}) \neq 0, \mathbb{H}(\mathbf{u}, \mathbf{v})] \downarrow$$

preuve> Nous reprenons des notations analogues à celles de la preuve de la proposition 2.3.

Nous notons \mathbf{u}' au lieu de \mathbf{u}, \mathbf{v} . L'incompatibilité donnée au départ s'écrit :

$$S(\mathbf{u}') + \sum_i q_i \cdot Q_i(\mathbf{u}') \cdot V_i^2(\mathbf{u}', x) + (1 - C(\mathbf{u}).x) \cdot V(\mathbf{u}', x) + \sum_j N_j(\mathbf{u}') \cdot W_j(\mathbf{u}', x) = 0$$

avec $S(\mathbf{u}') \in \mathcal{M}(F_{\neq}^2)$, $q_i > 0$ dans \mathbf{K} , $Q_i(\mathbf{u}') \in \mathcal{M}(F_{\geq})$, $N_j(\mathbf{u}') \in F_{=}$.

Si V est nul, on remplace x par 0. Sinon multiplions l'incompatibilité initiale par C^{2m} puis remplaçons chaque $C^k \cdot x^k$ dans chaque $C^m V_i$ et dans chaque $C^{2m} W_j$ par 1 modulo $(1 - C(\mathbf{u}).x)$. On obtient :

$$S(\mathbf{u}') \cdot C(\mathbf{u})^{2m} + \sum_i q_i \cdot Q_i(\mathbf{u}') \cdot A_i^2(\mathbf{u}') + (1 - C(\mathbf{u}).x) \cdot A(\mathbf{u}', x) + \sum_j N_j(\mathbf{u}') \cdot B_j(\mathbf{u}') = 0$$

Alors $A(\mathbf{u}', x) = 0$. On obtient donc une incompatibilité du type cherché :

$$S(\mathbf{u}') \cdot C(\mathbf{u})^{2m} + \sum_i q_i \cdot Q_i(\mathbf{u}') \cdot A_i^2(\mathbf{u}') + \sum_j N_j(\mathbf{u}') \cdot B_j(\mathbf{u}') = 0 \quad \square$$

Remarque: Cette preuve est très semblable au «Rabinovitch trick» (cf. par exemple l'exposé classique de van der Waerden sur le Nullstellensatz de Hilbert). De même, on aura :

Proposition 2.5 : (*autorisation de rajouter la racine carrée d'un positif ou nul*) ([Lom1])

Soit un système de conditions de signes $\mathbb{H}(\mathbf{u}, \mathbf{v})$, sans la variable x , et $C(\mathbf{u})$ un polynome. Alors on a la construction d'incompatibilités:

$$\downarrow [C(\mathbf{u}) = x^2, \mathbb{H}(\mathbf{u}, \mathbf{v})] \downarrow \downarrow_{\text{cons}} \downarrow [C(\mathbf{u}) \geq 0, \mathbb{H}(\mathbf{u}, \mathbf{v})] \downarrow$$

On déduit des deux propositions précédentes les corollaires suivants.

Corollaire 2.6 : (*le nullstellensatz général se déduit du nullstellensatz faible*) ([Lom1])

Supposons qu'on sache construire, pour un corps ordonné \mathbf{K} , une incompatibilité $\downarrow \mathbb{H} \downarrow$ pour tout système impossible \mathbb{H} dont les seules conditions de signes sont des égalités.

Alors, on a aussi le nullstellensatz réel effectif sous sa forme générale (pour le corps \mathbf{K})

Corollaire 2.7 : (*le nullstellensatz général se déduit d'une version particulière du 17ème problème de Hilbert*) Supposons qu'on sache construire, pour un corps ordonné \mathbf{K} , une incompatibilité $\downarrow P(\mathbf{u}) = 0 \downarrow$, pour tout polynome partout strictement positif dans \mathbf{R}^n .

