

THEOREME DES ZEROS REEL EFFECTIF
ET VARIANTES

Théorème des zéros réel effectif et variantes

1) Introduction	
2) Incompatibilités, évidences et implications fortes	
Notations et définitions	2
Incompatibilités fortes (définitions)	2
Quelques implications fortes triviales	4
Constructions d'implications fortes	5
Quelques exemples de constructions d'implications fortes	5
Le raisonnement par séparation des cas (selon le signe d'un polynôme)	5
Transitivité des implications fortes	7
Formules de Taylor mixtes (l'évidence forte du lemme de Thom).....	7
3) Existence potentielle	
Notations et définitions	10
Quelques règles de manipulation des énoncés d'existence potentielle	11
Existences potentielles fondamentales.....	13
4) Evidence forte des faits explicités par un tableau de Hormander	
Nullstellensatz réel en une variable	17
Une nouvelle preuve de l'existence et unicité de la clôture réelle d'un corps ordonné	22
5) Stellensatz réel effectif	22
Bibliographie :	26
Annexe : version algébrique du théorème des accroissements finis	27

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 $K[X_1, X_2, \dots, X_n]$ et impossible à satisfaire dans la clôture réelle de K , une identité algébrique dans $K[X_1, X_2, \dots, X_n]$ 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 réel, 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 field K , a uniformly primitive recursive algorithm that computes, for the input "a system of generalized signs conditions (gsc) on polynomials of $K[X_1, X_2, \dots, X_n]$ 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 K , X désigne une liste de variables X_1, X_2, \dots, X_n nous notons donc $K[X]$ l'anneau des polynômes $K[X_1, X_2, \dots, X_n]$.

Etant donnée une partie finie F de $K[X]$:

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 \mathbf{K} , P est dans $\mathcal{M}(F)$, Q est dans $\mathbf{K}[X]$. 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 $\mathbf{K}[X]$: $F_{>}$, F_{\geq} , $F_{=}$, F_{\neq} , contenant des polynômes auxquels on souhaite imposer respectivement les conditions de signes > 0 , ≥ 0 , $= 0$, $\neq 0$, on dira que $F = [F_{>} ; F_{\geq} ; F_{=} ; F_{\neq}]$ est *fortement incompatible* dans \mathbf{K}^1 si on a une égalité dans $\mathbf{K}[X]$ du type suivant :

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

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

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

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 \mathbf{K} .

Si on considère la clôture réelle \mathbf{R} de \mathbf{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 " $P=0, -Q \geq 0$ 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:

$$[S_1 > 0, \dots, S_i > 0, P_1 \geq 0, \dots, P_j \geq 0, Z_1 = 0, \dots, Z_k = 0, N_1 \neq 0, \dots, N_h \neq 0] \stackrel{\text{fort}}{\Rightarrow} Q \tau 0$$

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) : $Q_1 \tau_1 0, \dots, Q_k \tau_k 0$. Alors nous écrirons :

$$\mathbb{H} \stackrel{\text{fort}}{\Rightarrow} \mathbb{H}' \quad \text{pour signifier} \quad (\mathbb{H} \stackrel{\text{fort}}{\Rightarrow} Q_1 \tau_1 0) \quad \text{et} \quad \dots \quad \text{et} \quad (\mathbb{H} \stackrel{\text{fort}}{\Rightarrow} Q_k \tau_k 0)$$

¹ A priori, il faudrait parler d'"incompatibilité forte dans $\mathbf{K}[X]$ ", 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 $\mathbf{K}[X]$.

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 $\mathbf{K}[X]$, 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]), Efrogmson ([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 *positivstellensatz* 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 *nichtnegativstellensatz* 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.

