THEORIE DES NOMBRES

BESANCON

Année 1988/1989

Fascicule 1

THEOREME DES ZEROS REEL EFFECTIF ET VARIANTES

Henri LOMBARDI

Théorème des zéros réel effectif et variantes

THEOREME DES ZEROS REEL EFFECTIF ET VARIANTES

Henri LOMBARDI

Résumé Nous donnons une preuve constructive du théorème des zéros réel et de ses variantes. Il s'ensuit, pour tout corps ordonné **K** , un algorithme uniformément primitif récursif qui calcule, à partir d'un système de conditions de signes généralisées (csg) portant sur des polynômes de $\mathbf{K}[X_1,X_2,...,X_n]$ et impossible à satisfaire dans la clôture réelle de **K** , une identité algébrique dans $\mathbf{K}[X_1,X_2,...,X_n]$ qui rend cette impossibilité évidente. L'idée essentielle est de donner une version "identité algébrique" des axiomes universels et existentiels de la théorie des corps réels clos, ainsi que des méthodes de déduction élémentaires (comme le Modus Ponens, ou le raisonnement cas par cas). On applique ensuite cette problématique à l'algorithme de Hormander, qui est l'algorithme conceptuellement le plus simple pour tester l'impossibilité d'un système de csg dans la clôture réelle d'un corps ordonné.

Mots clés Théorème des zéros réels, Corps ordonné, Effectivité, Mathématiques constructives, Algorithme de Hormander, Implication forte, Existence potentielle, Formules de Taylor mixte.

Effective real nullstellensatz and variants

Abstract We give a constructive proof of the real nullstellensatz. So we obtain, for every ordered filed **K** , a uniformly primitive recursive algorithm that computes, for the input "a system of generalized signs conditions (gsc) on polynomials of $\mathbf{K}[X_1,X_2,...,X_n]$ impossible to satisfy in the real closure of **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 field, and of the simplest deduction rules of this theory (as Modus Ponens). We apply this idea to the Hormander algorithm, that is the conceptually simplest test for the impossibility of a gsc system in the real closure of an ordered field.

Key-words Real nullstellensatz, Ordered field, Effectivity, Constructive mathematics, Hormander algorithm, Strong implication, Potential existence, Mixed Taylor formulas.

Remerciements: Je remercie Marie-Françoise Roy pour ses nombreux commentaires et ses précieuses suggestions.

1) Introduction

Cet article est la suite directe de [**LR**] , où nous développons la théorie constructive élémentaire des corps ordonnés, avec en particulier la preuve constructive de l'existence de la clôture réelle d'un corps ordonné **K** lorsqu'on dispose d'un test pour le signe d'un élément de **K** .

L'idée générale est la suivante. Pour un corps ordonné **K** il y a un algorithme de conception très simple pour tester si un système de csg (conditions de signes généralisées) portant sur ces polynômes en plusieurs variables est possible ou impossible dans la clôture réelle de **K** . C'est l'algorithme de Hormander, appliqué de manière itérative pour diminuer

par étapes le nombre de variables sur lesquelles portent les csg. Si on regarde les arguments sur lesquels est basée la preuve d'impossibilité (en cas d'impossibilité), on voit qu'il y a essentiellement des identités algébriques (traduisant la division euclidienne), le théorème des accroissements finis et l'existence d'une racine pour un polynôme sur un intervalle où il change de signe. Les ...-stellensatz réels effectifs devaient donc pouvoir être obtenus si on arrivait à "algébriser" les arguments de base de la preuve et les méthodes de déduction impliquées.
Un pas important a déjà été réalisé avec la version algébrique du théorème des accroissements finis pour les polynômes (que nous rappelons en annexe à la fin de cet article).
On a ensuite vérifié que les axiomes purement universels s'exprimaient sous forme d'*implication forte* (c.-à-d. sous forme "identité algébrique" , c.-à-d. encore sous forme "stellensatzisée").
Un autre pas a consisté à traduire sous forme de *constructions d'implications fortes* certains raisonnements élémentaires (du genre si $A \Rightarrow B$ et $B \Rightarrow C$ alors $A \Rightarrow C$).
Il fallait en outre trouver une version "identité algébrique" des axiomes d'existence dans la théorie des corps réels clos. C'est ce qui est fait à travers la notion d'*existence potentielle.*
Signalons également qu'une simplification importante dans la construction du nullstellensatz réel est obtenu à travers une version "algébrisée" du lemme de Thom, donnée par ce que nous appelons les formules de Taylor mixtes.
Notons enfin que l'un des sous-produits de la construction effective des nullstellensatz réels est une nouvelle preuve constructive de l'existence la clôture réelle d'un corps ordonné discret.

Bien que nous nous placions a priori dans un cadre constructif "à la Bishop", tel que développé dans [**MRR**] pour ce qui concerne la théorie des corps discrets, comme nous ne précisons pas le sens du mot effectif ni celui du mot décidable, toutes les preuves peuvent être lues avec des lunettes adaptées à la philosophie ou au cadre de travail de chaque lecteur particulier.

Si on adopte un point de vue "classique" par exemple, les procédures effectives intervenant dans les définitions de départ peuvent être considérées comme données par des oracles. En conséquence, les preuves fournissent une preuve dans le cadre classique, *et sans recours à l'axiome du choix*, du théorème des zéros réels dans un corps ordonné arbitraire.

Si on adopte le point de vue de la théorie classique "récursive", les preuves données fournissent des algorithmes uniformément primitifs récursifs, "uniformément" s'entendant par rapport à un oracle qui donne la structure du corps des coefficients du système de csg considéré...

Du point de vue constructif, les preuves que nous donnons sont valables pour les "corps ordonnés discrets" (le signe d'un élément est décidable, et les lois de corps sont calculables). La théorie constructive du cas "non discret" reste à faire. Nous pensons cependant que ce sera plus facile que pour le "non discret, non ordonné": en particulier la construction de la clôture réelle par des méthodes inspirées de [**LR**] ne semble pas trop problématique.

2) Incompatibilités, évidences et implications fortes

Notations et définitions

Incompatibilités fortes (définitions)

Nous considérons un corps ordonné $\mathbf{K}$, $\mathbf{X}$ désigne une liste de variables $X_1, X_2, ..., X_n$ nous notons donc $\mathbf{K}[\mathbf{X}]$ l'anneau des polynômes $\mathbf{K}[X_1,X_2,...,X_n]$.
Etant donnée une partie finie F de $\mathbf{K}[\mathbf{X}]$:

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 $\mathcal{M}(F)$, et $\mathcal{M}_2(F) := \mathcal{M}(F^{*2})$. Nous noterons $\mathcal{M}_1(F)$ la partie de $\mathcal{M}(F)$ formée des produits où chaque élément intervient au plus une fois.

le *cône positif engendré* par F est l'ensemble des sommes d'éléments du type $p.P.Q^2$ où p est positif dans **K** , P est dans $\mathcal{M}(F)$, Q est dans **K[X]** . Nous le noterons $Cp(F)$. On remarque que dans la définition, on pourrait supposer que P est dans $\mathcal{M}_1(F)$, ce qu'on fera désormais.

enfin nous noterons $I(F)$ l'idéal engendré par F .

Définition 1 : Etant donnés 4 parties finies de **K[X]** : $F_>$, $F_\geq$, $F_=$, $F_\neq$, contenant des polynômes auxquels on souhaite imposer respectivement les conditions de signes >0 , $\geqslant 0$, $=0$, $\neq 0$, on dira que $\mathbf{F} = [F_> ; F_\geq ; F_= ; F_\neq]$ est *fortement incompatible* dans $\mathbf{K}$[1] si on a une égalité dans **K[X]** du type suivant :

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

Toute incompatibilité forte écrite sous la forme (1) ci-dessus peut être ramenée à une incompatibilité forte écrite sous la forme (2) suivante :

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

Il suffit en effet de multiplier la première égalité par un élément convenable de $\mathcal{M}_1(F_>)$ pour obtenir chaque polynôme avec une puissance paire dans le premier terme S .

Il est clair qu'une incompatibilité forte est une forme très forte d'incompatibilité. En particulier, elle implique l'impossibilité d'attribuer les signes indiqués aux polynômes souhaités, dans *n'importe quelle* extension ordonnée de **K** .

Si on considère la clôture réelle **R** de **K** , l'impossibilité ci-dessus est testable par l'algorithme de Hormander, par exemple. De plus elle est alors constructivement équivalente à sa formulation sous forme d'implications diverses: par exemple " $P=0 \Rightarrow Q>0$ " équivaut à " $P=0$, $-Q \geqslant 0$ est impossible". Nous parlerons donc de manière indifférente d'incompatibilité forte, d'implication forte, ou d'évidence forte. En nous ramenant toujours implicitement à une incompatibilité forte.

Notation : Nous utiliserons la notation suivante pour une implication forte:

$$[\, S_1 > 0,\ldots,S_i > 0,\ P_1 \geqslant 0,\ldots,P_j \geqslant 0,\ Z_1 = 0,\ldots,Z_k = 0,\ N_1 \neq 0,\ldots,N_h \neq 0 \,] \overset{\text{fort}}{\Rightarrow} \quad Q \,\tau\, 0$$

On notera qu'en prenant $1 = 0$ au second membre dans l'implication forte ci-dessus, et en appliquant les définitions, on obtient exactement l'incompatibilité forte pour le premier membre de l'implication. Ce qui nous permet de formuler toutes les incompatibilités fortes sous forme d'implications fortes.

Notation : Notons $\mathbb{H}$ le premier membre de l'implication forte ci dessus. Notons $\mathbb{H}'$ un système de conditions de signes généralisées (csg) : $Q_1 \,\tau_1\, 0$, ... , $Q_k \,\tau_k\, 0$. Alors nous écrirons :

$\mathbb{H} \overset{\text{fort}}{\Rightarrow} \mathbb{H}'$ pour signifier $(\mathbb{H} \overset{\text{fort}}{\Rightarrow} Q_1 \,\tau_1\, 0)$ et ..... et $(\mathbb{H} \overset{\text{fort}}{\Rightarrow} Q_k \,\tau_k\, 0)$

---

[1] A priori, il faudrait parler d'"incompatibilité forte dans **K[X]**" , mais si on a une incompatibilité forte obtenue en rajoutant des variables, il suffit de remplacer ces variables par 0 pour obtenir une incompatibilité forte dans **K[X]** .

Le théorème des zéros réels et ses variantes :

Les différentes variantes du théorème des zéros dans le cas réel disent toutes que les trois faits suivants, concernant un système de csg portant sur des polynômes de $\mathbf{K}[\mathbf{X}]$, sont équivalents:

l'incompatibilité forte dans $\mathbf{K}$

l'impossibilité dans $\mathbf{R}$

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

Ce théorème des zéros réels remonte à 1974 ([**Ste**]). Des variantes plus faibles ont été établies par Dubois ([**Du**]), Risler ([**Ris**]), Efroymson ([**Efr**]). Toutes les preuves jusqu'à maintenant faisaient un usage intensif de l'axiome du choix. Les premières formulations étaient géométriques : affirmation de l'existence d'une identité algébrique assurant qu'un polynôme donné vérifie une csg donnée sur un ensemble algébrique ou semialgébrique donné.

Notre preuve du théorème consiste à mettre en évidence que l'impossibilité dans $\mathbf{R}$, qui peut être algorithmiquement testée dans $\mathbf{K}$, implique l'incompatibilité forte (dans $\mathbf{K}$).

On parle de *nullstellensatz* quand on considère la condition pour qu'un polynôme appartienne à l'idéal d'une variété algébrique donnée (c.-à-d. une implication : "des égalités à zéro impliquent une égalité à zéro"); de *nullstellensatz faible* quand on considère la condition pour qu'une variété algébrique donnée soit vide (c.-à-d. "des égalités à zéro sont incompatibles"), de *positivestellensatz* lorsqu'on considère la condition pour qu'un polynôme soit strictement positif sur une variété semi-algébrique donnée (c.-à-d. la forme générale d'incompatibilité entre csg vue sous forme d'une implication avec pour conclusion un signe strictement positif), de *nichtnegativestellensatz* lorsqu'on considère la condition pour qu'un polynôme soit positif ou nul sur une variété semi-algébrique donnée (c.-à-d. la forme générale d'incompatibilité entre csg vue sous forme d'une implication avec pour conclusion un signe positif ou nul).

Quelques implications fortes triviales

Nous laissons au lecteur le soin de vérifier la validité de la :

Proposition 2 : On a les implications fortes qui suivent.

$$
\begin{aligned}
[\,U>0\,,V>0\,] &\overset{\text{fort}}{\Rightarrow} [\,U+V>0\,,U.V>0\,]\\
[\,U+V\geqslant 0\,,U.V>0\,] &\overset{\text{fort}}{\Rightarrow} [\,U>0\,,V>0\,]\\
[\,U>0\,,V\geqslant 0\,] &\overset{\text{fort}}{\Rightarrow} U+V>0\\
[\,U\geqslant 0\,,U.V>0\,] &\overset{\text{fort}}{\Rightarrow} V>0\\
U\neq 0 &\overset{\text{fort}}{\Rightarrow} U^2>0\\
U^2>0 &\overset{\text{fort}}{\Rightarrow} U\neq 0\\
U=0 &\overset{\text{fort}}{\Rightarrow} U.V=0\\
U=V &\overset{\text{fort}}{\Rightarrow} P(\mathbf{X},U)=P(\mathbf{X},V)\\
[\,U=V\,,V\ \tau\ 0\,] &\overset{\text{fort}}{\Rightarrow} U\ \tau\ 0 \qquad (\bullet\ \tau\ 0 \text{ est une csg})\\
[\,U=0\,,V\ \tau\ 0\,] &\overset{\text{fort}}{\Rightarrow} (U+V)\ \tau\ 0\\
[\,] &\overset{\text{fort}}{\Rightarrow} [\,1+U^2>U\ ,\ 1+U^2>-U\,]
\end{aligned}
$$

Proposition 3 : (principe de substitution) .

Si, dans une implication forte, on remplace toute occurrence d'une variable par un polynôme fixé, on obtient encore une implication forte.