Alors, on a aussi le nullstellensatz réel effectif sous sa forme générale (pour le corps \mathbf{K}).

preuve> Par le corollaire 2.6 on est ramené à traiter un système de conditions $P_i(\mathbf{u}) = 0$. On pose $P(\mathbf{u}) = \sum_i P_i(\mathbf{u})^2$. L'égalité $P(\mathbf{u}) = 0$ est impossible. L'incompatibilité $\downarrow P(\mathbf{u}) = 0 \downarrow$ se relit facilement comme une incompatibilité $\downarrow [P_i(\mathbf{u}) = 0, i = 1, \dots, k] \downarrow$. \square

3) La preuve du résultat

Rappelons tout d'abord le théorème de Polya [Pol]. L'inspection détaillée de sa preuve montrerait sa nature constructive.

Théorème 3.1 : (*théorème de Polya*, [Pol], [HLP])

Soit $P(\mathbf{u})$ un polynôme homogène de $\mathbb{Q}[u_1, \dots, u_n]$ strictement positif dans le premier orthant, c.-à-d. pour $u_1 \geq 0, \dots, u_n \geq 0, \sum_i u_i^2 \neq 0$. Alors, on peut trouver un exposant p tel que le polynôme $P(\mathbf{u}) (\sum_i u_i)^p$ ait ses coefficients tous > 0 .

Corollaire 3.2 : Soit $P(\mathbf{u})$ un polynôme homogène de $\mathbb{Q}[u_1, \dots, u_n]$ strictement positif dans le premier orthant. Alors on a une incompatibilité dans \mathbb{Q} :

$$\downarrow [u_1 \geq 0, \dots, u_n \geq 0, \sum_i u_i^2 \neq 0, P(\mathbf{u}) \leq 0] \downarrow$$

Théorème 3.3 : (*théorème de Habicht*, [Hab], [HLP])

Soit $P(\mathbf{u})$ un polynôme homogène de $\mathbb{Q}[u_1, \dots, u_n]$ strictement positif en dehors de $\mathbf{0}$.

Alors on a une incompatibilité dans \mathbb{Q} : $\downarrow [\sum_i u_i^2 \neq 0, P(\mathbf{u}) \leq 0] \downarrow$.

Soit $P(\mathbf{u})$ un polynôme de $\mathbb{Q}[u_1, \dots, u_n]$ minoré par un $a > 0$. Alors on a une incompatibilité dans \mathbb{Q} : $\downarrow P(\mathbf{u}) \leq 0 \downarrow$??????????????????

preuve> Dans le premier cas, on obtient une incompatibilité $\downarrow [P(\mathbf{u}) \leq 0, \sum_i u_i^2 \neq 0] \downarrow$ en raisonnant cas par cas (cf. proposition 2.3) à partir des identités fournies par le théorème de Polya dans chacun des orthants.

Hum Le cas non homogène s'en déduit facilement ??????????????????. \square

Théorème 3.4 : (*théorème de Habicht amélioré*)

Soit $P(\mathbf{u})$ un polynôme de $\mathbb{Q}[u_1, \dots, u_n]$ partout > 0 . Alors on a une incompatibilité dans \mathbb{Q} : $\downarrow P(\mathbf{u}) \leq 0 \downarrow$.

preuve> Il suffit de remarquer que, pour un certain exposant q le polynôme

$$P(\mathbf{u}) (1 + \sum_i u_i^2)^q$$

vérifie les hypothèses du théorème 3.3. \square

Théorème 3.5 :

Le nullstellensatz réel dans sa forme générale est effectif pour le cas du corps \mathbb{Q} .

preuve> Se déduit du théorème 3.4 et du corollaire 2.7 \square

Théorème 3.6 :

Le nullstellensatz réel dans sa forme générale est effectif pour tout corps ordonné explicite avec test de signe explicite.

preuve> Considérons un système de conditions de signes, $\mathbb{H}(\mathbf{u})$, portant sur des polynômes de $\mathbf{K}[\mathbf{u}]$ et incompatible dans \mathbf{R}^n . Remplaçons tous les coefficients par des paramètres \mathbf{c} . L'impossibilité du système avec paramètres $\mathbb{H}(\mathbf{c}, \mathbf{u})$ (où tous les coefficients non nuls sont