$$\begin{array}{lcl}
 [U > 0, V > 0] & \stackrel{\text{fort}}{\Rightarrow} & [U+V > 0, U.V > 0] \\
 [U+V \geq 0, U.V > 0] & \stackrel{\text{fort}}{\Rightarrow} & [U > 0, V > 0] \\
 [U > 0, V \geq 0] & \stackrel{\text{fort}}{\Rightarrow} & U+V > 0 \\
 [U \geq 0, U.V > 0] & \stackrel{\text{fort}}{\Rightarrow} & V > 0 \\
 U \neq 0 & \stackrel{\text{fort}}{\Rightarrow} & U^2 > 0 \\
 U^2 > 0 & \stackrel{\text{fort}}{\Rightarrow} & U \neq 0 \\
 U = 0 & \stackrel{\text{fort}}{\Rightarrow} & U.V = 0 \\
 U = V & \stackrel{\text{fort}}{\Rightarrow} & P(X,U) = P(X,V) \\
 [U = V, V \tau 0] & \stackrel{\text{fort}}{\Rightarrow} & U \tau 0 \quad (\cdot \tau 0 \text{ est une csg}) \\
 [U = 0, V \tau 0] & \stackrel{\text{fort}}{\Rightarrow} & (U+V) \tau 0 \\
 [] & \stackrel{\text{fort}}{\Rightarrow} & [1 + U^2 > U, 1 + U^2 > -U]
 \end{array}$$

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 $U(X)$ et $V(X)$.

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_{ons}

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

$$(H \stackrel{\text{fort}}{\Rightarrow} H' \text{ et } H' \stackrel{\text{fort}}{\Rightarrow} H'') \vdash_{\text{ons}} (H \stackrel{\text{fort}}{\Rightarrow} H'')$$

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

$$(H(X,W) \stackrel{\text{fort}}{\Rightarrow} H'(X,W)) \vdash_{\text{ons}} (H(X,P(X)) \stackrel{\text{fort}}{\Rightarrow} H'(X,P(X)))$$

Quelques exemples de constructions d'implications fortes

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

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

$$(H \stackrel{\text{fort}}{\Rightarrow} Q > 0) \vdash_{\text{ons}} (H \stackrel{\text{fort}}{\Rightarrow} Q \geq 0)$$

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

$$((H \stackrel{\text{fort}}{\Rightarrow} Q < 0) \text{ et } (H \stackrel{\text{fort}}{\Rightarrow} Q \geq 0)) \vdash_{\text{ons}} (H \stackrel{\text{fort}}{\Rightarrow} Q = 0).$$

De même :

$$((H \stackrel{\text{fort}}{\Rightarrow} Q < 0) \text{ et } (H \stackrel{\text{fort}}{\Rightarrow} Q \neq 0)) \vdash_{\text{ons}} (H \stackrel{\text{fort}}{\Rightarrow} Q < 0)$$

$$\text{et } ((H \stackrel{\text{fort}}{\Rightarrow} Q = 0) \text{ et } (H \stackrel{\text{fort}}{\Rightarrow} Q \neq 0)) \vdash_{\text{ons}} (H \stackrel{\text{fort}}{\Rightarrow} 1 = 0)$$

Théorème 7 : (raisonnement cas par cas, selon le signe d'un polynôme)

Pour démontrer que 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 $K[X]$ contenant des polynômes auxquels sont attribués les conditions de signes > 0 , ≥ 0 , $= 0$, $\neq 0$ dans l'hypothèse H .$$

L'hypothèse $H \stackrel{\text{fort}}{\Rightarrow} Q < 0$ se réécrit $[H, Q > 0] \stackrel{\text{fort}}{\Rightarrow} 1 = 0$ 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 $H \stackrel{\text{fort}}{\Rightarrow} Q \gg 0$ 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 :

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

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: $(H \stackrel{\text{fort}}{\Rightarrow} Q = 0)$.

Voyons maintenant la construction:

$$((H \stackrel{\text{fort}}{\Rightarrow} Q \leq 0) \text{ et } (H \stackrel{\text{fort}}{\Rightarrow} Q \neq 0)) \stackrel{\text{cons}}{\Rightarrow} (H \stackrel{\text{fort}}{\Rightarrow} Q < 0)$$

L'implication forte $(H \stackrel{\text{fort}}{\Rightarrow} Q \leq 0)$ correspond à une équation :

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

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

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

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 :

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

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

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

Voyons enfin la construction:

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

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

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

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

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

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 :

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

$$S_1.S_4 \in \mathcal{M}(F_{>}^{*2} \cup F_{\neq}^{*2}), P_1.(Y_4)^2, S_1.P_4 + R_1.(Y_4)^2 \in Cp(F_{\geq} \cup F_{>}), S_1.Z_4 + Z_1.(Y_4)^2$$

$\in I(F_{=})$ ce qui est bien l'implication forte cherchée \square

Transitivité des implications fortes

Théorème 8 :

Soient H, H', H'' trois systèmes de csg portant sur des polynômes de $K[X]$.

