THéORèME DES ZéROS RéEL EFFECTIF ET VARIANTES
(avec une majoration explicite des degrés)

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 Hörmander, 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.
L'article est complété par une annexe où est calculée une majoration explicite des degrés des polynômes dans l'identité algébrique construite.

Mots clés Théorème des zéros réels, Corps ordonné, Effectivité, Mathématiques constructives, Algorithme de Hörmander, 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 Hörmander algorithm, that is the conceptually simplest test for the impossibility of a gsc system in the real closure of an ordered field.
We have added to the paper the calculus of an explicit bound for the degrees of polynomials in the constructed algebraic identity.

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

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

Table des matières

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**.

Nous reprenons ici pour l'essentiel l'article [**Lom**a], avec quelques améliorations de détails (essentiellement des notations plus claires).

Nous avons de plus rajouté une annexe substantielle donnant une majoration explicite des degrés des polynômes dans l'identité algébrique qui est l'objet du théorème des zéros réels.

Une version anglaise abrégée peut être trouvée dans [**Lom**b]. Les résultats ont aussi été présentés dans une note au CRAS ([**Lom**c]).

Nous donnons une preuve constructive du théorème des zéros réel et de ses variantes. Le théorème général sur lequel sont basées ce théorème et ses variantes est le suivant (cf [**BCR**] théorème 4.4.2) : on considère un système d'égalités et inégalités portant sur des polynômes de $\mathbf{K}[\mathbf{X}] = \mathbf{K}[X_1,X_2,...,X_n]$, où **K** est un corps ordonné de clôture réelle **R** ; ce système définit une partie S de $\mathbf{R}^n$ (S est appelé un sous-ensemble semialgébrique) ; le théorème affirme que S est vide si et seulement si il y a une certaine identité algébrique construite à partir des polynômes donnés. (Pour plus de détails voir le début du § 2)

L'idée générale de notre preuve constructive 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 Hörmander (cf. la preuve du principe de Tarski-Seidenberg dans [**BCR**] chap. 1, et cet article § 4), 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 (cf [**LR**]).
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 obtenue 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, ..., X_n nous notons donc **K**[**X**] l'anneau des polynômes **K**[X_1,X_2,...,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 $M(F)$, et $M_2(F) := M(F^{*2})$. Nous noterons $M_1(F)$ la partie de $M(F)$ 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 $M(F)$, Q est dans **K**[**X**]. Nous le noterons $Cp(F)$[1]. On remarque que dans la définition, on pourrait supposer que P est dans $M_1(F)$, 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, ≥ 0, $= 0$, $\neq 0$, on dira que $\mathbf{F} = [F_> ; F_\geq ; F_= ; F_\neq]$ est *fortement incompatible* dans $\mathbf{K}^2$ si on a une égalité dans **K**[**X**] du type suivant :

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

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

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

Il suffit en effet de multiplier la première égalité par un élément convenable de $M_1(F_>)$ 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 Hörmander, 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:

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

---

1 On devrait à vrai dire noter $Cp(F,\mathbf{K}^+;\mathbf{K}[\mathbf{X}])$ pour indiquer que : a) les positifs de **K** sont dans le cône, b) on est dans l'anneau **K**[**X**].

2 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**] .

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 :
$^*(\mathbb{H} \Rightarrow \mathbb{H}')^*$ pour signifier $^*(\mathbb{H} \Rightarrow Q_1 \tau_1 0)^*$ et ..... et $^*(\mathbb{H} \Rightarrow Q_k \tau_k 0)^*$

Remarque : On pourrait obtenir une version "identité algébrique" pour toute formule sans quantificateur du langage de la théorie des anneaux ordonnés avec constantes dans **K**.

Le théorème des zéros réels et ses variantes :
Les différentes variantes du théorème des zéros dans le cas réel sont conséquence du théorème général suivant :

Théorème : Soit **K** un corps ordonné et **R** une extension réelle close de **K**. Les trois faits suivants, concernant un système de csg portant sur des polynômes de **K**[**X**], sont équivalents :

l'incompatibilité forte dans **K**

l'impossibilité dans **R**

l'impossibilité dans toutes les extensions ordonnées de **K**

Ce théorème des zéros réels remonte à 1974 ([**Ste**]). Des variantes plus faibles ont été établies par Krivine ([**Kri**]), 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.
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). Enonçons par exemple la forme générale géométrique du positivestellensatz.