égaux à 1) est vraie lorsque ces paramètres vérifient certains systèmes de conditions de signes $\mathbb{H}_1(\mathbf{c}), \dots, \mathbb{H}_m(\mathbf{c})$, que l'on peut calculer par élimination des quantificateurs. Un de ces systèmes, par exemple $\mathbb{H}_1(\mathbf{c})$ est justement vérifié par les coefficients dans \mathbf{K} (ici, on suppose que \mathbf{K} est un corps ordonné explicite avec test de signe explicite). On a donc l'impossibilité du système $[\mathbb{H}(\mathbf{c}, \mathbf{u}), \mathbb{H}_1(\mathbf{c})]$ où tous les polynômes sont à coefficients dans \mathbb{Q} . On peut appliquer le théorème 3.5. On termine en remplaçant les paramètres \mathbf{c} par les coefficients dans \mathbf{K} correspondants. \square

Plus généralement, la preuve fournit un algorithme où l'entrée est le système $\mathbb{H}(\mathbf{c}, \mathbf{u})$ et où la structure du corps \mathbf{K} peut être représentée par un oracle qui donne le signe de $Q(\mathbf{c})$ si Q est un polynôme à coefficients entiers qui représente la question posée à l'oracle.

Henri LOMBARDI
Laboratoire de Mathématiques
URA CNRS 741
UFR des Sciences et Techniques
Université de Franche-Comté
25 030 Besançon cédex
France
email : hl@grenet.fr

Marie-Françoise ROY
I R M A R
URA CNRS 305
Université de Rennes 1
Campus de Beaulieu
35 042 Rennes cédex
France
costeroy@univ-rennes1.fr

Bibliographie:

- [Du] Dubois, D. W.: *A nullstellensatz for ordered fields*, Arkiv for Mat., Stockholm, 8, 1969, 111-114
- [Efr] Efroymsen, G.: *Local reality on algebraic varieties*, J. of Algebra, 29, 1974, 113-142.
- [Hab] Habicht W.: *Über die Zerlegung strikte definiter Formen in Quadrate*. Comm. Math. Helvetici 12, 317-322 (1940).
- [HLP] Hardy G., Littlewood J., Polya G.: *Inequalities*. (second edition). Cambridge University Press, 1967
- [Kri] Krivine, J. L.: *Anneaux préordonnés*. Journal d'analyse mathématique, t.12, 1964, p. 307-326
- [Lom1] Lombardi H.: *Effective real nullstellensatz and variants*. p. 263-288 in Effective Methods in Algebraic Geometry. Ed. Mora T., Traverso C.. Birkhäuser 1991. Progress in Math. n° 94 (Comptes rendus du colloque MEGA 90 Castiglioncello, Italie). Version française plus détaillée: *Théorème effectif des zéros réel et variantes*. Publications Mathématiques de l'Université (Besançon). 88-89. Fascicule 1.
- [Lom2] Lombardi H.: *Une borne sur les degrés pour le Théorème des zéros réel effectif*. p 323-345. In : Real Algebraic Geometry. Proceedings, Rennes 1991, Lecture Notes in Mathematics n°1524. Eds. : Coste M., Mahé L., Roy M.-F.. (Springer-Verlag, 1992).
- [Pol] Polya G. : *Über positive Darstellung von Polynomen*. d. natur. Ges. Zür, 73, 141-145, 1928. See Collected Papers vol 2 MIT press, 309-313, 1974.
- [Ris] Risler, J.-J. : *Une caractérisation des idéaux des variétés algébriques réelles*. C.R.A.S. Paris, t. 271, 1970, série A, p. 1171-1173.
- [Ste] Stengle, G. : *A Nullstellensatz and a Positivstellensatz in semialgebraic geometry*. Math. Ann. 207, 87-97 (1974)