La preuve est triviale. Ainsi, les implications fortes de la proposition 2 , énoncées pour des variables U et V , sont encore valables pour des polynômes $U(\mathbf{X})$ et $V(\mathbf{X})$.

Constructions d'implications fortes

Définition 4 : Nous parlerons de construction d'une implication forte à partir d'autres implications fortes, lorsque nous avons un algorithme qui permet de construire la première à partir des autres.

Il s'agit donc d'une implication logique, au sens constructif, liant des implications fortes.

Notation : Nous noterons cette implication logique (au sens constructif) par le signe de déduction "constructif" : $\vdash_{cons}$

Par exemple nous explicitons un peu plus loin la construction qui prouve :

$$(\mathbb{H} \overset{fort}{\Rightarrow} \mathbb{H}' \text{ et } \mathbb{H}' \overset{fort}{\Rightarrow} \mathbb{H}'') \vdash_{cons} (\mathbb{H} \overset{fort}{\Rightarrow} \mathbb{H}'')$$

Comme autre exemple, nous pouvons énoncer le principe de substitution sous la forme:

$$(\mathbb{H}(X,W) \overset{fort}{\Rightarrow} \mathbb{H}'(X,W)) \vdash_{cons} (\mathbb{H}(X,P(X)) \overset{fort}{\Rightarrow} \mathbb{H}'(X,P(X)))$$

Quelques exemples de constructions d'implications fortes

Le raisonnement par séparation des cas (selon le signe d'un polynôme)

Lemme 5 : Soit $\mathbb{H}$ un système de csg portant sur des polynômes de $\mathbf{K}[X]$, Q un élément de $\mathbf{K}[X]$. Alors toute implication forte du type $(\mathbb{H} \overset{fort}{\Rightarrow} Q \tau 0)$ (où τ est $=$, $<$ ou $>$) fournit par relecture toute implication forte "plus faible" $(\mathbb{H} \overset{fort}{\Rightarrow} Q \tau' 0)$. Par exemple, on a:

$$(\mathbb{H} \overset{fort}{\Rightarrow} Q>0) \vdash_{cons} (\mathbb{H} \overset{fort}{\Rightarrow} Q\geqslant 0)$$

Proposition 6 : Soit $\mathbb{H}$ un système de csg portant sur des polynômes de $\mathbf{K}[X]$, Q un élément de $\mathbf{K}[X]$, alors:

$$((\mathbb{H} \overset{fort}{\Rightarrow} Q\leqslant 0) \text{ et } (\mathbb{H} \overset{fort}{\Rightarrow} Q\geqslant 0)) \vdash_{cons} (\mathbb{H} \overset{fort}{\Rightarrow} Q=0).$$

De même :

$$((\mathbb{H} \overset{fort}{\Rightarrow} Q\leqslant 0) \text{ et } (\mathbb{H} \overset{fort}{\Rightarrow} Q\neq 0)) \vdash_{cons} (\mathbb{H} \overset{fort}{\Rightarrow} Q<0)$$

$$\text{et } ((\mathbb{H} \overset{fort}{\Rightarrow} Q=0) \text{ et } (\mathbb{H} \overset{fort}{\Rightarrow} Q\neq 0)) \vdash_{cons} (\mathbb{H} \overset{fort}{\Rightarrow} 1=0)$$

Théorème 7 : (raisonnement cas par cas, selon le signe d'un polynôme)
Pour démontrer que $\mathbb{H}$ est fortement incompatible, on peut raisonner en séparant selon les 3 cas $Q>0$, $Q<0$, $Q=0$, et en construisant une incompatibilité forte dans chacun des 3 cas.

preuve> Le lemme 5 est une simple constatation à faire dans chaque cas.
Le théorème 7 est un corollaire de la proposition 6 .
Le lecteur voudra bien excuser le caractère un peu répétitif des 3 constructions qui suivent.

Voyons la première construction d'implication forte dans la proposition 6.
Notons : $F_>$, $F_\geq$, $F_=$, $F_\neq$ les 4 parties finies de $\mathbf{K}[X]$ contenant des polynômes auxquels sont attribués les conditions de signes >0 , $\geqslant 0$, $=0$, $\neq 0$ dans l'hypothèse $\mathbb{H}$.
L'hypothèse $\mathbb{H} \overset{fort}{\Rightarrow} Q\leqslant 0$ se réécrit $[\ \mathbb{H}\ ,\ Q>0\ ] \overset{fort}{\Rightarrow} 1=0$ et signifie qu'on a une égalité :

$S + P + Z = 0$ avec $S \in \mathcal{M}(F_>^{*2} \cup F_{\neq}^{*2} \cup \{Q^2\})$, $P \in Cp(F_{\geq} \cup F_> \cup \{Q\})$, $Z \in I(F_=)$
c.-à-d. encore :

$$Q^{2n}.S_1 + Q.P_1 + R_1 + Z_1 = 0 \text{ avec } S_1 \in \mathcal{M}(F_>^{*2} \cup F_{\neq}^{*2}),\ P_1, R_1 \in Cp(F_{\geq} \cup F_>),\ Z_1 \in I(F_=)$$

De même l'hypothèse $\mathbb{H} \overset{fort}{\Rightarrow} Q \geqslant 0$ signifie qu'on a une égalité :

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

On récrit les 2 égalités obtenues sous forme :

$-Q.P_1 = Q^{2n}.S_1 + R_1 + Z_1$ et $Q.P_2 = Q^{2m}.S_2 + R_2 + Z_2$ et on les multiplie :

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

d'où $Q^{2n+2m}.S_1.S_2 + V + W = 0$ avec :

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

ce qui est précisément l'implication forte cherchée: $(\mathbb{H} \overset{fort}{\Rightarrow} Q = 0)$.

Voyons maintenant la construction:

$$((\mathbb{H} \overset{fort}{\Rightarrow} Q \leqslant 0) \text{ et } (\mathbb{H} \overset{fort}{\Rightarrow} Q \neq 0)) \vdash_{cons} (\mathbb{H} \overset{fort}{\Rightarrow} Q < 0)$$

L'implication forte $(\mathbb{H} \overset{fort}{\Rightarrow} Q \leqslant 0)$ correspond à une équation :

$Q^{2m}.S_1 + Q.P_1 + R_1 + Z_1 = 0$ avec $S_1 \in \mathcal{M}(F_>^{*2} \cup F_{\neq}^{*2})$, $P_1, R_1 \in Cp(F_{\geq} \cup F_>)$, $Z_1 \in I(F_=)$

L'implication forte $(\mathbb{H} \overset{fort}{\Rightarrow} Q \neq 0)$ correspond à une équation :

$S_3 + P_3 + Q.Y_3 + Z_3 = 0$ avec $S_3 \in \mathcal{M}(F_>^{*2} \cup F_{\neq}^{*2})$, $P_3 \in Cp(F_{\geq} \cup F_>)$, $Z_3 \in I(F_=)$

équation qu'on réécrit $-Q.Y_3 = S_3 + P_3 + Z_3$

En élevant cette égalité à la puissance 2m on obtient $Q^{2m}.(Y_4)^2 = S_4 + P_4 + Z_4$ avec de nouveau $S_4 \in \mathcal{M}(F_>^{*2} \cup F_{\neq}^{*2})$, $P_4 \in Cp(F_{\geq} \cup F_>)$, $Z_4 \in I(F_=)$

On multiplie la première équation par $(Y_4)^2$ et la dernière par S_1 et on conclut :

$$S_1.S_4 + S_1.P_4 + S_1.Z_4 + Q.P_1.(Y_4)^2 . + R_1.(Y_4)^2 + Z_1.(Y_4)^2 = 0 \quad \text{avec}$$

$S_1.S_4 \in \mathcal{M}(F_>^{*2} \cup F_{\neq}^{*2})$, $P_1.(Y_4)^2$, $S_1.P_4 + R_1.(Y_4)^2 \in Cp(F_{\geq} \cup F_>)$,

$S_1.Z_4 + Z_1.(Y_4)^2 \in I(F_=)$ ce qui est bien l'implication forte cherchée : $(\mathbb{H} \overset{fort}{\Rightarrow} Q < 0)$

Voyons enfin la construction:

$$((\mathbb{H} \overset{fort}{\Rightarrow} Q = 0) \text{ et } (\mathbb{H} \overset{fort}{\Rightarrow} Q \neq 0)) \vdash_{cons} (\mathbb{H} \overset{fort}{\Rightarrow} 1 = 0)$$

L'implication forte $(\mathbb{H} \overset{fort}{\Rightarrow} Q = 0)$ correspond à une équation :

$Q^{2m}.S_1 + P_1 + Z_1 = 0$ avec $S_1 \in \mathcal{M}(F_>^{*2} \cup F_{\neq}^{*2})$, $P_1 \in Cp(F_{\geq} \cup F_>)$, $Z_1 \in I(F_=)$

L'implication forte $(\mathbb{H} \overset{fort}{\Rightarrow} Q \neq 0)$ correspond à une équation :

$S_3 + P_3 + Q.Y_3 + Z_3 = 0$ avec $S_3 \in \mathcal{M}(F_>^{*2} \cup F_{\neq}^{*2})$, $P_3 \in Cp(F_{\geq} \cup F_>)$, $Z_3 \in I(F_=)$

équation qu'on réécrit $-Q.Y_3 = S_3 + P_3 + Z_3$

En élevant cette égalité à la puissance 2m on obtient $Q^{2m}.(Y_4)^2 = S_4 + P_4 + Z_4$ avec de nouveau $S_4 \in \mathcal{M}(F_>^{*2} \cup F_{\neq}^{*2})$, $P_4 \in Cp(F_{\geq} \cup F_>)$, $Z_4 \in I(F_=)$

On multiplie la première équation par $(Y_4)^2$ et la dernière par S_1 et on conclut :

$$S_1.S_4 + S_1.P_4 + S_1.Z_4 + P_1.(Y_4)^2 + Z_1.(Y_4)^2 = 0 \quad \text{avec}$$

$S_1.S_4 \in \mathcal{M}(F_>^{*2} \cup F_{\neq}^{*2})$, $P_1.(Y_4)^2$, $S_1.P_4 + R_1.(Y_4)^2 \in Cp(F_{\geq} \cup F_>)$, $S_1.Z_4 + Z_1.(Y_4)^2 \in I(F_=)$ ce qui est bien l'implication forte cherchée ❑

Transitivité des implications fortes

Théorème 8 :

Soient $\mathbb{H}$, $\mathbb{H}'$, $\mathbb{H}''$ trois systèmes de csg portant sur des polynômes de $\mathbf{K[X]}$.

Alors: $\{ (\mathbb{H} \overset{fort}{\Rightarrow} \mathbb{H}') \text{ et } ([\mathbb{H} , \mathbb{H}'] \overset{fort}{\Rightarrow} \mathbb{H}'') \} \vdash_{cons} (\mathbb{H} \overset{fort}{\Rightarrow} \mathbb{H}'')$

preuve> Il suffit d'enlever une à une les hypothèses de $\mathbb{H}'$ dans $(\mathbb{H} , \mathbb{H}') \overset{fort}{\Rightarrow} \mathbb{H}''$. Donc on peut supposer que $\mathbb{H}'$ contient une unique hypothèse $Q \tau 0$. Il suffit donc de montrer que si on a deux implications fortes $\mathbb{H} \overset{fort}{\Rightarrow} Q \tau 0$, et $[\mathbb{H} , Q \tau 0 , A] \overset{fort}{\Rightarrow} 1 = 0$, alors on peut construire l'implication forte $[\mathbb{H} , A] \overset{fort}{\Rightarrow} 1 = 0$ (où A est une csg portant sur un polynôme). Or cela peut se faire cas par cas selon le signe de Q . ❑

En combinant la transitivité des implications fortes et les implications fortes triviales, on obtient autant de corollaires, par exemple:

Corollaire : $(\mathbb{H} \overset{fort}{\Rightarrow} [P.Q > 0 , Q \geqslant 0]) \vdash_{cons} (\mathbb{H} \overset{fort}{\Rightarrow} P > 0)$

Formules de Taylor mixtes (l'évidence forte du lemme de Thom)

On considère deux variables U et V et on pose $\Delta := U - V$. On considère un polynôme P à coefficients dans un corps ordonné $\mathbf{K}$ ou *plus généralement dans un anneau commutatif* $\mathbf{A}$ *qui est une* $\mathbb{Q}$*-algèbre.*

Si $\deg(P) = 1$, la formule de Taylor est simplement :

$$P(U) - P(V) = \Delta.P'$$

Elle relie sous forme d'une évidence forte le signe de $P(U) - P(V)$ et celui de $\Delta.P'$.

Si $\deg(P) \leqslant 2$, la formule de Taylor précédente se scinde en 2 selon que l'on met $P'(U)$ ou $P'(V)$:

$$P(U) - P(V) = \Delta.P'(V) + (1/2).\Delta^2.P''$$
$$P(U) - P(V) = \Delta.P'(U) - (1/2).\Delta^2.P''$$

Supposons maintenant que U et V "attribuent un même signe strict" σ à P' , alors, quel que soient les signes de Δ et P'' , on a l'évidence forte que $P(U) - P(V)$ et $\Delta.\sigma$ ont le même signe, fournie par l'une des deux formules de Taylor.

Si $\deg(P) \leqslant 3$, chaque formule de Taylor mixte précédente se scinde en 2 selon que l'on met $P''(U)$ ou $P''(V)$ et on a les 4 formules de Taylor mixtes suivantes[1]:

$$P(U) - P(V) = \Delta.P'(V) + (1/2).\Delta^2.P''(V) + (1/6).\Delta^3.P^{(3)}$$
$$P(U) - P(V) = \Delta.P'(V) + (1/2).\Delta^2.P''(U) - (1/3).\Delta^3.P^{(3)}$$
$$P(U) - P(V) = \Delta.P'(U) - (1/2).\Delta^2.P''(V) - (1/3).\Delta^3.P^{(3)}$$
$$P(U) - P(V) = \Delta.P'(U) - (1/2).\Delta^2.P''(U) + (1/6).\Delta^3.P^{(3)}$$

Supposons maintenant que U et V "attribuent un même signe strict" σ à P' , et un même signe strict σ'' à P'' . Alors, chaque fois qu'on attribue un signe à Δ et à $P^{(3)}$, l'une des 4 formules de Taylor mixtes constitue une évidence forte que $P(U) - P(V)$ et $\Delta.\sigma$ ont le même signe. Par exemple, si $\sigma = +1$, $\sigma'' = -1$ et si $\Delta > 0$, $P^{(3)} < 0$, la troisième formule de Taylor mixte peut se relire :

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

---

[1] Pour le prouver on peut prendre $V = 0$, puis vérifier pour le polynôme U^3 puisqu'elles sont vraies pour les polynômes de degré $\leqslant 2$.