Théorème : (Positivestellensatz) Soit **K** un corps ordonné et **R** une extension réelle close de **K**. Soit A l'ensemble semi algebrique dans $\mathbf{R}^n$ defini par :
$A = \{\mathbf{x} \in \mathbf{R}^n : S_1(\mathbf{x}) > 0,...,S_i(\mathbf{x}) > 0, P_1(\mathbf{x}) \geq 0,...,P_j(\mathbf{x}) \geq 0, Z_1(\mathbf{x}) = 0,...,Z_k(\mathbf{x}) = 0,$
$N_1(\mathbf{x}) \neq 0,...,N_h(\mathbf{x}) \neq 0 \}$
Soit $Q \in \mathbf{K}[\mathbf{X}]$. Alors Q est strictement positif en chaque point de A si et seulement si on a une identité algébrique : $Q.P = S.N^2 + R + Z$
où : P et R sont dans le cône positif de **K**[**X**] : $Cp(S_1,...,S_i, P_1,...,P_j)$

Z est dans l'idéal de $\mathbf{K}[\mathbf{X}]$: $I(Z_1,...,Z_k)$

S est dans le monoïde $M(S_1,...,S_i)$ et N dans le monoïde $M(N_1,...,N_h)$

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.

$$\begin{aligned}
{}^*([\,U>0,\,V>0\,] &\Rightarrow [\,U+V>0,\,U.V>0\,])^*\\
{}^*([\,U+V\geq 0,\,U.V>0\,] &\Rightarrow [\,U>0,\,V>0\,])^*\\
{}^*([\,U>0,\,V\geq 0\,] &\Rightarrow U+V>0)^*\\
{}^*([\,U\geq 0,\,U.V>0\,] &\Rightarrow V>0)^*\\
{}^*(U\neq 0 &\Rightarrow U^2>0)^*\\
{}^*(U^2>0 &\Rightarrow U\neq 0)^*\\
{}^*(U=0 &\Rightarrow U.V=0)^*\\
{}^*(U=V &\Rightarrow P(\mathbf{X},U)=P(\mathbf{X},V))^*\\
{}^*([\,U=V\,,\,V\,\tau\,0\,] &\Rightarrow U\,\tau\,0)^* \quad (\bullet\,\tau\,0 \text{ est une csg})\\
{}^*([\,W=0,\,U=V+W.Z\,] &\Rightarrow U=V)^*\\
{}^*([\,W=0,\,U=V+W.Z\,,\,V\,\tau\,0\,] &\Rightarrow U\,\tau\,0)^*\\
{}^*([\,] &\Rightarrow [\,1+U^2>U\,,\;1+U^2>-U\,])^*
\end{aligned}$$

une preuve> Par exemple l'avant-dernière implication forte dans le cas où τ est $>$. Nous devons donner une incompatibilité forte entre les csg :

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

nous pouvons prendre :

$$V^2+((-U).V)+((Z.V).W+(-V).(V+W.Z-U))=0 \quad \text{avec}$$

$V^2\in M(F_>{}^{*2}\cup F_{\neq}{}^{*2})$, $(-U).V\in Cp(F_{\geq}\cup F_>)$, $(Z.V).W+(-V).(V+W.Z-U)\in I(F_=)$ ❑

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" : $\vdash_{\overline{\text{cons}}}$

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

$$[\,{}^*(\mathbb{H}\Rightarrow\mathbb{H}')^*\ \text{et}\ {}^*(\mathbb{H}'\Rightarrow\mathbb{H}'')^*\,]\ \vdash_{\overline{\text{cons}}}\ {}^*(\mathbb{H}\Rightarrow\mathbb{H}'')^*$$

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

$$ {}^*(\mathbb{H}(\mathbf{X},W) \Rightarrow \mathbb{H}'(\mathbf{X},W))^* \quad |\!\!-_{\overline{cons}} \; {}^*(\mathbb{H}(\mathbf{X},P(\mathbf{X})) \Rightarrow \mathbb{H}'(\mathbf{X},P(\mathbf{X})))^* $$