Alors: $\{ (H \xrightarrow{\text{fort}} H') \text{ et } ([H, H'] \xrightarrow{\text{fort}} H'') \} \vdash_{\text{ons}} (H \xrightarrow{\text{fort}} H'')$

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

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

Corollaire : $(H \xrightarrow{\text{fort}} [P.Q > 0, Q \geq 0]) \vdash_{\text{ons}} (H \xrightarrow{\text{fort}} P > 0)$

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 K ou plus généralement dans un anneau commutatif 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 $\deg(P) \leq 2$, 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 $\deg(P) \leq 3$, 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 suivantes¹:

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

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

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

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

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 ≤ 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 $\deg(P) \leq 4$, 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 suivantes¹:

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

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 :

$$\begin{aligned} P(U) - P(V) &= (\Delta/6) (2.P'(U/6 + 5V/6) + P'(U/3 + 2V/3) + \dots + \dots) \\ &= (\Delta/6) (2.P'(U_1) + P'(U_2) + P'(U_3) + 2.P'(U_4)) \end{aligned}$$

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

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

où les c_i 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:

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

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

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

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 $\Delta^{i-1} P^{(i-1)}(U)$ \square

Théorème 10 : (évidence forte du lemme de Thom)

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

On note \mathbb{H} le système de csg : $P'(X,U) \equiv \sigma_1, \dots, P^{(i)}(X,U) \equiv \sigma_i, \dots, P^{(d)}(X,U) \equiv \sigma_d$,

$P'(X,V) \equiv \sigma_1, \dots, P^{(i)}(X,V) \equiv \sigma_i, \dots, P^{(d)}(X,V) \equiv \sigma_d$ (dérivées par rapport à T).

On a alors les évidences fortes suivantes :

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

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

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

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

$$[\mathbb{H}, P^{(i)}(X,W) \neq \sigma_i] \stackrel{\text{fort}}{\Rightarrow} (W - U).(W - V) > 0 \quad (i = 1, \dots, d) \quad (\text{e})$$

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

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

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 $P^{(i)}$. \square

On remarquera que le (b) permet de rendre fortement évident le signe de $u - v$ lorsque u est un élément de \mathbf{R} codé à la Thom dans \mathbf{K} et v un élément de \mathbf{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 $H \stackrel{\text{fort}}{\Rightarrow} H'$ est une forme forte (par identité algébrique) pour l'implication *universelle* correspondante : $\forall X (H \Rightarrow H')$.

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 :

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

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:

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

Définition 11 :

Soient H_1 un système de csg portant sur des polynômes de $K[X]$, H_2 un système de csg portant sur des polynômes de $K[X, T_1, T_2, \dots, T_m] = K[X, T]$.

Nous dirons que *les hypothèses H_1 autorisent l'existence des T_i vérifiant H_2* lorsque, pour tout système de csg H portant sur des polynômes de $K[X, Y]$, on a la construction d'implication forte :

$$([\ H_2(X, T) \ , \ H(X, Y) \] \stackrel{\text{fort}}{\Rightarrow} 1 = 0) \text{ cons } ([\ H_1(X) \ , \ H(X, Y) \] \stackrel{\text{fort}}{\Rightarrow} 1 = 0).$$

Nous parlerons également *d'existence potentielle des T_i vérifiant H_2 sous les hypothèses H_1*

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

Notation : Nous noterons cette existence potentielle par : $H_1 \longrightarrow \tilde{\exists} T \ H_2$.

Nous pouvons préciser de plus les variables sur lesquelles portent les systèmes de csg, nous écrivons alors :

$$H_1(X) \longrightarrow \tilde{\exists} T \ H_2(X, T).$$

Lorsque le système H_1 est vide, nous utiliserons la notation $\tilde{\exists} T \ H_2$.