Inversement ces formules de Taylor mixtes fournissent aussi l'évidence forte pour déduire le signe de Δ du signe de $P(U) - P(V)$. En particulier, elles fournissent l'évidence forte que deux racines de P codées à la Thom sont égales si le codage est le même.

Si $\deg(P) \leqslant 4$, chaque formule de Taylor mixte précédente se scinde en 2 selon que l'on met $P^{(3)}(U)$ ou $P^{(3)}(V)$ et on a les 8 formules de Taylor mixtes suivantes[1]:

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

Comme toutes les combinaisons de signes possibles se présentent, on obtient : si U et V n'attribuent pas la même suite de signes à un polynôme P de degré ≤ 4 et à ses dérivées successives, alors on a l'évidence forte qui permet de déduire à partir de ces hypothèses le signe de $U - V$: la formule de Taylor mixte à utiliser est avec $P^{(i)}$ ($i = 0, 1, 2,$ ou 3) où i est le dernier indice pour lequel les deux signes ne sont pas identiques. On en déduit alors sans trop de problème l'évidence forte de tous les faits énoncés dans le lemme de Thom.

Théorème 9 : (formule de Taylor mixte)

Pour chaque degré d , il y a 2^{d-1} formules de Taylor mixtes et toutes les combinaisons de signes possibles apparaissent.

preuve> Le mieux serait de trouver un argument "direct" qui montre que le scindage introduit le même signe pour le dernier terme et l'avant dernier terme si on a mis V dans l'avant dernier terme, et des signes distincts si on a mis U dans l'avant dernier terme. La preuve la plus naturelle est sans doute la preuve basée sur une utilisation récurrente du théorème des accroissements finis (version constructive), mais ce n'est pas très folichon. Esquissons la pour le degré 4 : supposons qu'on veuille établir la sixième formule de Taylor mixte donnée ci-dessus; le théorème des accroissements finis pour le degré 4 donne une formule :

$$P(U) - P(V) = (\Delta/6)\ (2.P'(U/6 + 5V/6) + P'(U/3 + 2V/3) + ... + ...)$$
$$= (\Delta/6)\ (2.P'(U_1) + P'(U_2) + P'(U_3) + 2.P'(U_4))$$

Pour chacun des $P'(U_i)$ on peut écrire une formule des accroissements finis en degré 3.

$$P'(U_i) = P'(U) + (U_i - U)\ (r_1.P''(U_{i,1}) + r_2.P''(U_{i,2}) + r_3.P''(U_{i,3}))$$
$$= P'(U) - c_i\ \Delta\ (r_1.P''(U_{i,1}) + r_2.P''(U_{i,2}) + r_3.P''(U_{i,3}))$$

où les c_i et et r_j sont des rationnels positifs et les $U_{i,j}$ sont spécifiés comme barycentres à coefficients rationnels positifs de U et U_i.

En substituant les $P'(U_i)$ dans la première égalité il vient une égalité (1) du genre:

$$P(U) - P(V) = \gamma_1\ \Delta\ P'(U) - \Delta^2 \sum_{i,j} r_{i,j}\ P''(U_{i,j}) \quad \text{avec } \gamma_1 \text{ et les } r_{i,j} \text{ rationnels positifs}$$

On écrit maintenant pour chaque $P''(U_{i,j})$ une formule des accroissements finis en degré 2.

$$P''(U_{i,j}) = P''(V) + (U_{i,j} - V)\ (s_1.P^{(3)}(U_{i,j,1}) + s_2.P^{(3)}(U_{i,j,2}))$$
$$= P''(V) + c_{i,j}\ \Delta\ (s_1.P^{(3)}(U_{i,j,1}) + s_2.P^{(3)}(U_{i,j,2}))$$

En substituant les $P''(U_{i,j})$ dans l'égalité (1) il vient une égalité du genre:

---

[1] Même preuve, en vérifiant pour U^4 .

$P(U) - P(V) = \gamma_1 \Delta P'(U) - \gamma_2 \Delta^2 P''(V) - \Delta^3 \sum_{i,j,k} r_{i,j,k} P^{(3)}(U_{i,j,k})$ avec γ_1 , γ_2 et les $r_{i,j,k}$ rationnels positifs. etc...

Dans le cas général, on peut mener le calcul de manière à obtenir pour chaque $P^{(i)}$, au choix $P^{(i)}(U)$ ou $P^{(i)}(V)$, et la règle pour le signe du coefficient de $\Delta^i P^{(i)}$ est qu'il est le même ou l'opposé de celui de $\Delta^{i-1} P^{(i-1)}$ selon qu'on a choisi de construire une formule de Taylor mixte avec $\Delta^{i-1} P^{(i-1)}(V)$ ou avec $\Delta^{i-1} P^{(i-1)}(U)$ ❑

Théorème 10 : (évidence forte du lemme de Thom)

Soit $P \in \mathbf{K}[X][T]$, de degré d en T , $\sigma_1, \sigma_2, ..., \sigma_d$ une liste de signes stricts.

On note $\mathbb{H}$ le système de csg : $P'(X,U) \equiv \sigma_1$, ..., $P^{(i)}(X,U) \equiv \sigma_i$, ..., $P^{(d)}(X,U) \equiv \sigma_d$, $P'(X,V) \equiv \sigma_1$, ..., $P^{(i)}(X,V) \equiv \sigma_i$, ..., $P^{(d)}(X,V) \equiv \sigma_d$ (dérivées par rapport à T) .

On a alors les évidences fortes suivantes :

$[\, \mathbb{H} , P(X,U) = P(X,V) \,] \overset{fort}{\Rightarrow} U = V$ (a)

$[\, \mathbb{H} , P(X,U) > P(X,V) \,] \overset{fort}{\Rightarrow} U - V \equiv \sigma_1$ (b)

$[\, \mathbb{H} , U - V \equiv \sigma_1 \,] \overset{fort}{\Rightarrow} P(X,U) > P(X,V)$ (c)

$[\, \mathbb{H} , (W - U).(W - V) \leqslant 0 \,] \overset{fort}{\Rightarrow} P^{(i)}(X,W) \equiv \sigma_i \quad (i = 1,...,d)$ (d)

$[\, \mathbb{H} , P^{(i)}(X,W) \not\equiv \sigma_i \,] \overset{fort}{\Rightarrow} (W - U).(W - V) > 0 \quad (i = 1,...,d)$ (e)

Soit par ailleurs $\mathbb{H}'$ le système de csg obtenu à partir de $\mathbb{H}$ en relachant toutes les conditions de signe sauf celles relatives à $P^{(d)}$. On a alors l'évidence forte suivante :

$[\, \mathbb{H}' , U < W < V \,] \overset{fort}{\Rightarrow} P^{(i)}(X,W) \equiv \sigma_i \quad (i = 1,...,d)$ (f)

preuve> (a), (b), (c) sont donnés par une formule de Taylor mixte pour P .

(d) et (e) sont identiques. (d) se démontre de proche en proche, pour i décroissant de d à 1 , en utilisant pour la dérivée i-ème une formule de Taylor mixte pour $P^{(i)}$, et en faisant appel à la transitivité des implications fortes.

(f) se démontre comme (d) : le fait de supposer $P^{(d)}$ avec un signe strict permet d'avoir un terme qui assure le signe strict de $P^{(i)}(X,W)$ lorsqu'on utilise une formule de Taylor mixte relative à $P^{(i)}$. ❑

On remarquera que le (b) permet de rendre fortement évident le signe de $u - v$ lorsque u est un élément de **R** codé à la Thom dans **K** et v un élément de **K** .

On notera que le théorème 10 ne capture pas l'intégralité du lemme de Thom sous forme d'évidence forte : il manque les affirmations concernant les bornes de l'intervalle. Ce trou sera rempli au paragraphe sur les tableaux de Hormander, et nécessite la notion d'existence potentielle.

3) Existence potentielle

Notations et définitions

Une implication forte $\mathbb{H} \overset{fort}{\Rightarrow} \mathbb{H}'$ est une forme forte (par identité algébrique) pour l'implication *universelle* correspondante : $\forall X\ (\ \mathbb{H} \Rightarrow \mathbb{H}'\ )$.
Mais la théorie des corps réels clos a des axiomes qui ne sont pas purement universels. Aussi, nous avons besoin d'une forme "stellensatzisée" pour les énoncés du genre :

$$\forall X\ \exists T\quad \mathbb{H}(X,T)\ .$$

Nous voudrions parler d'existence potentielle lorsqu'un système de csg n'est pas fortement incompatible.
En fait, nous voulons un peu mieux. La non impossibilité de l'équation $P(X) = T^2$ prise isolément n'a pas le même statut que la non impossibilité de l'équation $P(X)^2 = T^4$. En effet, dans le second cas, contrairement au premier, quelles que soient les hypothèses faites par ailleurs sur X, le fait de rajouter l'équation ne peut introduire une contradiction. Cette distinction est traduite en logique par une alternance de quantificateurs:

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

Définition 11 :

Soient $\mathbb{H}_1$ un système de csg portant sur des polynômes de $\mathbf{K}[X]$, $\mathbb{H}_2$ un système de csg portant sur des polynômes de $\mathbf{K}[X,T_1,T_2,...,T_m] = \mathbf{K}[X,T]$.

Nous dirons que *les hypothèses* $\mathbb{H}_1$ *autorisent l'existence des* T_i *vérifiant* $\mathbb{H}_2$ lorsque, pour tout système de csg $\mathbb{H}$ portant sur des polynômes de $\mathbf{K}[X,Y]$, on a la construction d'implication forte :

$$(\ [\ \mathbb{H}_2(X,T)\ ,\ \mathbb{H}(X,Y)\ ]\ \overset{fort}{\Rightarrow}\ 1=0\ )\ \underset{cons}{\vdash}\ (\ [\ \mathbb{H}_1(X)\ ,\ \mathbb{H}(X,Y)\ ]\ \overset{fort}{\Rightarrow}\ 1=0\ ).$$

Nous parlerons également *d'existence potentielle des* T_i *vérifiant* $\mathbb{H}_2$ *sous les hypothèses* $\mathbb{H}_1$

NB: La condition sur $\mathbb{H}$ est qu'aucune des variables $T_1, T_2, ..., T_m$ ne figure dedans; mais d'autres variables que $X_1, X_2, ..., X_n$ peuvent y figurer, d'où le $\mathbf{K}[X,Y]$.

Notation : Nous noterons cette existence potentielle par : $\mathbb{H}_1 \longrightarrow \tilde{\exists} T\ \ \mathbb{H}_2$.

Nous pouvons préciser de plus les variables sur lesquelles portent les systèmes de csg, nous écrivons alors : $\mathbb{H}_1(X) \longrightarrow \tilde{\exists} T\ \ \mathbb{H}_2(X,T)$.

Lorsque le système $\mathbb{H}_1$ est vide, nous utiliserons la notation $\tilde{\exists} T\quad \mathbb{H}_2$.

Par exemple, nous montrons plus loin qu'on a :

$$P(X,U).P(X,V) < 0 \longrightarrow \tilde{\exists}\ W\ P(X,W) = 0$$

On notera que le principe de substitution énoncé au paragraphe précédent peut se réécrire sous la forme :

$$\mathbb{H}(X,P(X)) \longrightarrow \tilde{\exists} W\ \ \mathbb{H}(X,W)$$

Remarques : 1) Tout d'abord, nous insistons sur la lecture constructive de la définition ci-dessus: la construction d'implication forte doit être fournie par un procédé algorithmique uniforme.

2) La notation doit être lue comme un bloc indissociable (contrairement à la notation concernant les constructions d'implications fortes).

3) Si $\mathbf{L}$ est une extension ordonnée de $\mathbf{K}$ il n'y a pas de relation évidente a priori entre un énoncé $\mathbb{H}_1(X) \longrightarrow \tilde{\exists} T\ \ \mathbb{H}_2(X,T)$ lu dans $\mathbf{K}$ et le même énoncé lu dans $\mathbf{L}$. En fait, une fois démonté le théorème des zéros réels, il est clair que les deux énoncés

sont équivalents à l'énoncé $\forall X (H_1(X) \Rightarrow \exists T\ H_2(X,T))$ *lu dans la clôture ordonnée de* **K** .

4) Si nous appliquons la définition en prenant H_1 , H à la place de H , on obtient la construction d'implication forte :

$$([H_2 , H_1 , H] \overset{fort}{\Rightarrow} 1=0) \underset{cons}{\vdash} ([H_1 , H] \overset{fort}{\Rightarrow} 1=0)$$

5) Si nous appliquons la construction précédente plusieurs fois, nous obtenons que pour tout système de csg H' portant sur des polynômes de $\mathbf{K[X,Y]}$, on a :

$$([H_2 , H_1 , H] \overset{fort}{\Rightarrow} H') \underset{cons}{\vdash} ([H_1 , H] \overset{fort}{\Rightarrow} H')$$

Quelques règles de manipulation des énoncés d'existence potentielle

Des règles que nous allons énoncer, seule la règle de substitution n'est pas immédiate. Elles s'avèrent toutes bien utiles pour simplifier l'exposé.

Lemme 12 : Une existence potentielle $H_1(X) \longrightarrow \tilde{\exists} T\ H_2(X,T)$ reste vraie si on affaiblit la conclusion, si on renforce l'hypothèse, ou si on supprime derrière $\tilde{\exists}$ des variables ne figurant pas dans $H_2(X,T)$.