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 $\mathbf{K}[\mathbf{X}]$, Q un élément de $\mathbf{K}[\mathbf{X}]$. Alors toute implication forte du type ${}^*(\mathbb{H} \Rightarrow Q \,\tau\, 0)^*$ (où τ est $=$, $<$ ou $>$) fournit par relecture toute implication forte "plus faible" ${}^*(\mathbb{H} \Rightarrow Q \,\tau' \, 0)^*$. Par exemple, on a : ${}^*(\mathbb{H} \Rightarrow Q > 0)^* \; |\!\!-_{\overline{cons}} \; {}^*(\mathbb{H} \Rightarrow Q \geq 0)^*$

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

$[{}^*(\mathbb{H} \Rightarrow Q \leq 0)^* \text{ et } {}^*(\mathbb{H} \Rightarrow Q \geq 0)^*] \; |\!\!-_{\overline{cons}} \; {}^*(\mathbb{H} \Rightarrow Q = 0)^*$.

De même :

$[{}^*(\mathbb{H} \Rightarrow Q \leq 0)^* \text{ et } {}^*(\mathbb{H} \Rightarrow Q \neq 0)^*] \; |\!\!-_{\overline{cons}} \; {}^*(\mathbb{H} \Rightarrow Q < 0)^*$

et $[{}^*(\mathbb{H} \Rightarrow Q = 0)^* \text{ et } {}^*(\mathbb{H} \Rightarrow Q \neq 0)^*] \; |\!\!-_{\overline{cons}} \; {}^*(\mathbb{H} \Rightarrow 1 = 0)^*$.

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 $\mathbf{K}[\mathbf{X}]$ contenant des polynômes auxquels sont attribués les conditions de signes > 0, ≥ 0, $= 0$, $\neq 0$ dans l'hypothèse $\mathbb{H}$.
L'hypothèse ${}^*(\mathbb{H} \Rightarrow Q \leq 0)^*$ se réécrit ${}^*([\ \mathbb{H}, Q > 0\ ] \Rightarrow 1 = 0)^*$ et signifie qu'on a une égalité :

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

c.-à-d. encore :

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

De même l'hypothèse ${}^*(\mathbb{H} \Rightarrow Q \geq 0)^*$ signifie qu'on a une égalité :

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

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 :

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

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

Voyons maintenant la construction:

$$[\ {}^*(\ \mathbb{H}\ \Rightarrow\ Q \le 0\ )^*\ \text{ et }\ {}^*(\ \mathbb{H}\ \Rightarrow\ Q \ne 0\ )^*\ ]\ \vdash_{\overline{cons}}\ {}^*(\ \mathbb{H}\ \Rightarrow\ Q < 0\ )^*$$

L'implication forte ${}^*(\ \mathbb{H}\ \Rightarrow\ Q \le 0\ )^*$ correspond à une équation :

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

L'implication forte ${}^*(\ \mathbb{H}\ \Rightarrow\ Q \ne 0\ )^*$ correspond à une équation :

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

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 $S_4 \in M(F_>^{*2} \cup F_{\ne}^{*2})$, $P_4 \in Cp(F_{\ge} \cup F_>)$, $Z_4 \in I(F_=)$

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

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

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

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

Voyons enfin la construction:

$$[\ {}^*(\ \mathbb{H}\ \Rightarrow\ Q = 0\ )^*\ \text{ et }\ {}^*(\ \mathbb{H}\ \Rightarrow\ Q \ne 0\ )^*\ ]\ \vdash_{\overline{cons}}\ {}^*(\ \mathbb{H}\ \Rightarrow\ 1 = 0\ )^*$$

Répéter la construction précédente, avec le terme $Q.P_1$ en moins au départ et le terme $Q.P_1.(Y_4)^2$ en moins à l'arrivée. ❑

Transitivité des implications fortes

Théorème 8 :

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

Alors: $[\ {}^*(\ \mathbb{H}\ \Rightarrow\ \mathbb{H}'\ )^*\ \text{ et }\ {}^*(\ [\ \mathbb{H},\ \mathbb{H}'\ ]\ \Rightarrow\ \mathbb{H}''\ )^*\ ]\ \vdash_{\overline{cons}}\ {}^*(\ \mathbb{H}\ \Rightarrow\ \mathbb{H}''\ )^*$

preuve> Il suffit d'enlever une à une les hypothèses de $\mathbb{H}'$ dans ${}^*(\ [\ \mathbb{H},\ \mathbb{H}'\ ]\ \Rightarrow\ \mathbb{H}''\ )^*$. 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 :

$${}^*(\ \mathbb{H} \Rightarrow Q\ \tau\ 0\ )^* \quad \text{et} \quad {}^*(\ [\ \mathbb{H}, Q\ \tau\ 0, \mathbb{A}\ ] \Rightarrow 1 = 0\ )^*,$$