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 :

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

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 L est une extension ordonnée de K il n'y a pas de relation évidente a priori entre un énoncé $H_1(X) \longrightarrow \tilde{\exists} T \ H_2(X, T)$ lu dans K et le même énoncé lu dans 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 :

$$([H_2, H_1, H] \xrightarrow{\text{fort}} 1=0) \text{ c}_{\text{ons}} ([H_1, H] \xrightarrow{\text{fort}} 1=0)$$

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

$$([H_2, H_1, H] \xrightarrow{\text{fort}} H') \text{ c}_{\text{ons}} ([H_1, H] \xrightarrow{\text{fort}} H')$$

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 $H_1(X) \longrightarrow \exists T H_2(X,T)$ reste vraie si on affaiblit la conclusion, si on renforce l'hypothèse, ou si on supprime derrière \exists des variables ne figurant pas dans $H_2(X,T)$.

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

Si $H_1(X) \longrightarrow \exists T H_2(X,T)$ alors

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

(rappel de l'hypothèse dans la conclusion)

Si $H_1(X) \longrightarrow \exists T H_2(X,T)$ alors $H_1(X) \longrightarrow \exists T [H_2(X,T), H_1(X)]$

preuve> immédiat, le 2^{ème} point était l'objet de la remarque 4 \square

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 $H_1(X) \longrightarrow \exists T H_2(X)$ si et seulement si $H_1(X) \xrightarrow{\text{fort}} H_2(X)$.

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

Voyons l'implication dans l'autre sens. Soit $H(X,Y)$ un système de csg et supposons que $[H_2(X), H(X,Y)] \xrightarrow{\text{fort}} 1=0$. D'après l'hypothèse, on a évidemment : $[H_1(X), H(X,Y)] \xrightarrow{\text{fort}} [H_2(X), H(X,Y)]$. Il suffit d'appliquer la transitivité des implications fortes pour obtenir $[H_1(X), H(X,Y)] \xrightarrow{\text{fort}} 1=0$. \square

Proposition 15 : (raisonnement cas par cas)

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

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

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

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

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

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

Si $\mathbb{H}_1(X) \xrightarrow{\text{fort}} \mathbb{H}_2(X, P(X))$ alors $\mathbb{H}_1(X) \longrightarrow \exists T \mathbb{H}_2(X, T)$

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

Théorème 17 : (transitivité dans les existences potentielles)

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

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

alors on a aussi:

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

preuve> Immédiat d'après la définition. \square

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

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

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

preuve> Supposons qu'on ait

$$[\mathbb{H}_2(P(Z), T), \mathbb{H}(Z, Y)] \xrightarrow{\text{fort}} 1 = 0 \quad (1)$$

On veut construire

$$[\mathbb{H}_1(P(Z)), \mathbb{H}(Z, Y)] \xrightarrow{\text{fort}} 1 = 0 \quad (2)$$

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

Par transitivité (1) et (3) donnent :

$$[\mathbb{H}_2(X, T), \mathbb{H}(Z, Y), X = P(Z)] \xrightarrow{\text{fort}} 1 = 0 \quad (4)$$

Par définition de l'existence potentielle on sait construire:

$$[\mathbb{H}_1(X), \mathbb{H}(Z, Y), X = P(Z)] \xrightarrow{\text{fort}} 1 = 0 \quad (5)$$

Par ailleurs :

$$[\mathbb{H}_1(P(Z)), \mathbb{H}(Z, Y), X = P(Z)] \xrightarrow{\text{fort}} [\mathbb{H}_1(X), \mathbb{H}(Z, Y), X = P(Z)] \quad (6)$$

Par transitivité (5) et (6) donnent :

$$[\mathbb{H}_1(P(Z)), \mathbb{H}(Z, Y), X = P(Z)] \xrightarrow{\text{fort}} 1 = 0 \quad (7)$$

En substituant $P(Z)$ à X dans (7) , on obtient (2) \square

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:

$$U \succ 0 \longrightarrow \exists T \quad U = T^2$$

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 : $\mathbf{K}[\mathbf{X}, T] = \mathbf{K}[X_1, X_2, \dots, X_n, T]$.