Proposition 13 : (renforcement simultané de l'hypothèse et de la conclusion)

Si $H_1(X) \longrightarrow \tilde{\exists} T\ H_2(X,T)$ **alors**

$$[H_1(X) , H_3(X)] \longrightarrow \tilde{\exists} T\ [H_2(X,T) , H_3(X)]$$

(rappel de l'hypothèse dans la conclusion)

Si $H_1(X) \longrightarrow \tilde{\exists} T\ H_2(X,T)$ **alors** $H_1(X) \longrightarrow \tilde{\exists} T\ [H_2(X,T) , H_1(X)]$

preuve> immédiat, le 2ème point était l'objet de la remarque 4 ❑

Proposition 14 : (existence potentielle comme généralisation de l'implication forte)

Supposons que les systèmes de csg H_1 et H_2 portent sur les variables X .

Alors $H_1(X) \longrightarrow \tilde{\exists} T\ H_2(X)$ **si et seulement si** $H_1(X) \overset{fort}{\Rightarrow} H_2(X)$.

preuve> Voyons le seulement si: soit $Q\ \tau\ 0$ une csg dans H_2 et soit $Q\ \tau'\ 0$ la csg opposée. On a $[H_2(X), Q\ \tau'\ 0] \overset{fort}{\Rightarrow} 1 = 0$. Donc, par l'existence potentielle, on a également $[H_1(X), Q\ \tau'\ 0] \overset{fort}{\Rightarrow} 1 = 0$, c.-à-d. $H_1(X) \overset{fort}{\Rightarrow} Q\tau 0$.

Voyons l'implication dans l'autre sens. Soit $H(X,Y)$ un système de csg et supposons que $[H_2(X), H(X,Y)] \overset{fort}{\Rightarrow} 1 = 0$. D'après l'hypothèse, on a évidemment :

$[H_1(X), H(X,Y)] \overset{fort}{\Rightarrow} [H_2(X), H(X,Y)]$. Il suffit d'appliquer la transitivité des implications fortes pour obtenir $[H_1(X), H(X,Y)] \overset{fort}{\Rightarrow} 1=0$. ❑

Proposition 15 : (raisonnement cas par cas)

Soit Q un polynôme de $\mathbf{K[X]}$. Pour démontrer une existence potentielle

$H_1(X) \longrightarrow \tilde{\exists} T\ H_2(X,T)$ il suffit de démontrer chacune des existences potentielles

$[H_1(X) , Q \equiv \sigma] \longrightarrow \tilde{\exists} T\ H_2(X,T)$ pour les 3 signes σ possibles.

preuve> Immédiat d'après les définitions et le théorème 7 . ❑

Proposition 16 : (l'existence implique l'existence potentielle)

Soient $P_1,P_2,...,P_m \in \mathbf{K[X]}$ et notons $\mathbf{P(X)}$ pour $P_1(\mathbf{X}), ..., P_m(\mathbf{X})$.

Si $\mathbb{H}_1(\mathbf{X}) \overset{fort}{\Rightarrow} \mathbb{H}_2(\mathbf{X},\mathbf{P(X)})$ **alors** $\mathbb{H}_1(\mathbf{X}) \longrightarrow \tilde{\exists}\,\mathbf{T}\ \mathbb{H}_2(\mathbf{X},\mathbf{T})$

preuve> immédiat : si $[\,\mathbb{H}_2(\mathbf{X},\mathbf{T}),\ \mathbb{H}(\mathbf{X},\mathbf{Y})\,] \overset{fort}{\Rightarrow} 1=0$, on obtient par substitution $[\,\mathbb{H}_2(\mathbf{X},\mathbf{P(X)}),\ \mathbb{H}(\mathbf{X},\mathbf{Y})\,] \overset{fort}{\Rightarrow} 1=0$ puis par transitivité des implications fortes: $[\,\mathbb{H}_1(\mathbf{X}),\ \mathbb{H}(\mathbf{X},\mathbf{Y})\,] \overset{fort}{\Rightarrow} 1=0$ ❑

Théorème 17 : (transitivité dans les existences potentielles)

On considère des variables $X_1,X_2,...,X_n$, $T_1,T_2,...,T_m$, $U_1,U_2,...,U_k$ et des systèmes de csg $\mathbb{H}_1(\mathbf{X})$, $\mathbb{H}_2(\mathbf{X},\mathbf{T})$ et $\mathbb{H}_3(\mathbf{X},\mathbf{T},\mathbf{U})$.

Si on a $\mathbb{H}_1(\mathbf{X}) \longrightarrow \tilde{\exists}\,\mathbf{T}\ \mathbb{H}_2(\mathbf{X},\mathbf{T})$ et $\mathbb{H}_2(\mathbf{X},\mathbf{T}) \longrightarrow \tilde{\exists}\,\mathbf{U}\ \mathbb{H}_3(\mathbf{X},\mathbf{T},\mathbf{U})$

alors on a aussi:

$$\mathbb{H}_1(\mathbf{X}) \longrightarrow \tilde{\exists}\,\mathbf{T},\mathbf{U}\ [\,\mathbb{H}_1(\mathbf{X})\ ,\ \mathbb{H}_2(\mathbf{X},\mathbf{T})\ ,\ \mathbb{H}_3(\mathbf{X},\mathbf{T},\mathbf{U})\,]$$

preuve> Immédiat d'après la définition. ❑

Remarque 6 : En combinant le théorème précédent et la proposition 14, on obtient des variantes. Une implication forte suivie d'une existence potentielle donne une existence potentielle. Une existence potentielle suivie d'une implication forte donne une existence potentielle.

Théorème 18 : (principe de substitution dans les existences potentielles)

On considère des variables $X_1,X_2,...,X_n$, $Z_1,Z_2,...,Z_k$,$T_1,T_2,...,T_m$, et des polynômes $P_1,P_2,...,P_n$ de $\mathbf{K[Z]}$. Notons $\mathbf{P(Z)}$ pour $P_1(\mathbf{Z}), ..., P_n(\mathbf{Z})$.

Si on a $\mathbb{H}_1(\mathbf{X}) \longrightarrow \tilde{\exists}\,\mathbf{T}\ \mathbb{H}_2(\mathbf{X},\mathbf{T})$ (a)

alors on a aussi $\mathbb{H}_1(\mathbf{P(Z)}) \longrightarrow \tilde{\exists}\,\mathbf{T}\ \mathbb{H}_2(\mathbf{P(Z)},\mathbf{T})$ (b)

preuve> Supposons qu'on ait

$$[\,\mathbb{H}_2(\mathbf{P(Z)},\mathbf{T})\ ,\ \mathbb{H}(\mathbf{Z},\mathbf{Y})\,] \overset{fort}{\Rightarrow} 1=0 \qquad (1)$$

On veut construire

$$[\,\mathbb{H}_1(\mathbf{P(Z)})\ ,\ \mathbb{H}(\mathbf{Z},\mathbf{Y})\,] \overset{fort}{\Rightarrow} 1=0 \qquad (2)$$

On a : $[\,\mathbb{H}_2(\mathbf{X},\mathbf{T})\ ,\ \mathbb{H}(\mathbf{Z},\mathbf{Y})\ ,\ \mathbf{X}=\mathbf{P(Z)}\,] \overset{fort}{\Rightarrow} [\,\mathbb{H}_2(\mathbf{P(Z)},\mathbf{T})\ ,\ \mathbb{H}(\mathbf{Z},\mathbf{Y})\,]$ (3)

Par transitivité (1) et (3) donnent :

$$[\,\mathbb{H}_2(\mathbf{X},\mathbf{T})\ ,\ \mathbb{H}(\mathbf{Z},\mathbf{Y})\ ,\ \mathbf{X}=\mathbf{P(Z)}\,] \overset{fort}{\Rightarrow} 1=0 \qquad (4)$$

Par définition de l'existence potentielle on sait construire:

$$[\,\mathbb{H}_1(\mathbf{X})\ ,\ \mathbb{H}(\mathbf{Z},\mathbf{Y})\ ,\ \mathbf{X}=\mathbf{P(Z)}\,] \overset{fort}{\Rightarrow} 1=0 \qquad (5)$$

Par ailleurs :

$$[\,\mathbb{H}_1(\mathbf{P(Z)})\ ,\ \mathbb{H}(\mathbf{Z},\mathbf{Y})\ ,\ \mathbf{X}=\mathbf{P(Z)}\,] \overset{fort}{\Rightarrow} [\,\mathbb{H}_1(\mathbf{X})\ ,\ \mathbb{H}(\mathbf{Z},\mathbf{Y})\ ,\ \mathbf{X}=\mathbf{P(Z)}\,] \qquad (6)$$

Par transitivité (5) et (6) donnent :

$$[\,\mathbb{H}_1(\mathbf{P(Z)})\ ,\ \mathbb{H}(\mathbf{Z},\mathbf{Y})\ ,\ \mathbf{X}=\mathbf{P(Z)}\,] \overset{fort}{\Rightarrow} 1=0 \qquad (7)$$

En substituant $\mathbf{P(Z)}$ à $\mathbf{X}$ dans (7) , on obtient (2) ❑

Remarque 7 : Les preuves d'existence potentielle peuvent en général être données directement sous la forme (b). Le théorème 18 permet seulement d'y voir plus clair en énonçant les théorèmes d'existence potentielle sous la forme la plus simple.

Remarque 8 : Si on applique le théorème 18 une nouvelle fois, on peut substituer certains des X_j à certains des Z_i . On voit donc que l'hypothèse selon laquelle les X_j et les Z_i sont des variables distinctes est en fait inutile.

Existences potentielles fondamentales

Théorème 19 : (autorisation de rajouter la racine carrée d'un positif)

On a l'existence potentielle de la racine carrée d'un positif. Ce qui s'écrit:

$$U \geqslant 0 \longrightarrow \tilde{\exists} T \quad U = T^2$$

preuve> *On supposera, ce qui n'est pas restrictif, que* U *est la variable* X_n .
On considère un système de csg $\mathbb{H}(\mathbf{X})$ et on reprend les notations de la preuve de la proposition 6.
On notera Cp', I' lorsqu'on considère le cône positif ou l'idéal engendré dans l'anneau des polynômes avec la variable supplémentaire T : $\mathbf{K}[\mathbf{X},T] = \mathbf{K}[X_1,X_2,...,X_n,T]$.

On veut expliciter la construction:
$([\mathbb{H}, U - T^2 = 0] \overset{fort}{\Rightarrow} 1 = 0) \underset{cons}{\vdash} ([\mathbb{H}, U \geqslant 0] \overset{fort}{\Rightarrow} 1 = 0))$.
L'hypothèse correspond à une équation :
$S_1(\mathbf{X}) + P_1(\mathbf{X},T) + (U - T^2).Y_1(\mathbf{X},T) + Z_1(\mathbf{X},T) = 0$ avec $S_1 \in \mathcal{M}(F_>^{*2} \cup F_{\neq}^{*2})$, $P_1 \in Cp'(F_{\geq} \cup F_>)$, $Z_1 \in I'(F_=)$.
Plus précisément

$$P_1 = \sum_{i=1}^{h} Q_i(\mathbf{X}).V_i^2(\mathbf{X},T) \quad \text{et} \quad Z_1 = \sum_{j=1}^{r} N_j(\mathbf{X}).W_j(\mathbf{X},T)$$

avec $Q_i(\mathbf{X}) \in Cp(F_{\geq} \cup F_>)$ et $N_j(\mathbf{X}) \in F_=$. Les polynômes $V_i(\mathbf{X},T)$ et $W_j(\mathbf{X},T)$ peuvent être pris modulo $U - T^2$ (ce qui modifie $Y_1(\mathbf{X},T)$), et sont alors de degré ≤ 1 en T .
Si $V_i(\mathbf{X},T) = A_i(\mathbf{X}) + B_i(\mathbf{X}).T$, $W_j(\mathbf{X},T) = C_j(\mathbf{X}) + D_j(\mathbf{X}).T$, on a :
$V_i^2(\mathbf{X},T)) = A_i^2(\mathbf{X}) + B_i^2(\mathbf{X}).T^2 + 2.A_i(\mathbf{X}).B_i(\mathbf{X}).T$, et comme T^2 peut être remplacé par U modulo $U - T^2$ on obtient :

$$S_1(\mathbf{X}) + \sum_{i=1}^{h} Q_i(\mathbf{X}).(A_i^2(\mathbf{X}) + 2.A_i(\mathbf{X}).B_i(\mathbf{X}).T + B_i^2(\mathbf{X}).U) +$$

$$(U - T^2).Y_2(\mathbf{X},T) + \sum_{j=1}^{r} N_j(\mathbf{X}).(C_j(\mathbf{X}) + D_j(\mathbf{X}).T) = 0$$

Considérons le polynôme du premier membre comme un élément de $\mathbf{K}[X_1,X_2,...,X_n][T]$. Si $Y_2(\mathbf{X},T)$ n'était pas nul, le monôme dominant en T du polynôme $-T^2.Y_2(\mathbf{X},T)$ serait aussi le monôme dominant en T du polynôme du premier membre. Donc $Y_2(\mathbf{X},T) = 0$. On écrit alors que le coefficient constant du polynôme restant est nul :

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

Ceci est exactement une implication forte du type voulu. ❑

Théorème 20 : (autorisation de rajouter l'inverse d'un non nul)

On a l'existence potentielle de l'inverse d'un non nul. Ce qui s'écrit:

$$U \neq 0 \longrightarrow \tilde{\exists} T \quad 1 = U.T$$

preuve> Mêmes notations qu'au théorème précédent. On veut expliciter la construction:
$([\mathbb{H}, 1 - U.T = 0] \overset{fort}{\Rightarrow} 1 = 0) \underset{cons}{\vdash} ([\mathbb{H}, U \neq 0] \overset{fort}{\Rightarrow} 1 = 0))$.

L'hypothèse correspond à une équation :

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

Travaillons modulo $(1 - U.T)$. Remplaçons dans les V_i et les W_j partout T par $1/U$ de manière à y faire disparaître T, puis multiplions le tout par une puissance U^{2m} convenable de manière à chasser les dénominateurs (la puissance est paire à cause de V_i^2) . On obtient:

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

Comme dans la preuve précédente, $Y_2(X,T) = 0$. Et l'annulation du polynôme restant nous donne une incompatibilité forte du type cherché:

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

Remarque 9 : On notera que les théorèmes 19 et 20 "donnent l'autorisation" de rajouter la ou les racines d'une équation de degré 1 ou 2 .