(où $\mathbb{A}$ est une csg portant sur un polynôme) alors on peut construire l'implication forte

$${}^*(\ [\ \mathbb{H}, \mathbb{A}\ ] \Rightarrow 1 = 0\ )^* \quad .$$

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 (exemple) **:** ${}^*(\ \mathbb{H}\ \Rightarrow\ [\ P.Q > 0, Q \ge 0\ ]\ )^*\ \vdash_{\overline{cons}}\ {}^*(\ \mathbb{H}\ \Rightarrow\ P > 0\ )^*$

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 $\deg(P) \leq 2$, 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 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 :

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

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 suivantes[2]:

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

Comme toutes les combinaisons de signes possibles se présentent, on obtient : si U et V attribuent la même suite de signes aux dérivées d'un polynôme P de degré ≤ 4, alors on a les évidences fortes que $P(U) - P(V)$ et $(U - V).P'(U)$ ont le même signe. (cela correspond à 6 implications fortes).

Inversement si U et V n'attribuent pas la même suite de signes pour un polynôme P de degré ≤ 4 et ses dérivées successives, alors on a l'évidence forte qui donne le signe de $U - V$ à partir des signes des $P^{(i)}(U)$ et des $P^{(i)}(V)$: 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 a donc l'évidence forte de faits énoncés dans le lemme de Thom.

---

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 .

2 Même preuve, en vérifiant pour U^4 .

Théorème 9 : (formule de Taylor mixte)

Pour chaque degré s, il y a 2^{s-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:

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

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 et majorations 10 : (évidence forte du lemme de Thom)

Soit T une variable distincte des X_i. Soit $P \in \mathbf{K}[\mathbf{X}][T]$, de degré s en T , $\sigma_1, \sigma_2, ..., \sigma_s$ une liste formée de $<$ ou $>$.

On note $\mathbb{H}(\mathbf{X},T)$ ou $\mathbb{H}(T)$ le système de csg : $P'(\mathbf{X},T)\ \sigma_1\ 0, ..., P^{(i)}(\mathbf{X},T)\ \sigma_i\ 0, ..., P^{(s)}(\mathbf{X},T)\ \sigma_s\ 0$ (les dérivées sont par rapport à T).

Soit $\mathbb{H}'(T)$ le système de csg obtenu à partir de $\mathbb{H}(T)$ en relachant toutes les conditions de signe sauf celle relative à $P^{(s)}$.

Soit $\mathbb{H}_1(T)$ le système de csg : $P^{(s)}(\mathbf{X},T) > 0$, $P^{(i)}(\mathbf{X},T) \geq 0$, i = 1, ..., s–1 .

On a alors les évidences fortes suivantes :

$$^*(\ [\ \mathbb{H}'(U),\ \mathbb{H}'(V),\ P(U) = P(V)\ ]\ \Rightarrow\ U = V\ )^* \qquad (1)$$

$$^*(\ [\ \mathbb{H}'(U),\ \mathbb{H}'(V)\ ,\ U\ \sigma_1\ V\ ]\ \Rightarrow\ P(U) > P(V)\ )^* \qquad (2,a)$$

$$^*(\ [\ \mathbb{H}'(U),\ \mathbb{H}'(V)\ ,\ P(U)\ \sigma_1\ P(V)\ ]\ \Rightarrow\ U > V\ )^* \qquad (2,b)$$

$$^*(\ [\ \mathbb{H}_1(U),\ V > U\ ]\ \Rightarrow\ P(V) > P(U)\ )^* \qquad (2,c)$$

$^*([\, \mathbb{H}_1(U),\ P(U) > P(V)\,] \ \Rightarrow\ U > V)^*$ (2,d)

$^*([\, \mathbb{H}(U),\ \mathbb{H}(V),\ (Z-U).(Z-V) \le 0\,] \ \Rightarrow\ \mathbb{H}(Z))^*$ (3)

$^*([\, \mathbb{H}(U),\ \mathbb{H}(V),\ P^{(i)}(Z)\ \mathfrak{G}_i\ 0\,] \Rightarrow (Z-U).(Z-V) > 0)^*$ (i = 1,...,s) (4)

$^*([\, \mathbb{H}'(U)\ ,\ \mathbb{H}'(V),\ U < Z < V\,] \ \Rightarrow\ \mathbb{H}(Z))^*$ (5)

preuve> Les implications fortes (2) sont donnés par une formule de Taylor mixte pour P. L'implication forte (1) résulte de l'implication forte (2,a) et de l'implication forte "symétrique" provenant de l'échange de U et V.