On veut expliciter la construction:

$$([\mathbb{H}, U - T^2 = 0] \stackrel{\text{fort}}{\Rightarrow} 1 = 0) \stackrel{\text{cons}}{\Leftarrow} ([\mathbb{H}, U \succ 0] \stackrel{\text{fort}}{\Rightarrow} 1 = 0).$$

L'hypothèse correspond à une équation :

$$S_1(\mathbf{X}) + P_1(\mathbf{X}, T) + (U - T^2) \cdot Y_1(\mathbf{X}, T) + Z_1(\mathbf{X}, T) = 0 \text{ avec } S_1 \in \mathcal{M}(F_{>}^{*2} \cup F_{\neq}^{*2}), \\ P_1 \in Cp'(F_{\geq} \cup F_{>}), Z_1 \in I'(F_{=}).$$

Plus précisément

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

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 $V_i(\mathbf{X}, T) = A_i(\mathbf{X}) + B_i(\mathbf{X}) \cdot T$, $W_j(\mathbf{X}, T) = C_j(\mathbf{X}) + D_j(\mathbf{X}) \cdot T$, on a :

$V_i^2(\mathbf{X}, T) = A_i^2(\mathbf{X}) + B_i^2(\mathbf{X}) \cdot T^2 + 2 \cdot A_i(\mathbf{X}) \cdot B_i(\mathbf{X}) \cdot T$, et comme T^2 peut être remplacé par U modulo $U - T^2$ on obtient :

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

Considérons le polynôme du premier membre comme un élément de $\mathbf{K}[X_1, X_2, \dots, X_n][T]$. Si $Y_2(\mathbf{X}, T)$ n'était pas nul, le monôme dominant en T du polynôme $-T^2 \cdot Y_2(\mathbf{X}, T)$ 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 :

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

Ceci est exactement une implication forte du type voulu. \square

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:

$$U \neq 0 \longrightarrow \exists T \quad 1 = U \cdot T$$

preuve > Mêmes notations qu'au théorème précédent. On veut expliciter la construction:

$$([\mathbb{H}, 1 - U \cdot T = 0] \stackrel{\text{fort}}{\Rightarrow} 1 = 0) \stackrel{\text{cons}}{\Leftarrow} ([\mathbb{H}, U \neq 0] \stackrel{\text{fort}}{\Rightarrow} 1 = 0).$$

L'hypothèse correspond à une équation :

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

Travaillons modulo $(1 - U \cdot T)$. 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:

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

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

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

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:

$$U > 0 \longrightarrow \exists T \quad 1 = U \cdot T^2$$

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

Par ailleurs $[U > 0, U = W^2] \stackrel{\text{fort}}{\implies} W \neq 0$ donc par transitivité :

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

Par ailleurs $W \neq 0 \longrightarrow \exists T \quad 1 = W \cdot T$ d'après le théorème 20, donc

par transitivité : $U > 0 \longrightarrow \exists W, T \quad [U = W^2, W \neq 0, 1 = W \cdot T]$

Enfin $[U = W^2, 1 = W \cdot T] \stackrel{\text{fort}}{\implies} 1 = U \cdot T^2$ donc par transitivité :

$$U > 0 \longrightarrow \exists W, T \quad [U = W^2, W \neq 0, 1 = W \cdot T, 1 = U \cdot T^2]$$

et a fortiori $U > 0 \longrightarrow \exists T \quad 1 = U \cdot T^2 \quad \square$

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 $\mathbf{K}[\mathbf{X}]$, 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 $\mathbf{K}[\mathbf{X}]$, l'impossibilité dans \mathbf{R} implique l'incompatibilité forte dans \mathbf{K} .

preuve > Considérons un système de csg portant sur des polynômes de $\mathbf{K}[\mathbf{X}]$. Si on a une csg $P > 0$ 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 $1 - Q \cdot T_Q^2 = 0$. Si on a une csg $R \neq 0$ on la remplace par $1 - R \cdot T_R = 0$. 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:

$$U > 0 \longrightarrow \exists T \quad U = T^2 \quad \text{permet de remplacer } P - T_p^2 = 0 \text{ par } P > 0 \quad (\text{théorème 19})$$

$U > 0 \longrightarrow \exists T \quad 1 = U.T^2$ permet de remplacer $1 - Q.T_Q^2 = 0$ par $Q > 0$ (corollaire 1)

$U \neq 0 \longrightarrow \exists T \quad 1 = U.T$ permet de remplacer $1 - R.T_R = 0$ par $R \neq 0$ (théorème 20) \square

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 : $P(X,U).P(X,V) \leq 0 \longrightarrow \exists W \quad P(X,W) = 0$

preuve > Nous faisons une preuve par récurrence¹ 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:

$([\mathbb{H}, P(X,W) = 0] \stackrel{\text{fort}}{\Rightarrow} 1 = 0) \stackrel{\text{cons}}{\Leftarrow} ([\mathbb{H}, P(X,U).P(X,V) \leq 0] \stackrel{\text{fort}}{\Rightarrow} 1 = 0)$

qui peut se relire :

$(\mathbb{H} \stackrel{\text{fort}}{\Rightarrow} P(X,W) \neq 0) \stackrel{\text{cons}}{\Leftarrow} (\mathbb{H} \stackrel{\text{fort}}{\Rightarrow} P(X,U).P(X,V) > 0)$

Supposons tout d'abord P unitaire.

L'implication forte $\mathbb{H} \stackrel{\text{fort}}{\Rightarrow} P(X,W) \neq 0$ 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 $Q_i(X) \in \mathcal{C}_P(F_{\geq} \cup F_{>})$ 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 $\deg(G) \leq \deg(P) - 2$. 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:

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

On déduit par substitution:

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

D'où : $\mathbb{H} \stackrel{\text{fort}}{\Rightarrow} P(X,U).G(X,U).P(X,V).G(X,V) > 0$

Par hypothèse de récurrence, on déduit de (1) que : $\mathbb{H} \stackrel{\text{fort}}{\Rightarrow} G(X,U).G(X,V) > 0$.

Enfin, on a trivialement:

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

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 $C(X)$.

1^{er} 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 $\mathbb{K}[W]/P(W)$ 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 : $[P(X,U).P(X,V) < 0 , C(X) = 0] \stackrel{\text{fort}}{\Rightarrow} G(X,U).G(X,V) < 0$

et par hypothèse de récurrence, on a :

$$G(X,U).G(X,V) < 0 \longrightarrow \exists W \ G(X,W) = 0$$

et comme :

$$[G(X,W) = 0 , C(X) = 0] \stackrel{\text{fort}}{\Rightarrow} P(X,W) = 0$$

on conclut par transitivité.

2^{ème} cas : $C(X) \neq 0$.

On a : $C(X) \neq 0 \longrightarrow \exists T \ 1 = C(X).T$, et : $1 = C(X).T \stackrel{\text{fort}}{\Rightarrow} P(X,W) = P_1(X,T,W)$

et donc :

$$[P(X,U).P(X,V) < 0 , C(X) \neq 0] \longrightarrow \exists T \ [1 = C(X).T , P_1(X,T,U).P_1(X,T,V) < 0]$$

Comme on a déjà traité le cas d'un polynôme unitaire on a :

$$[P_1(X,T,U).P_1(X,T,V) < 0] \longrightarrow \exists W \ P_1(X,T,W) = 0$$

On conclut alors facilement par transitivité \square

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 :

$$P(X,U).P(X,V) < 0 \longrightarrow \exists W \ [P(X,W) = 0 , P(X,U).P(X,V) < 0 , (W - U).(W - V) < 0]$$

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 :

$$P(X,U).P(X,V) < 0 \longrightarrow \exists W \ [P(X,W) = 0 , P(X,U).P(X,V) < 0,]$$

Nous allons démontrer l'existence potentielle :

$$P(X,U).P(X,V) < 0 \longrightarrow \exists W' \ [P(X,W') = 0 , P(X,U).P(X,V) < 0 , (W' - U).(W' - V) < 0]$$

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 :

1^{er} sous cas : $W - U = 0$, on obtient aisément $P(X,U) = P(X,W) = 0$, l'hypothèse

$H_1(X,W)$ est fortement incompatible, l'existence potentielle :

$H_1(X,W) \longrightarrow \exists W' \ H_2(X,W')$ est donc assurée.

2^{ème} sous cas : $W - U \neq 0$, on obtient aisément $W - V = 0$, on est ramené au premier sous cas

3^{ème} 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 $H_1(X,W)$ 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 :

$$H_1(X,W) \stackrel{\text{fort}}{\Rightarrow} P(T) = R(T).(T - W) , \text{ et donc aussi :}$$

$$H_1(X,W) \stackrel{\text{fort}}{\Rightarrow} [R(U).(W - U).R(V).(W - V) = P(U).P(V) < 0 , (W - U).(W - V) > 0]$$

et donc aussi