Corollaire 1 : (autorisation de rajouter l'inverse de la racine carrée d'un strictement positif)

On a l'existence potentielle de l'inverse d'un non nul. Ce qui s'écrit:

$$U > 0 \longrightarrow \tilde{\exists} T \quad 1 = U.T^2$$

preuve> $U \geqslant 0 \longrightarrow \tilde{\exists} W \quad U = W^2$ d'après le théorème 19 .

Par ailleurs $[\, U > 0 , U = W^2 \,] \overset{forl}{\Rightarrow} W \neq 0$ donc par transitivité :

$U > 0 \longrightarrow \tilde{\exists} W \quad [\, U = W^2 , W \neq 0 \,]$

Par ailleurs $W \neq 0 \longrightarrow \tilde{\exists} T \quad 1 = W.T$ d'après le théorème 20, donc par transitivité : $U > 0 \longrightarrow \tilde{\exists} W, T \quad [\, U = W^2 , W \neq 0 , 1 = W.T \,]$

Enfin $[\, U = W^2 , 1 = W.T \,] \overset{forl}{\Rightarrow} 1 = U.T^2$ donc par transitivité :

$U > 0 \longrightarrow \tilde{\exists} W, T \quad [\, U = W^2 , W \neq 0 , 1 = W.T , 1 = U.T^2 \,]$

et a fortiori $U > 0 \longrightarrow \tilde{\exists} T \quad 1 = U.T^2$ $\square$

Corollaire 2 : (le nullstellensatz réel faible implique les autres stellensatz réels)

Supposons que pour tout entier n et tout système d'égalités à 0 portant sur des polynômes de $\mathbf{K}[X]$, l'impossibilité dans $\mathbf{R}$ (clôture réelle de $\mathbf{K}$) implique l'incompatibilité forte dans $\mathbf{K}$. Alors, pour tout système de csg portant sur des polynômes de $\mathbf{K}[X]$, l'impossibilité dans $\mathbf{R}$ implique l'incompatibilité forte dans $\mathbf{K}$.

preuve> Considérons un système de csg portant sur des polynômes de $\mathbf{K}[X]$. Si on a une csg $P \geqslant 0$ on la remplace par $P - T_P^2 = 0$ (la variable T_P est une nouvelle variable). Si on a une csg $Q > 0$ on la remplace par $1 - Q.T_Q^2 = 0$. Si on a une csg $R \neq 0$ on la remplace par $1 - R.T_R = 0$. Toutes les csg sont donc maintenant des égalités à 0 . On en déduit une incompatibilité forte sur ces nouvelles csg . Il faut ensuite en déduire une incompatibilité forte sur les csg initiales . Cela se fait une csg après l'autre. On peut donc supposer qu'il n'y a qu'une csg à traiter. Trois cas se présentent selon le type de la csg.

Or l'élimination de la csg (vu le théorème de substitution) résulte de l'existence potentielle correspondante:

$U \geqslant 0 \longrightarrow \tilde{\exists} T \quad U = T^2$ permet de remplacer $P - T_P^2 = 0$ par $P \geqslant 0$ (théorème 19)

$U>0 \longrightarrow \widetilde{\exists} T \quad 1 = U.T^2$ permet de remplacer $1 - Q.T_Q{}^2 = 0$ par $Q>0$ (corollaire 1)
$U \neq 0 \longrightarrow \widetilde{\exists} T \quad 1 = U.T$ permet de remplacer $1 - R.T_R = 0$ par $R \neq 0$ (théorème 20) ❑

Théorème 21 : (autorisation de rajouter une racine à un polynôme qui change de signe)
On a l'existence potentielle d'une racine pour un polynôme qui change de signe. Ce qui s'écrit : $P(X,U).P(X,V) \lessdot 0 \longrightarrow \widetilde{\exists} W \; P(X,W) = 0$

preuve> Nous faisons une preuve par récurrence[1] sur le degré de $P(X,T)$ en T (avec $d(0) = -1$). Lorsque $\deg(P) = 0$ ou -1, le résultat est facile. Nous reprenons les notations de la preuve de la proposition 6 . On peut supposer que les variables U et V sont deux des variables X_i [(2)] . Il s'agit, pour tout système $\mathbb{H}$ de csg où ne figure pas la variable W , d'expliciter la construction:

$$([\mathbb{H} , P(X,W) = 0] \overset{fort}{\Rightarrow} 1 = 0) \underset{cons}{\vdash} ([\mathbb{H} , P(X,U).P(X,V) \lessdot 0] \overset{fort}{\Rightarrow} 1 = 0))$$

qui peut se relire :

$$(\mathbb{H} \overset{fort}{\Rightarrow} P(X,W) \neq 0) \underset{cons}{\vdash} (\mathbb{H} \overset{fort}{\Rightarrow} P(X,U).P(X,V) > 0)$$

Supposons tout d'abord P unitaire.
L'implication forte $\mathbb{H} \overset{fort}{\Rightarrow} P(X,W) \neq 0$ s'écrit sous forme :

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

avec $Q_i(X) \in Cp(F_{\geq} \cup F_{>})$ et $N_j(X) \in F_{=}$. Les polynômes $B_i(X,W)$ et $C_j(X,W)$ peuvent être pris modulo P en W (parce que P est unitaire), auquel cas $\deg(G) \lessdot \deg(P) - 2$. Ce qui fait qu'on peut supposer que le degré en W de G est inférieur ou égal à $\deg(P) - 2$ (avec $0 - 2 = -1$).
La même égalité se relit de plusieurs manières:

$$\mathbb{H} \overset{fort}{\Rightarrow} G(X,W) \neq 0 \; (1), \quad \mathbb{H} \overset{fort}{\Rightarrow} P(X,W).G(X,W) > 0 \; (2) .$$

On déduit par substitution:

$$\mathbb{H} \overset{fort}{\Rightarrow} P(X,U).G(X,U) > 0 , \quad \mathbb{H} \overset{fort}{\Rightarrow} P(X,V).G(X,V) > 0$$

D'où : $\mathbb{H} \overset{fort}{\Rightarrow} P(X,U).G(X,U).P(X,V).G(X,V) > 0$
Par hypothèse de récurrence, on déduit de (1) que : $\mathbb{H} \overset{fort}{\Rightarrow} G(X,U).G(X,V) > 0$.
Enfin, on a trivialement:

$$[P(X,U).G(X,U).P(X,V).G(X,V) > 0 , G(X,U).G(X,V) > 0] \overset{fort}{\Rightarrow} P(X,U).P(X,V) > 0$$

On conclut par transitivité des implications fortes.

Voyons maintenant le cas où P n'est pas unitaire.
Soit C(X) son coefficient dominant en W .
Soit G le polynôme obtenu en supprimant le coefficient dominant de P en W .
On considère une nouvelle variable T . On considère le polynôme $P_1(X,T,W)$ obtenu à partir de P en multipliant tous ses coefficients (comme polynôme en W) par T , sauf le coefficient dominant qui est remplacé par 1 .
Démontrons l'existence potentielle en raisonnant cas par cas, selon le signe de C(X).
1er cas : $C(X) = 0$

---

[1] Cette preuve "recopie" la preuve classique de "si un corps est ordonné et si $P(u).P(v) < 0$ avec P irréductible, alors le corps $K[W]/P(W)$ est réel"

[2] D'après le théorème de substitution dans les existences potentielles, on peut supposer en fait qu'on est dans la situation générique où U, V et les coefficients du polynôme sont chacun une des variables X_i .

On a : $[\ P(X,U).P(X,V) \leqslant 0\ ,\ C(X) = 0\ ] \overset{fort}{\Rightarrow} G(X,U).G(X,V) \leqslant 0$
et par hypothèse de récurrence, on a:
$$G(X,U).G(X,V) \leqslant 0 \longrightarrow \tilde{\exists} W\ G(X,W) = 0$$
et comme :
$$[\ G(X,W) = 0,\ C(X) = 0\ ] \overset{fort}{\Rightarrow} P(X,W) = 0$$
on conclut par transitivité.
2ème cas : $C(X) \neq 0$.
On a : $C(X) \neq 0 \longrightarrow \tilde{\exists} T\ 1 = C(X).T$, et : $1 = C(X).T \overset{fort}{\Rightarrow} P(X,W) = P_1(X,T,W)$
et donc:
$$[\ P(X,U).P(X,V) \leqslant 0\ ,\ C(X) \neq 0\ ] \longrightarrow \tilde{\exists} T\ [\ 1 = C(X).T,\ P_1(X,T,U).P_1(X,T,V) \leqslant 0\ ]$$
Comme on a déjà traité le cas d'un polynôme unitaire on a:
$$[\ P_1(X,T,U).P_1(X,T,V) \leqslant 0\ ] \longrightarrow \tilde{\exists} W\ P_1(X,T,W) = 0$$
On conclut alors facilement par transitivité ❑

Théorème 22 : (autorisation de rajouter une racine sur l'intervalle où le signe change)
On a l'existence potentielle d'une racine sur l'intervalle où un polynôme change de signe. Ce qui s'écrit :
$$P(X,U).P(X,V) < 0 \longrightarrow \tilde{\exists} W\ [P(X,W) = 0,\ P(X,U).P(X,V) < 0,\ (W - U).(W - V) < 0]$$

preuve> Nous allons mimer le raisonnement classique qui dit : si w est hors de l'intervalle d'extrémités u et v , alors on considère le polynôme obtenu en divisant P(Z) par (Z – w), il change de signe aux bornes de l'intervalle, et on fait fonctionner une récurrence sur le degré de P . Voici ce que ça donne.

On va démontrer le théorème par récurrence sur le degré en W de P(X,W) .
Si ce degré est – 1 , le théorème est trivial. Passons de d à d+1. Supposons le degré d+1.
D'après le théorème 21 et la proposition 13, on a déjà:
$$P(X,U).P(X,V) < 0 \longrightarrow \tilde{\exists} W\ [P(X,W) = 0,\ P(X,U).P(X,V) < 0,]$$
Nous allons démontrer l'existence potentielle:
$P(X,U).P(X,V) < 0 \longrightarrow \tilde{\exists} W'\ [P(X,W') = 0,\ P(X,U).P(X,V) < 0,\ (W' - U).(W' - V) < 0]$
cas par cas, selon le signe de (W – U).(W – V) .
Si (W – U).(W – V) < 0 tout va bien : l'existence (vérifiée par W) implique l'existence potentielle (pour la nouvelle variable W') .
Si on rajoute (W – U).(W – V) = 0 on peut de nouveau séparer les cas :
1er sous cas : W – U = 0, on obtient aisément P(X,U) = P(X,W) = 0 , l'hypothèse $\mathbb{H}_1(X,W)$ est fortement incompatible, l'existence potentielle :
$\mathbb{H}_1(X,W) \longrightarrow \tilde{\exists} W'\ \mathbb{H}_2(X,W')$ est donc assurée.
2éme sous cas : W – U ≠ 0, on obtient aisément W – V = 0 , on est ramené au premier sous cas
3ème cas : Si on rajoute (W – U).(W – V) > 0 .
On considère une nouvelle variable T et le polynôme R défini par :
$$R(X,W,T) := (\ P(X,T) - P(X,W))\ /\ (T - W)\ .$$
Notons pour alléger R(T) pour R(X,W,T) et P(T) pour P(X,T) .
Notons $\mathbb{H}_1(X,W)$ pour [P(U).P(V) < 0, P(W) = 0 ,(W – U).(W – V) > 0] .
(c'est l'hypothèse de l'existence potentielle que nous voulons démontrer)
On a facilement l'implication forte:
$\mathbb{H}_1(X,W) \overset{fort}{\Rightarrow} P(T) = R(T).(T - W)$, et donc aussi :
$\mathbb{H}_1(X,W) \overset{fort}{\Rightarrow} [\ R(U).(W - U).R(V).(W - V) = P(U).P(V) < 0\ ,\ (W - U).(W - V) > 0\ ]$
et donc aussi

$\mathbb{H}_1(X,W) \overset{fort}{\Rightarrow} R(U).R(V) < 0$

Comme R(T) est degré d en T on applique l'hypothèse de récurrence. On obtient :

$R(U).R(V) < 0 \longrightarrow \tilde{\exists} W' \ [R(W') = 0, R(U).R(V) < 0, (W' - U).(W' - V) < 0]$

et on conclut facilement par quelques implications fortes et la transitivité des existences algébriques faibles ❑

Remarque 10 : On notera à quel point les raisonnements "formels" (sous forme d'implications fortes et existences potentielles) sont proches des raisonnements mathématiques correspondants de la théorie des corps ordonnés.

4) Evidence forte des faits explicités par un tableau de Hormander

Nullstellensatz réel en une variable

Rappelons tout d'abord l'algorithme de Hormander ainsi que la définition des codages à la Thom.

Proposition 23 : (Tableau et algorithme de Hormander)

Soit **K** un corps ordonné, sous-corps d'un corps réel clos **R** .

Soit $L = [P_1, P_2, ..., P_k]$ une liste de polynômes de **K**[X] .

Soit $\mathcal{P}$ la famille de polynômes engendrée par les éléments de L et par les opérations $P \longmapsto P'$, et $(P,Q) \longmapsto \mathbf{Rst}(P,Q)$. Alors :

1) $\mathcal{P}$ est finie.
2) On peut établir le tableau complet des signes pour $\mathcal{P}$ en utilisant les seules informations suivantes : le degré de chaque polynôme de la famille; les diagrammes des opérations $P \longmapsto P'$, et $(P,Q) \longmapsto \mathbf{Rst}(P,Q)$ (où $\deg(P) \geqslant \deg(Q)$) dans $\mathcal{P}$; et les signes des constantes de $\mathcal{P}$[1].

preuve> 1) A priori, pour construire $\mathcal{P}$ on prend la liste L et on applique systématiquement l'opération "reste de tous les couples de polynômes précédement obtenus" ainsi que l'opération "dérivation de tous polynômes précédement obtenus". Si d est le degré maximum dans L , en appliquant une fois les opérations "dérivation" et "reste" on n'introduit que des polynômes de degré $< d$. On peut donc, la deuxième fois, n'appliquer l'opération "dérivation" qu'à des nouveaux polynômes, tous de degré $< d$ et l'opération "reste" à des nouveaux couples de polynômes, donc avec le deuxième polynôme de degré $< d$. En conséquence les polynômes obtenus la deuxième fois sont tous de degré $< d - 1$. La même remarque s'applique à nouveau. Le processus ainsi contrôlé est donc fini.