Les s implications fortes de (5) :

$^*([\, \mathbb{H}'(U)\ ,\ \mathbb{H}'(V), U < Z < V] \Rightarrow P^{(i)}(Z)\ \sigma_i\ 0)^*$ (i = 1,...,s)

se démontrent de proche en proche, pour i décroissant de s à 1, en utilisant pour la dérivée i-ème une formule de Taylor mixte pour $P^{(i)}$, et en utilisant une formule précédemment écrite chaque fois qu'intervient un $P^{(j)}(Z)$ avec $j > i$: cf. l'exemple qui suit. Le fait de supposer $P^{(s)}$ avec un signe strict permet d'avoir un terme qui assure le signe strict de $P^{(i)}(\mathbf{X},Z)$ lorsqu'on utilise une formule de Taylor mixte relative à $P^{(i)}$.

Les implications fortes (3) et (4) sont identiques.

Les s implications fortes de (3) peuvent se démontrer cas par cas, selon les positions relatives de U, V, Z en utilisant dans les cas non triviaux les formules établies pour les implications fortes (5) ❑

On remarquera que le (2) 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** .

Un exemple : Considérons le polynôme générique de degré 4

$$P(X) = c_0 X^4 + c_1 X^3 + c_2 X^3 + c_3 X^2 + c_4 X^4 + c_5$$

Et soit $\mathbb{H}(U)$: $P(U) > 0,\ P'(U) < 0,\ P^{(2)}(U) < 0,\ P^{(3)}(U) < 0,\ P^{(4)}(U) = 24\, c_0 = c > 0.$

Donc $\mathbb{H}'(U)$: $P(U) \ge 0,\ P'(U) \le 0,\ P^{(2)}(U) \le 0,\ P^{(3)}(U) \le 0,\ P^{(4)}(U) = 24\, c_0 = c > 0.$

On écrit les formules de Taylor mixtes suivantes :

$\alpha)$ $P^{(3)}(Z) = P^{(3)}(V) + c\,(Z - V)$

$\beta)$ $P^{(2)}(Z) = P^{(2)}(U) + P^{(3)}(Z).(Z - U) - c/2\,(Z - U)^2$

$\gamma)$ $P'(Z) = P'(U) + P^{(2)}(U).(Z - U) + 1/2\, P^{(3)}(Z).(Z - U)^2 - c/3\,(Z - U)^3$

$\delta)$ $P(Z)=P(V)+P'(Z).(Z - V) - 1/2P^{(2)}(Z).(Z - V)^2+1/6P^{(3)}(V).(Z - V)^3+c/8(Z - V)^4$

Dans $\beta)$ on remplace $P^{(3)}(Z)$ par son expression donnée dans $\alpha)$ et on obtient :

$\beta')$ $P^{(2)}(Z) = P^{(2)}(U) + P^{(3)}(V).(Z - U) + c\,[(Z - U).(Z - V) - 1/2\,(Z - U)^2]$

On obtient de la même manière, par substitutions :

$\gamma')$ $P'(Z) = P'(U) + P^{(2)}(U).(Z - U) + 1/2\, P^{(3)}(V).(Z - U)^2$
$+ c\,[(Z - U)^2.(Z - V)/2 - (Z - U)^3/3]$

$\delta')$ $P(Z) = P(V) + P'(U).(Z - V) + P^{(2)}(U)[(Z - U).(Z - V) - 1/2(Z - V)^2]$
$+ P^{(3)}(V).[\,(Z - U)^2.(Z - V)/2 - (Z - U).(Z - V)^2/2 + (Z - V)^3/6]$
$+ c\,[\,-(Z - U)^3.(Z - V)/3 + (Z - U)^2.(Z - V)^2/2 - (Z - U).(Z - V)^3/2 + (Z - V)^4/8]$

Les égalités $\alpha)$, $\beta')$, $\gamma')$, $\delta')$ donnent donc :

$^*([\, \mathbb{H}'(U)\ ,\ \mathbb{H}'(V),\ U < Z < V\,] \ \Rightarrow\ \mathbb{H}(Z))^*$

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 Hörmander, et nécessite la notion d'existence potentielle.