2) Numérotons les polynômes de la famille avec un ordre qui respecte la croissance des degrés. Soit $\mathcal{P}_n$ la sous-famille de $\mathcal{P}$ consituée des polynômes numérotés de 1 à n . Elle est évidemment stable par les opérations 'dérivation' et 'reste de division', qui abaissent le degré. Notons enfin $\mathcal{T}_n$ le tableau de Hormander correspondant.

Montrons, par récurrence sur le numéro n du polynôme, qu'on peut établir le tableau complet des signes des polynômes de la famille $\mathcal{P}_n$, en utilisant les seules informations autorisées. Tant que les polynômes sont de degré 0 , c'est clair.

---

[1] On notera que les constantes $\mathcal{P}$ sont essentiellement : les coefficients dominants des polynômes de $\mathcal{P}$, et les valeurs $P(\xi)$ où P est un polynôme de $\mathcal{P}$ et ξ une racine d'un polynôme de degré 1 de $\mathcal{P}$.

Supposons vrai jusqu'à n . Soit P le polynôme de numéro n + 1 dans $\mathcal{P}$. Sur chacun des intervalles du tableau $\mathcal{T}_n$, le polynôme P est strictement monotone, d'après le théorème des accroissements finis. Chacun des points ξ du tableau $\mathcal{T}_n$ est ou bien $+\infty$, ou bien $-\infty$, ou bien une racine d'un certain polynôme Q de numéro $\leq$ n , et dans ce cas, si $R = \mathbf{Rst}(P,Q)$, on a $P(\xi) = R(\xi)$. Le signe de $P(\xi)$ est donc connu dans tous les cas à partir des informations autorisées. On en déduit sur quels intervalles ouverts de $\mathcal{T}_n$ le polynôme P reste de signe constant, en quels points déjà introduits s'annule P et sur quels intervalles ouverts de $\mathcal{T}_n$ sont les racines de P dans **R** qui ne figuraient pas encore dans $\mathcal{T}_n$. Soit ζ une racine de P sur l'un de ces intervalles ouverts $I =]\xi,\xi'[$. Si Q est un polynôme de numéro $\leq$ n dans $\mathcal{P}$, son signe sur I est connu donc aussi en ζ ,sur $]\xi,\zeta[$ et sur $]\zeta,\xi'[$. Quant à P ,son signe sur $]\xi,\zeta[$ et celui sur $]\zeta,\xi'[$ sont également connus . On a donc construit le tableau complet des signes pour $\mathcal{P}_{n+1}$ à partir des informations autorisées et du tableau complet des signes pour $\mathcal{P}_n$. ❑

Définition 24 : (codage à la Thom)

Soit **K** un corps ordonné, **R** sa clôture réelle.

Un élément ξ de **R** est dit *codé à la Thom* (dans **K**) s'il est présenté comme racine d'un polynôme P , de **K**[X] , en précisant les signes stricts [1] de $P'(\xi)$, $P''(\xi)$, etc...

Un intervalle ouvert non borné de **R** est dit *codé à la Thom* (dans **K**) s'il est présenté comme l'ensemble des éléments ζ qui attribuent des signes stricts précisés à une liste de polynômes [P , P' , P" , etc...]) l'extrémité finie α de l'intervalle étant obtenue pour $P(\alpha) = 0$.

Un intervalle ouvert borné de **R** est dit *codé à la Thom* (dans **K**) s'il est présenté comme l'ensemble des éléments ζ qui attribuent des signes stricts précisés à deux listes de polynômes [P , P' , P" , etc...] et [Q , Q' , Q" , etc...]) , les extrémités α et β de l'intervalle étant obtenues pour $P(\alpha) = 0$ et $Q(\beta) = 0$.

NB : Tout point de **R** peut être codé à la Thom dans **K** . Mais des intervalles ouverts de **R** peuvent ne pas être codables à la Thom dans **K** . L'important est que les intervalles ouverts minimaux des tableaux de Hormander le soient.

Le § 4) est essentiellement consacré à la preuve du théorème suivant :

Théorème 25 : (nullstellensatz réel en une variable)

Soit **K** un corps ordonné et **R** sa clôture réelle. Soit $\mathcal{P}$ une famille de polynômes de **K**[X] et $\mathbb{H}(X)$ un système de csg portant sur des éléments de $\mathcal{P}$. Alors :

ou bien $\mathbb{H}(x)$ est impossible dans **R** et alors $\mathbb{H} \overset{\text{for}}{\Rightarrow} 1 = 0$ dans **K** , et donc $\mathbb{H}(x)$ est impossible dans toute extension ordonnée de **K** .

ou bien $\mathbb{H}(x)$ est possible dans **R** et alors $\widetilde{\exists} X\, \mathbb{H}(X)$ dans **K** et dans toute extension ordonnée de **K** .

On peut supposer que la famille $\mathcal{P}$ est stable par les opérations "reste" et "dérivation". (proposition 23).

L'impossibilité de $\mathbb{H}(x)$ dans **R** ou l'existence de x dans **R** vérifiant $\mathbb{H}(x)$ est directement lisible sur le tableau de Hormander de la famille, et se teste uniquement par des calculs dans **K** . Nous allons montrer que la construction même du tableau de Hormander peut

---

[1] Rappelons que nous disons qu'un signe est strict s'il est +1 ou −1 .

être traduite, pas à pas, en *évidences fortes* et en *existences potentielles* qui rendent compte de tous les fait lisibles sur le tableau de Hormander. Si on considère maintenant une extension ordonnée $\mathbf{L}$ de $\mathbf{K}$, on pourra appliquer pour $\mathbb{H}$, $\mathbf{L}$ et sa clôture réelle, les résultats obtenus pour $\mathbb{H}$, $\mathbf{K}$ et $\mathbf{R}$; comme le test se fait uniquement par des calculs dans $\mathbf{K}$ la possibilité ou l'impossibilité sera équivalente dans les deux cas.

Nous commençons par considérer le cas où le corps $\mathbf{K}$ est réel clos, qui est beaucoup plus simple à traiter.

Lorsque le corps K est réel clos

preuve du théorème dans ce cas > On a donc $\mathbf{R} = \mathbf{K}$. Soient $\upsilon_1, \upsilon_2, ..., \upsilon_k$ la liste ordonnée des points finis du tableau de Hormander de la famille $\mathcal{P}$. On peut calculer υ_0 et υ_{k+1} dans $\mathbf{R}$ tels que l'évidence forte des signes de tous les $P \in \mathcal{P}$ soit facile à établir en $x \lessdot \upsilon_0$ et en $x \gtrdot \upsilon_{k+1}$.
La possibilité dans $\mathbf{R}$ pour un système de csg donné est immédiatement lisible et explicitable, soit en un υ_i, soit en un $x = (\upsilon_i + \upsilon_{i+1})/2$. Cela implique l'existence potentielle.
L'incompatibilité dans $\mathbf{R}$ pour une système $\mathbb{H}$ de csg est également lisible sur le tableau de Hormander, mais l'incompatibilité forte demande un peu plus de fatigue. On commence par remarquer qu'on peut raisonner en séparant les cas : $X < \upsilon_0$, $X = \upsilon_0$, $X > \upsilon_0$. Le troisième cas se scinde de nouveau en trois cas $X < \upsilon_1$, $X = \upsilon_1$, $X > \upsilon_1$ etc... De sorte qu'il suffit d'établir l'incompatibilité forte de l'une des csg de $\mathbb{H}$ au moins : en chacun des points υ_i d'une part, sur chacun des intervalles ouverts $]\upsilon_i, \upsilon_{i+1}[$ d'autre part, et enfin pour $X < \upsilon_0$ et pour $X > \upsilon_{k+1}$.
Dans le dernier cas, le travail a déjà été fait. En un point υ_i le signe de chaque $P(\upsilon_i)$ est fortement évident dans $\mathbf{R}$ (puisque $\upsilon_i \in \mathbf{R}$). Sur un intervalle $]\upsilon_i, \upsilon_{i+1}[$, les signes, constants et non nuls, des $P \in \mathcal{P}$ sont tous fortement évidents à partir des signes aux bords modulo une formule de Taylor mixte convenable (cf. théorème 10 (f)).

Dans le corps des coefficients

Nous voulons établir, pour tous les faits lisibles sur le tableau de Hormander, incompatibilité forte et existence potentielle dans $\mathbf{K}$, sans hypothèse de clôture. Le corps le plus petit possible à considérer est le corps des coefficients des polynômes de la famille $\mathcal{P}$.
Il nous faut cette fois-ci suivre l'algorithme de Hormander pas à pas, c.-à-d. en introduisant les points du tableau de Hormander un à un.
Nous commençons par calculer a et b dans $\mathbf{K}$, au delà desquels les signes des polynômes de $\mathcal{P}$ sont fortement évidents. Ces 2 éléments de $\mathbf{K}$ remplaceront pour nous $-\infty$ et $+\infty$ dans le tableau de Hormander.

Lemme 26 : (évidence forte et existence potentielle pour les faits élémentaires lisibles sur un tableau de Hormander)
Soit $\mathbf{K}$ un corps ordonné et $\mathbf{R}$ sa clôture réelle. Soit $\mathcal{P}$ une famille de polynômes de $\mathbf{K}[X]$ stable par les opérations "reste" et "dérivation", soit $\mathcal{T}$ son tableau de Hormander.
1) les points du tableau de Hormander, définis à la Thom par leur construction même, vérifient l'existence potentielle pour leur codage à la Thom [1].

---

[1] Un même point peut être codé à la Thom via des polynômes distincts. Le codage que nous considérons ici est le premier qui se présente pour le point dans la construction du tableau.

2) la comparaison (pour l'ordre) de 2 points du tableau est fortement évidente à partir de leur codage à la Thom.
3) en chaque point du tableau, les signes de tous les polynômes de la famille sont fortement évidents à partir du codage à la Thom du point considéré.
4) sur chaque intervalle ouvert minimal du tableau les signes de tous les polynômes précédemment introduits sont fortement évidents à partir du codage à la Thom des extrémités de l'intervalle (si l'intervalle est non borné, seule l'extrémité finie intervient, naturellement) et du fait que le point est situé entre les extrémités, ou encore à partir du codage à la Thom de l'intervalle.

preuve du lemme> Nous démontrons le lemme pour la famille $\mathcal{P}_n$ et le tableau $\mathcal{T}_n$, par récurrence sur n. En suivant pas à pas la preuve de la proposition 23. Le lemme est évident lorsque la famille $\mathcal{P}_n$ ne contient que des constantes.
Passons de n à n+1. Si λ est un point de $\mathcal{T}_n$, nous noterons $Q_\lambda(X)$ le polynôme à partir duquel il est codé à la Thom, et $\mathbb{H}_\lambda(X)$ le système de csg qui constitue son codage à la Thom (λ est le seul point de $\mathbf{R}$ vérifiant $\mathbb{H}_\lambda(\lambda)$. Soit alors P le polynôme numéroté n+1, non constant, de degré d.
Dans la preuve qui suit nous n'examinons que le cas des intervalles ouverts minimaux bornés, l'adaptation au cas non borné étant immédiate en utilisant les points a et b qui remplacent $-\infty$ et $+\infty$.

Voyons le point 1) Seuls les points introduits à l'étape n+1 posent a priori problème. Il est clair que le signe de P en un point λ de $\mathcal{T}_n$ est fortement évident à partir du signe de $\mathbf{Rst}(P,Q_\lambda)(\lambda)$ et du fait que $Q_\lambda(\lambda)=0$; donc aussi, d'après l'hypothèse de récurrence (3), à partir de $\mathbb{H}_\lambda(\lambda)$. Soit ζ une racine de P située sur l'intervalle ouvert minimal $]\alpha,\beta[$ de $\mathcal{T}_n$. On a donc, en considérant α et β comme des variables (sauf lorsqu'ils sont en indice d'un $\mathbb{H}$ [1]) :

$$\mathbb{H}_\alpha(\alpha) \overset{fort}{\Rightarrow} P(\alpha)>0 \quad \text{et} \quad \mathbb{H}_\beta(\beta) \overset{fort}{\Rightarrow} P(\beta)<0 \quad \text{ou vice-versa}$$

Par le théorème 22 et la transitivité des existences potentielles, on a donc :

$$[\,\mathbb{H}_\alpha(\alpha)\,,\mathbb{H}_\beta(\beta)\,] \longrightarrow \tilde{\exists}\, X\,[\,\alpha<X<\beta\,,P(X)=0\,] \quad (2)$$

Par ailleurs, toujours par hypothèse de récurrence (3), il y a des $\tau_i \in \{<,>\}$ (i = 1, ..., d) tels que, en appelant τ'_i le signe $\leqslant$ ou $\geqslant$ associé à τ_i, on ait :

$$\mathbb{H}_\alpha(\alpha) \overset{fort}{\Rightarrow} [P^{(i)}(\alpha)\ \tau'_i\ 0 \quad (i=1,...,d-1)] \quad \text{et} \quad \mathbb{H}_\alpha(\alpha) \overset{fort}{\Rightarrow} P^{(d)}(\alpha)\ \tau_d\ 0$$
$$\mathbb{H}_\beta(\beta) \overset{fort}{\Rightarrow} [P^{(i)}(\beta)\ \tau'_i\ 0 \quad (i=1,...,d-1)] \quad \text{et} \quad \mathbb{H}_\beta(\beta) \overset{fort}{\Rightarrow} P^{(d)}(\beta)\ \tau_d\ 0 \quad (3)$$

Par application des formules de Taylor mixtes (théorème 10 f) et de la transitivité on obtient:

$$[\,\mathbb{H}_\alpha(\alpha)\,,\mathbb{H}_\beta(\beta)\,] \longrightarrow \tilde{\exists}\, X\,[\,\alpha<X<\beta\,,P(X)=0\,,\ P^{(i)}(X)\ \tau_i\ 0 \quad (i=1,...,d)\,]$$

Et comme on a déjà :

$$\tilde{\exists}\,\alpha,\beta\ [\,\mathbb{H}_\alpha(\alpha)\,,\ \mathbb{H}_\beta(\beta)\,]$$

On en déduit par transitivité:

$$\tilde{\exists}\, X\,[\ P(X)=0\,,\ P^{(i)}(X)\ \tau_i\ 0 \quad (i=1,...,d)\ ]$$

---

[1] Il serait plus correct d'utiliser une variable X_α associée à α, mais la preuve serait moins lisible.

[2] On a en effet facilement $[\,\alpha<\beta\,,(X-\alpha)(X-\beta)<0\,] \overset{fort}{\Rightarrow} \alpha<X<\beta$.

[3] Les affirmations concernant $P^{(d)}(.)$ sont particulièrement évidentes puisque $P^{(d)}$ est une constante, nous les avons mentionnées essentiellement en vue d'une relecture de cette preuve lorsque les coefficients de P dépendront de paramètres.

que nous réécrivons pour plus de lisibilité:

$$\tilde{\exists}\zeta\ \mathbb{H}_\zeta(\zeta)$$

Voyons le point 2) Vues les implications fortes:
$\mathbb{H}_\alpha(\alpha) \overset{fort}{\Rightarrow} P^{(i)}(\alpha)\ \tau'_i\ 0$, $\mathbb{H}_\alpha(\alpha) \overset{fort}{\Rightarrow} P(\alpha) > 0$ (ou < 0) et $\mathbb{H}_\alpha(\alpha) \overset{fort}{\Rightarrow} P^{(d)}(\alpha)\ \tau_d\ 0$, le signe de $\alpha - \zeta$ est fortement évident à partir des codages à la Thom via le théorème 10 b), (de même pour $\beta - \zeta$). En clair :

$$[\ \mathbb{H}_\alpha(\alpha)\ ,\ \mathbb{H}_\zeta(\zeta)\ ] \overset{fort}{\Rightarrow} \alpha < \zeta$$

Le point 2) pour $\mathcal{T}_{n+1}$ se déduit alors du point 2) pour $\mathcal{T}_n$: si par exemple $\lambda \in \mathcal{T}_n$ avec $\lambda < \alpha$ on a par hypothèse de récurrence :

$$[\ \mathbb{H}_\alpha(\alpha)\ ,\ \mathbb{H}_\lambda(\lambda)\ ] \overset{fort}{\Rightarrow} \lambda < \alpha$$

Donc : $$[\ \mathbb{H}_\alpha(\alpha)\ ,\ \mathbb{H}_\lambda(\lambda)\ ,\ \mathbb{H}_\zeta(\zeta)\ ] \overset{fort}{\Rightarrow} \lambda < \alpha < \zeta$$

Et comme $\tilde{\exists}\alpha\ \mathbb{H}_\alpha(\alpha)$:

$$[\ \mathbb{H}_\lambda(\lambda)\ ,\ \mathbb{H}_\zeta(\zeta)\ ] \overset{fort}{\Rightarrow} \lambda < \zeta$$

Voyons le point 3) On a déjà vu que le signe de P en tout point λ de $\mathcal{T}_n$ est fortement évident à partir du codage à la Thom de λ . Il reste à voir que le signe de $Q \in \mathcal{P}_n$ en un point nouvellement introduit (tel que le ζ du 1)) est fortement évident à partir de son codage à la Thom. On sait d'après le 2) que l'on a :

$$[\ \mathbb{H}_\alpha(\alpha)\ ,\ \mathbb{H}_\beta(\beta)\ ,\ \mathbb{H}_\zeta(\zeta)\ ] \overset{fort}{\Rightarrow} \alpha < \zeta < \beta$$

Par ailleurs, vue l'hypothèse de récurrence (3) le signe de Q en α et β est fortement évident à partir de $\mathbb{H}_\alpha(\alpha)$ et $\mathbb{H}_\beta(\beta)$.
En appliquant de nouveau le théorème 10 f) (formule de Taylor mixte) et la transitivité, on obtient :

$$[\ \mathbb{H}_\alpha(\alpha)\ ,\ \mathbb{H}_\beta(\beta)\ ,\ \mathbb{H}_\zeta(\zeta)\ ] \overset{fort}{\Rightarrow} Q(\zeta)\ \tau\ 0 \quad \text{avec } \tau \in \{<, >\}$$

Et comme : $$\tilde{\exists}\alpha,\beta\ [\ \mathbb{H}_\alpha(\alpha)\ ,\ \mathbb{H}_\beta(\beta)\ ]$$

on obtient le résultat voulu :

$$\mathbb{H}_\zeta(\zeta)\ ] \overset{fort}{\Rightarrow} Q(\zeta)\ \tau\ 0 \quad \text{avec } \tau \in \{<, >\}\ ^1$$

Voyons le point 4) Notons $\mathbb{H}_{\lambda,\mu}(X)$ le codage à la Thom d'un intervalle ouvert minimal de $\mathcal{T}_{n+1}$. Il est obtenu en prenant $\mathbb{H}_\lambda(X)$, $\mathbb{H}_\mu(X)$ et en remplaçant les conditions de signes $Q_\lambda(X) = 0$ et $Q_\mu(X) = 0$ par les conditions strictes convenables. Par application du théorème 10 b) on obtient:

$$[\ \mathbb{H}_\mu(\mu)\ ,\ \mathbb{H}_\lambda(\lambda)\ ,\ \mathbb{H}_{\lambda,\mu}(X)\ ] \overset{fort}{\Rightarrow} \lambda < X < \mu$$

Si maintenant Q est un polynôme arbitraire de $\mathcal{P}_{n+1}$ on raisonne comme au point 3) pour le signe de Q en ζ et on obtient l'évidence forte du signe $Q(X)$ sous l'hypothèse $\mathbb{H}_{\lambda,\mu}(X)$ ❑

preuve du théorème 25 > Nous voulons montrer l'existence potentielle ou l'incompatibilité forte pour un système $\mathbb{H}$ de csg portant sur des éléments de $\mathcal{P}$. Vu le lemme 26, nous pouvons recopier, avec les précautions d'usage, ce que nous avons fait dans le cas d'un corps réel clos. La disjonction des cas va pouvoir être pratiquée grâce à (2). L'évaluation du signe d'un polynôme en un point du tableau sera remplacée par l'évidence forte du signe de ce polynôme etc... ❑

---

[1] On notera que l'usage des formules de Taylor mixtes permet de déduire que les signes fortement évidents de Q et Q' en des points successifs de $\mathcal{T}_{n+1}$ respectent le théorème des accroissements finis sans faire appel à ce théorème, donc sans faire appel non plus à l'existence d'une clôture réelle de $\mathbf{K}$.

Une nouvelle preuve de l'existence et unicité de la clôture réelle d'un corps ordonné

On commence par remarquer que les résultats établis jusqu'ici, avant ce qui concerne l'algorithme de Hormander, ont été établis sans supposer l'existence d'une clôture réelle de **K** . Pour ce qui concerne l'algorithme de Hormander et son "algébrisation" dans le corps des coefficients, on remarque que le travail peut être fait "en aveugle" même sans supposer l'existence d'une clôture réelle. Par exemple, on ne suppose jamais a priori qu'un polynôme P ne peut passer de + à − dans le tableau de Hormander "aveugle" sur un intervalle où P' est marqué + , c.-à-d. qu'on ne suppose pas a priori l'existence d'une extension ordonnée contenant les racines marquées dans le tableau, cela se déduit au contraire des formules de Taylor mixtes.

Sans supposer savoir déjà l'existence d'une clôture réelle de **K** , les preuves données jusqu'ici montrent donc que :

Si P est un polynôme de **K**[X], de degré $n+1$, et $[\sigma_1, ..., \sigma_n]$ une liste de signes stricts, et si $\mathbb{H}$ est le système de csg : $P(X) = 0$, $P'(X) \equiv \sigma_1$, ..., $P^{(i)}(X) \equiv \sigma_i$, ..., $P^{(n)}(X) \equiv \sigma_n$: ou bien $\mathbb{H}$ est fortement incompatible dans **K** , ou bien on a l'existence potentielle d'un X vérifiant $\mathbb{H}$ (lue dans **K**) .

Dans ce dernier cas, si Q est un polynôme de **K**[X] , il y a exactement un signe σ tel que l'on ait l'implication forte :

$$\mathbb{H} \overset{\text{fort}}{\Rightarrow} Q(X) \equiv \sigma$$

Ceci fournit alors un algorithme d'affectation de signes dans **K**[X].

Il est alors immédiat que l'algorithme d'affectation de signes ainsi défini est cohérent. Ceci montre l'existence et l'unicité forte d'une extension de **K** engendrée par une racine de P spécifiée à la Thom, à condition que cette spécification ne soit pas fortement absurde (ce qui est testable par la construction du tableau de Hormander de la famille stable engendrée par P).

On peut enfin déduire de ce résultat, sans trop de fatigue supplémentaire, l'existence et l'unicité forte de la clôture réelle de **K** .

5) Stellensatz réel effectif

A partir du moment où on a démontré la version "implication forte" des axiomes et des régles de déduction de la théorie formelle intuitionniste des corps réels clos avec les éléments de **K** pour constantes, il n'est pas étonnant qu'on puisse traduire sous forme d'implication forte tout énoncé démontrable dans cette théorie formelle. En quelque sorte, le plus difficile a été fait avec la validation du raisonnement "cas par cas", la transitivité des implications fortes et l'autorisation de rajouter une racine à un polynôme sur un intervalle où il change de signe. En fait, comme nous n'avons pas de version "implication forte" pour des énoncés avec trop d'alternances de quantificateurs, ce n'est pas tout à fait aussi simple.

La preuve du nullstellensatz consiste donc en quelque sorte à vérifier que l'algorithme proposé dans [**LR**] pour décider un énoncé purement universel de la théorie des corps réels clos n'utilise pas d'arguments logiques impliquant des énoncés à trop d'alternances de quantificateurs. Cela tient notamment au fait que le théorème des accroissements finis, et par suite le lemme de Thom, a été mis sous une forme purement algébrique.

Nous commençons par rappeler le théorème concernant les tableaux de Hormander paramétrés. (cf. [**BCR**]).

Proposition 27 : (Tableau de Hormander paramétré)

Soit **K** un corps ordonné, sous-corps d'un corps réel clos **R** .

Soit $L = [Q_1 , Q_2 , ..., Q_k]$ une liste de polynômes de $\mathbf{K}[U_1, U_2, ..., U_n][X]$.

On peut construire une famille finie $\mathcal{F}$ de polynômes de $\mathbf{K}[U_1, U_2, ..., U_n]$ telle que, pour tout $u_1, u_2, ..., u_n$ dans **K** , en posant $P_i(X) = Q_i(u_1, u_2, ..., u_n;X)$, le tableau complet des signes pour $L = [P_1 , P_2 , ..., P_k]$ est calculable à partir des signes des $S(u_1, u_2, ..., u_n)$ pour $S \in \mathcal{F}$.

preuve> On remarque que les constantes de *l'algorithme de Hormander* (cf. proposition 23) sont toutes obtenues comme fractions rationnelles en les coefficients des polynômes de la liste initiale L . Par ailleurs, le calcul de la famille $\mathcal{P}$ est "uniforme" à ceci près que le calcul d'un reste **Rst**(P,Q) dépend du degré de Q . Comme les coefficients de Q sont fractions rationnelles en les coefficients des polynômes de la liste initiale L , le degré de Q , pour une spécialisation $u_1, u_2, ..., u_n$ donnée de $U_1, U_2, ..., U_n$, dépend de l'annulation de certains polynômes en les coefficients des polynômes de la liste initiale L . On met donc dans la famille $\mathcal{F}$ tous les polynômes apparaissant au numérateur ou dénominateur d'un coefficient d'un polynôme de la famille $\mathcal{P}$, pour toutes les familles $\mathcal{P}$ possibles . ❑

Nous sommes maintenant en mesure de démontrer le :

Théorème 28 : (Tableau de Hormander paramétré, implications fortes et existences potentielles) Soit **K** un corps ordonné, sous-corps d'un corps réel clos **R** .

Soit $L = [Q_1 , Q_2 , ..., Q_k]$ une liste de polynômes de $\mathbf{K}[U_1,U_2,...,U_n][X]$.

On construit la famille finie $\mathcal{F}$ de polynômes de $\mathbf{K}[U_1,U_2,...,U_n]$ comme à la proposition 27 .

Soit $\mathbb{H}(U_1,U_2,...,U_n,X)$ un système de csg portant sur des polynômes de la liste L .

Soit un élément $\Sigma = (\sigma_S)_{S \in \mathcal{F}}$ de $\{-1 , 0 , +1\}^{\mathcal{F}}$. On note $\mathbb{H}_\Sigma(U_1,U_2,...,U_n)$ le système de conditions de signes $[S(U_1,U_2,...,U_n) \equiv \sigma_S ; S \in \mathcal{F}]$. On suppose qu'il existe $u_1,u_2,...,u_n \in \mathbf{R}$ vérifiant $\mathbb{H}_\Sigma(u_1,u_2,...,u_n)$. Alors :

ou bien $\forall\, u_1,u_2,...,u_n \in \mathbf{R}$ $(\mathbb{H}_\Sigma(u_1,u_2,...,u_n) \Rightarrow \exists\, x \in \mathbf{R}$ $\mathbb{H}(u_1,u_2,...,u_n,x))$ et alors : $\mathbb{H}_\Sigma(U_1,U_2,...,U_n) \longrightarrow \widetilde{\exists} X$ $\mathbb{H}(U_1,U_2,...,U_n,X)$ (lu dans **K**)

ou bien $\forall\, u_1,u_2,...,u_n,x \in \mathbf{R}$ $(\mathbb{H}_\Sigma(u_1,u_2,...,u_n)$ et $\mathbb{H}(u_1,u_2,...,u_n,x)) \Rightarrow 1 = 0$ et alors : $[\mathbb{H}_\Sigma(U_1,U_2,...,U_n) , \mathbb{H}(U_1,U_2,...,U_n,X)] \overset{\text{fort}}{\Rightarrow} 1 = 0$ (dans **K**)

preuve> Les conditions de signe $\mathbb{H}_\Sigma$ imposent les degrés des polynômes de la famille stable (par reste et dérivation) engendrée par L , ainsi que le tableau de Hormander de la famille. Pour ne pas avoir à utiliser des fractions rationnelles en $U_1,U_2,...,U_n$ comme coefficients des polynômes de la famille stable engendrée, nous pouvons remplacer, après avoir calculé la famille, chaque polynôme par un polynôme obtenu en le multipliant par un facteur carré convenable dans $\mathbf{K}[U_1,U_2,...,U_n]$, facteur fortement non nul sous les hypothèses $\mathbb{H}_\Sigma$. Nous pouvons alors répéter avec les précautions d'usage[1] les raisonnements de la preuve du théorème 25 , et nous obtenons le théorème 25 "avec paramètres" , c.-à-d. le théorème 28 . ❑

---

[1] Par exemple les points a et b qui remplacent $-\infty$ et $+\infty$ dans la preuve du théorème 23 sont représentés maintenant par des variables A et B avec l'existence potentielle convenable.