3) Existence potentielle

Notations et définitions

Une implication forte $^*(\mathbb{H} \Rightarrow \mathbb{H}')^*$ est une forme forte (par identité algébrique) pour l'implication *universelle* correspondante : $\forall \mathbf{X} (\mathbb{H} \Rightarrow \mathbb{H}')$.
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 :

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

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 $P(\mathbf{X}) = T^2$ prise isolément n'a pas le même statut que la non impossibilité de l'équation $P(\mathbf{X})^2 = T^4$. En effet, dans le second cas, contrairement au premier, quelles que soient les hypothèses faites par ailleurs sur $\mathbf{X}$, le fait de rajouter l'équation ne peut introduire une contradiction. Cette distinction est traduite en logique par une alternance de quantificateurs:

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

Une traduction "mot à mot" de cette alternance en termes d'implications fortes semblerait devoir être : pour toute spécification à la Thom non fortement incompatible des X_i, le système $\mathbb{H}(\mathbf{X},T)$ est lui-même non fortement incompatible. Mais, dans une preuve, les valeurs prises par les X_i peuvent dépendre de valeurs prises par des paramères Y_j. En outre, il nous faut donner une forme constructive à l'implication " A non fortement incompatible " implique " B non fortement incompatible ". Ceci nous conduit à considérer la contrapposée de cette implication, et à lire l'implication obtenue sous forme d'une construction. Nous obtenons en fin de compte la définition suivante.

Définition 11 :

Soient $\mathbb{H}_1$ un système de csg portant sur des polynômes de $\mathbf{K}[\mathbf{X}]$, $\mathbb{H}_2$ un système de csg portant sur des polynômes de $\mathbf{K}[\mathbf{X},T_1,T_2,...,T_m] = \mathbf{K}[\mathbf{X},\mathbf{T}]$.
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 $\mathbf{K}[\mathbf{X},\mathbf{Y}]$[1], on a la construction d'implication forte :

$$^*([\mathbb{H}_2(\mathbf{X},\mathbf{T}), \mathbb{H}(\mathbf{X},\mathbf{Y})] \Rightarrow 1 = 0)^* \;\; \vdash_{\text{cons}} \; ^*([\mathbb{H}_1(\mathbf{X}), \mathbb{H}(\mathbf{X},\mathbf{Y})] \Rightarrow 1 = 0)^*.$$

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

Notation : Nous noterons cette existence potentielle par : $^*(\mathbb{H}_1 \Rightarrow \exists \mathbf{T} \; \mathbb{H}_2)^*$.

Nous pouvons préciser de plus les variables sur lesquelles portent les systèmes de csg, nous écrivons alors : $^*(\mathbb{H}_1(\mathbf{X}) \Rightarrow \exists \mathbf{T} \; \mathbb{H}_2(\mathbf{X},\mathbf{T}))^*$.
Lorsque le système $\mathbb{H}_1$ est vide, nous utiliserons la notation $^*(\exists \mathbf{T} \; \mathbb{H}_2(\mathbf{X},\mathbf{T}))^*$.

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

$$^*(P(\mathbf{X},U).P(\mathbf{X},V) < 0 \Rightarrow \exists W \; P(\mathbf{X},W) = 0)^*$$

[1] 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 $\mathbf{K}[\mathbf{X},\mathbf{Y}]$.

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

$$^*(\mathbb{H}(\mathbf{X},P(\mathbf{X})) \Rightarrow \exists\ W\ \mathbb{H}(\mathbf{X},W))^*$$

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 $^*(\mathbb{H}_1(\mathbf{X}) \Rightarrow \exists\ \mathbf{T}\ \mathbb{H}_2(\mathbf{X},\mathbf{T}))^*$ 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 $\forall\ \mathbf{x}\ (\mathbb{H}_1(\mathbf{x}) \Rightarrow \exists\ \mathbf{t}\ \mathbb{H}_2(\mathbf{x},\mathbf{t}))$ lu dans la clôture ordonnée de **K**.