On notera que la preuve du théorème 25 serait peu perturbée si $\mathbb{H}_\Sigma$ était incompatible. On obtiendrait qu'au moins l'une des deux conclusions est valable.

Le nullstellensatz réel effectif général est maintenant facile.

Théorème 29 : (nullstellensatz, positivestellensatz et nichtnegativestellensatz réels effectifs[1])

Soit **K** un corps ordonné, sous-corps d'un corps réel clos **R** .

Soit $\mathbb{H}(U_1,U_2,...,U_n)$ un système de csg portant sur une famille finie de polynômes de $\mathbf{K}[U_1,U_2,...,U_n]$. Ce système est impossible dans **R** si et seulement si il est fortement incompatible dans **K** . En termes plus formalisés :

Si $\forall\, u_1,u_2,...,u_n \in \mathbf{R}$ $\mathbb{H}(u_1,u_2,...,u_n)$ est absurde,

alors : $\mathbb{H}(U_1,U_2,...,U_n) \overset{\text{fort}}{\Rightarrow} 1=0$ (dans **K**).

Si $\mathbb{H}(U_1,U_2,...,U_n) \overset{\text{fort}}{\Rightarrow} 1=0$ (dans **K**) , **alors** les csg $\mathbb{H}$ sont impossibles à réaliser dans n'importe quelle extension ordonnée de **K** .

preuve> La partie "réciproque" est évidente. Pour la partie "directe", on fait un raisonnement par récurrence sur le nombre de variables. Pour $n=1$, c'est le théorème 25. Passons de n à n+1 . On appelle X la $n+1^{\text{ème}}$ variable, on va utiliser le théorème 28. Pour construire l'implication forte demandée, on raisonne cas par cas, selon les signes que prennent les polynômes de la famille $\mathcal{F}$. Soit donc Σ un élément arbitraire de $\{-1\,,0\,,+1\}^{\mathcal{F}}$.

Nous voulons construire l'implication forte:

$$[\,\mathbb{H}_\Sigma(u_1,u_2,...,u_n)\,,\ \mathbb{H}(u_1,u_2,...,u_n,x)\,] \overset{\text{fort}}{\Rightarrow} 1=0\,.$$

Si $\mathbb{H}_\Sigma$ est impossible dans **R** (ce qui est testable par l'algorithme de Hormander appliqué de manière itérative), on applique l'hypothèse de récurrence, on en déduit :

$$\mathbb{H}_\Sigma \overset{\text{fort}}{\Rightarrow} 1=0 \qquad \text{et a fortiori} \qquad [\,\mathbb{H}_\Sigma\,,\ \mathbb{H}\,] \overset{\text{fort}}{\Rightarrow} 1=0\,.$$

Sinon, on applique le théorème 28 , c'est forcément la deuxième alternative qui se présente puisque $\mathbb{H}(u_1,u_2,...,u_n,x)$ est impossible dans **R** . ❑

Vu le caractère uniformément primitif récursif des algorithmes donnés dans nos preuves, on a également :

Théorème 30 : (nullstellensatz réel uniformément primitif récursif)

Soit **K** un corps ordonné, sous-corps d'un corps réel clos **R** .

Soit $\mathbb{H}(U_1,U_2,...,U_n)$ un système de csg portant sur une famille finie de polynômes de $\mathbf{K}[U_1,U_2,...,U_n]$. Soit $(c_i)_{i\in I}$ la famille finie des coefficients des polynômes figurant dans $\mathbb{H}$. Considérons que la structure de corps ordonné du corps des coefficients $\mathbb{Q}((c_i)_{i\in I})$ est donnée par un oracle qui répond à la question : " quel est le signe de $P((c_i)_{i\in I})$ " , où l'entrée est le polynôme $P\in \mathbb{Z}[(C_i)_{i\in I}]$.

Il existe un algorithme uniformément primitif récursif qui décide si $\mathbb{H}$ est impossible dans **R** et qui construit, dans le cas de réponse positive, une implication forte $\mathbb{H} \overset{\text{fort}}{\Rightarrow} 1=0$ (dans **K**).

Remarque 11 : Il serait facile de prouver, par récurrence sur le nombre de variables, un additif au théorème 29 qui affirmerait que l'existence dans **R** implique l'existence potentielle lue dans **K** , et vice versa. En fait, une fois établi le théorème des zéros réels, on en déduit

---

[1] "effectifs" parce que toutes nos preuves sont constructives et réfèrent à des algorithmes

immédiatement l'interprétation suivante de l'existence potentielle sous conditions :
Soient $\mathbb{H}_1$ un système de csg portant sur des polynômes de $\mathbf{K}[\mathbf{X}] = \mathbf{K}[X_1,X_2,...,X_n]$, et $\mathbb{H}_2$ un système de csg portant sur des polynômes de $\mathbf{K}[\mathbf{X},T_1,T_2,...,T_m] = \mathbf{K}[\mathbf{X},\mathbf{T}]$. Alors on a:

$$\mathbb{H}_1(\mathbf{X}) \longrightarrow \tilde{\exists}\,\mathbf{T}\ \mathbb{H}_2(\mathbf{X},\mathbf{T}) \quad \text{(lu dans } \mathbf{K}\text{)}$$

si et seulement si :

$$\forall\, \mathbf{x} \in \mathbf{R}^n\ (\ \mathbb{H}_1(\mathbf{x}) \Rightarrow \exists\, \mathbf{t} \in \mathbf{R}^m\ \mathbb{H}_2(\mathbf{x},\mathbf{t})\ )$$

Nous terminons par un théorème qui explicite une signification constructive du théorème de mathématiques classiques: "tout corps réel possède une extension réelle close" (ce théorème est non démontrable, en tant que tel, constructivement). Nous commençons par rappeler un résultat de [**LR**].

Théorème 31 :

Soit $\mathbf{K}$ un corps ordonné discret et $T_1(\mathbf{K})$ la théorie formelle intuitionniste des corps réels clos discrets, avec les éléments $\mathbf{K}$ pour constantes et les axiomes explicitant la structure de corps ordonné de $\mathbf{K}$. Alors $T_1(\mathbf{K})$ est décidable, complète et non contradictoire. En outre, pour toute formule F , F ou $\neg F$ est un théorème.

Le théorème des zéros réels permet alors d'établir constructivement:

Théorème 32 :

Soit $\mathbf{K}$ un corps réel discret et $T_2(\mathbf{K})$ la théorie formelle intuitionniste des corps réels clos discrets, avec les éléments $\mathbf{K}$ pour constantes et les axiomes explicitant la structure de corps de $\mathbf{K}$. Alors $T_2(\mathbf{K})$ est non contradictoire[1].

preuve> La théorie $T_2(\mathbb{Q})$ et la théorie $T_1(\mathbb{Q})$ sont équivalentes. Si on a une contradiction dans la théorie $T_2(\mathbf{K})$, sa démonstration fait appel à un nombre fini d'axiomes traduisant la structure de corps de $\mathbf{K}$. Si $c_1, c_2, ..., c_n$ sont les éléments de $\mathbf{K}$ intervenant dans ces axiomes, on remarque que ces axiomes s'écrivent sous la forme $P_i(c_1, c_2, ..., c_n) = 0$ pour des polynômes $P_i(X_1, X_2, ..., X_n) \in \mathbf{K}[X_1, X_2, ..., X_n]$ $i = 1, 2, ..., k$. La preuve de la contradiction dans $T_2(\mathbf{K})$ fournit donc une preuve dans $T_2(\mathbb{Q})$ d'un théorème de la forme:

$$(P_1(X_1, X_2, ..., X_n) = 0 \text{ et } ... \text{ et } P_k(X_1, X_2, ..., X_n) = 0\ ) \Rightarrow 1 = 0$$

Le même théorème est prouvable dans $T_1(\mathbb{Q})$. D'après le théorème des zéros réels, on en déduit une identité algébrique de la forme :

$$1 + \sum_{i=1}^{h} p_i.R_i^2 + \sum_{j=1}^{k} P_j.T_j = 0$$

avec p_i positif dans $\mathbb{Q}$, R_i et T_j dans $\mathbf{K}[X_1, X_2, ..., X_n]$. En remplaçant les X_i par les c_i dans cette identité algébrique, on obtient que le corps $\mathbf{K}$ n'est pas réel . ❑

---

[1] Nous avons utilisé deux notations distinctes $T_1(\mathbf{K})$ et $T_2(\mathbf{K})$ pour souligner que dans le deuxième cas, les axiomes liant les constantes explicitent la structure de corps de $\mathbf{K}$ tandis que dans le premier cas, il y a aussi les axiomes sur les constantes explicitant la structure d'ordre. En fait, on peut formuler la théorie formelle des corps réels clos sans recours à la structure d'ordre: -1 n'est pas un carré, $\forall\, x$ x ou $-x$ est un carré, tout polynôme de degré impair admet une racine. Le tiers exclu restreint est alors formulé: $\forall\, x$ $x = 0$ ou $x \neq 0$. Si on adopte ce point de vue, la théorie formelle $T_1(\mathbf{K})$ contient, pour chaque élément positif a de $\mathbf{K}$ l'axiome $\exists\, x$ $x^2 = a$.

Le théorème 32 nous dit en particulier que, tant qu'on cherche à démontrer un énoncé purement universel de la théorie des corps réels discrets (avec constantes dans **K**) on peut faire comme si **K** était un corps réel clos.

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

Bibliographie :

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

[Du] Dubois, D. W. : A nullstellensatz for ordered fields, Arkiv for Mat., Stockholm, t. 8, 1969, p. 111-114

[Efr] Efroymson, G. : Local reality on algebraic varieties, J. of Algebra, t. 29, 1974, p. 113-142.

[LR] Lombardi H., Roy M.-F. Théorie constructive élémentaire des corps ordonnés. 1989.

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

[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 Positivestellensatz in semialgebraic geometry. Math. Ann. 207, 87-97 (1974)

Annexe : le théorème algébrique des acrroissements finis

Exemple : Pour tout polynôme de degré ≤ 4 on a l'identité:

$P(a) - P(b) =$

$(a - b)\,(P'(a/6 + 5b/6)/3 + P'(a/3 + 2b/3)/6 + P'(2a/3 + b/3)/6 + P'(5a/6 + b/6)/3)$

Plus généralement on a les résultats suivants :

Lemme :

Il existe deux suites $(\lambda_{i,j})_{1\leq i\leq j;j=1,2,...,n,...}$ et $(r_{i,j})_{1\leq i\leq j;j=1,2,...,n,..}$ de rationnels $\in]\,0\,,\,1\,[$ telles que, pour tout polynôme $P \in \mathbb{Q}\,[X]$ de degré $\leq n$, on ait :

$$P(a) - P(b) = (a - b) \times \sum_{i=1}^{n} r_{i,n} \,.\, P'(a + \lambda_{i,n}(b - a))$$

Théorème 1 : (théorème des accroissements finis)

Il existe deux suites $(\lambda_{i,j})_{1\leq i\leq j;j=1,2,...,n,...}$ et $(r_{i,j})_{1\leq i\leq j;j=1,2,...,n,..}$ de rationnels $\in]\,0\,,\,1\,[$ telles que, pour tout corps ordonné $\mathbf{K}$ et tout polynôme $P \in \mathbf{K}[X]$ de degré $\leq n$, on ait :

$$P(a) - P(b) = (a - b) \times \sum_{i=1}^{n} r_{i,n} \,.\, P'(a + \lambda_{i,n}(b - a))$$

En particulier,

1) si P' est de signe positif sur un intervalle, la fonction polynôme est croissante sur cet intervalle.

2) sur tout intervalle borné, le taux de variation de P est majoré (la fonction définie par P est lipschitzienne sur tout intervalle borné)

preuve> Le théorème est une conséquence immédiate du lemme: ce dernier fournit en effet des identités algébriques concernant les variables " a, b, et les coefficients du polynôme " qui s'appliquent alors dans tout anneau commutatif qui est une $\mathbb{Q}$ -algèbre, et en particulier dans les corps commutatifs de caractéristique nulle.

Démontrons le lemme.

Par changement de variable affine, on se ramène au cas où $a = -1$ et $b = 1$. Considérons le degré n fixé. L'application $P \longmapsto P(1) - P(-1)$ est une forme linéaire ne faisant pas intervenir le coefficient constant. Les formes linéaires ne faisant pas intervenir le coefficient constant forment un espace de dimension n . Pour tout choix de n rationnels $\lambda_{i,n}$, les formes linéaires $P \longmapsto P'(\lambda_{i,n})$ sont indépendantes et ne font pas intervenir le coefficient constant. Il correspond donc à ce choix des rationnels $r_{i,n}$ qui rendent la formule vraie. La difficulté consiste à déterminer des $\lambda_{i,n} \in]\,0\,,\,1\,[$ tels que les $r_{i,n}$ correspondants soient également sur $]\,0\,,\,1\,[$. Les formules de quadrature de Gauss correspondent à un tel choix, mais avec des réels alors que nous voulons des rationnels. Il suffit alors de choisir des $\lambda_{i,n}$ rationnels suffisamment voisins des $\lambda_{i,n}$ de Gauss (zéros des polynômes de Legendre) pour que les $r_{i,n}$ correspondants restent positifs. ❑

Université de Franche-Comté
UFR des Sciences et Techniques
Laboratoire de Mathématiques
25030 BESANCON CEDEX