4) Si nous appliquons la définition en prenant $\mathbb{H}_1$, $\mathbb{H}$ à la place de $\mathbb{H}$, on obtient la construction d'implication forte :

$$^*([\ \mathbb{H}_2,\ \mathbb{H}_1\ ,\ \mathbb{H}\ ] \Rightarrow 1 = 0)^* \ \vdash_{\overline{\text{cons}}}\ ^*([\ \mathbb{H}_1,\ \mathbb{H}\ ] \Rightarrow 1 = 0)^*$$

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

$$^*([\ \mathbb{H}_2,\ \mathbb{H}_1\ ,\ \mathbb{H}\ ] \Rightarrow \mathbb{H}')^* \ \vdash_{\overline{\text{cons}}}\ ^*([\ \mathbb{H}_1,\ \mathbb{H}\ ] \Rightarrow \mathbb{H}')^*$$

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.
Nous dirons qu'un système de csg est *renforcé* lorsqu'on lui rajoute des csg, ou lorsqu'on remplace une csg par une condition de signe plus forte ($\geq$ par $>$ par exemple). Définition symétrique pour *affaiblir* un système de csg.

Lemme 12 : Une existence potentielle $^*(\mathbb{H}_1(\mathbf{X}) \Rightarrow \exists\ \mathbf{T}\ \mathbb{H}_2(\mathbf{X},\mathbf{T}))^*$ reste vraie si on affaiblit la conclusion, si on renforce l'hypothèse, ou si on supprime derrière $\exists$ des variables ne figurant pas dans $\mathbb{H}_2(\mathbf{X},\mathbf{T})$.

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

Si $^*(\mathbb{H}_1(\mathbf{X}) \Rightarrow \exists\ \mathbf{T}\ \mathbb{H}_2(\mathbf{X},\mathbf{T}))^*$ **alors**

$$^*([\ \mathbb{H}_1(\mathbf{X})\ ,\ \mathbb{H}_3(\mathbf{X})\ ] \Rightarrow \exists\ \mathbf{T}\ [\ \mathbb{H}_2(\mathbf{X},\mathbf{T}),\ \mathbb{H}_3(\mathbf{X})\ ])^*$$

(rappel de l'hypothèse dans la conclusion)

Si $^*(\mathbb{H}_1(\mathbf{X}) \Rightarrow \exists\ \mathbf{T}\ \mathbb{H}_2(\mathbf{X},\mathbf{T}))^*$ **alors** $^*(\mathbb{H}_1(\mathbf{X}) \Rightarrow \exists\ \mathbf{T}\ [\ \mathbb{H}_2(\mathbf{X},\mathbf{T}),\ \mathbb{H}_1(\mathbf{X})\ ])^*$

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 $\mathbb{H}_1$ et $\mathbb{H}_2$ portent sur les seules variables **X**.

Alors $^*(\mathbb{H}_1(\mathbf{X}) \Rightarrow \exists\ \mathbf{T}\ \mathbb{H}_2(\mathbf{X}))^*$ **si et seulement si** $^*(\mathbb{H}_1(\mathbf{X}) \Rightarrow \mathbb{H}_2(\mathbf{X}))^*$.

preuve> Voyons le seulement si: soit $Q\ \tau\ 0$ une csg dans $\mathbb{H}_2$ et soit $Q\ \tau'\ 0$ la csg opposée. On a $^*([\ \mathbb{H}_2(\mathbf{X}),\ Q\ \tau'\ 0\ ] \Rightarrow 1 = 0)^*$. Donc, par l'existence potentielle, on a également $^*([\ \mathbb{H}_1(\mathbf{X}),\ Q\ \tau'\ 0\ ] \Rightarrow 1 = 0)^*$, c.-à-d. $^*(\mathbb{H}_1(\mathbf{X}) \Rightarrow Q\ \tau\ 0)^*$.
Voyons l'implication dans l'autre sens. Soit $\mathbb{H}(\mathbf{X},\mathbf{Y})$ un système de csg et supposons que $^*([\ \mathbb{H}_2(\mathbf{X}),\ \mathbb{H}(\mathbf{X},\mathbf{Y})\ ] \Rightarrow 1 = 0)^*$. D'après l'hypothèse, on a évidemment :

$^*([\, \mathbb{H}_1(\mathbf{X}), \mathbb{H}(\mathbf{X},\mathbf{Y}) \,] \Rightarrow [\, \mathbb{H}_2(\mathbf{X}), \mathbb{H}(\mathbf{X},\mathbf{Y}) \,])^*$. Il suffit d'appliquer la transitivité des implications fortes pour obtenir $^*([\, \mathbb{H}_1(\mathbf{X}) , \mathbb{H}(\mathbf{X},\mathbf{Y}) \,] \Rightarrow 1 = 0)^*$. ❑

Proposition 15 : (raisonnement cas par cas)

Soit Q un polynôme de $\mathbf{K}[\mathbf{X}]$. Pour démontrer une existence potentielle $^*(\mathbb{H}_1(\mathbf{X}) \Rightarrow \exists\ \mathbf{T}\ \mathbb{H}_2(\mathbf{X},\mathbf{T}))^*$ il suffit de démontrer chacune des existences potentielles $^*([\, \mathbb{H}_1(\mathbf{X}),\ Q\ \sigma\ 0 \,] \Rightarrow \exists\ \mathbf{T}\ \mathbb{H}_2(\mathbf{X},\mathbf{T}))^*$ pour les 3 signes σ possibles.

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

Théorème 16 : (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

$^*(\mathbb{H}_1(\mathbf{X}) \Rightarrow \exists\ \mathbf{T}\ \mathbb{H}_2(\mathbf{X},\mathbf{T}))^*$ et $^*([\, \mathbb{H}_1(\mathbf{X}), \mathbb{H}_2(\mathbf{X},\mathbf{T}) \,] \Rightarrow \exists\ \mathbf{U}\ \mathbb{H}_3(\mathbf{X},\mathbf{T},\mathbf{U}))^*$

alors on a aussi :

$$^*(\mathbb{H}_1(\mathbf{X}) \Rightarrow \exists\ \mathbf{T}, \mathbf{U}\ [\, \mathbb{H}_1(\mathbf{X}),\ \mathbb{H}_2(\mathbf{X},\mathbf{T}),\ \mathbb{H}_3(\mathbf{X},\mathbf{T},\mathbf{U}) \,])^*$$

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.

Proposition 17 : (l'existence implique l'existence potentielle)

Soient $P_1,P_2,...,P_m \in \mathbf{K}[\mathbf{X}]$ et notons $\mathbf{P}(\mathbf{X})$ pour $P_1(\mathbf{X}), ..., P_m(\mathbf{X})$. On a l'existence potentielle : $^*(\mathbb{H}_2(\mathbf{X},\mathbf{P}(\mathbf{X})) \Rightarrow \exists\ \mathbf{T}\ \mathbb{H}_2(\mathbf{X},\mathbf{T}))^*$

Corollaire : (mêmes hypothèses)

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

preuve> Substituer les P_i aux T_i dans l'implication forte :

$$^*([\, \mathbb{H}_2(\mathbf{X},\mathbf{T}),\ \mathbb{H}(\mathbf{X},\mathbf{Y}) \,] \Rightarrow 1 = 0)^*$$

Le corollaire suit par transitivité des existences potentielles. ❑

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 $\mathbf{K}[\mathbf{Z}]$. Notons $\mathbf{P}(\mathbf{Z})$ pour $P_1(\mathbf{Z}), ..., P_n(\mathbf{Z})$.

Si on a $^*(\mathbb{H}_1(\mathbf{X}) \Rightarrow \exists\ \mathbf{T}\ \mathbb{H}_2(\mathbf{X},\mathbf{T}))^*$ (a)

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

preuve> Supposons qu'on ait

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

On veut construire

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

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

Par transitivité (1) et (3) donnent :

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

Par définition de l'existence potentielle on sait construire:

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

Par ailleurs :

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

Par transitivité (5) et (6) donnent :

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

En substituant **P**(**Z**) à **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 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:

$$^*\big(\ U \geq 0\ \Rightarrow\ \exists\ T\quad U = T^2\ \big)^*$$

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 $\mathcal{C}p'$, $\mathcal{I}'$ 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:

$$^*\big([\ \mathbb{H},\ U - T^2 = 0\ ]\ \Rightarrow\ 1 = 0\ \big)^* \quad \vdash_{\overline{\text{cons}}}\ ^*\big([\ \mathbb{H},\ U \geq 0\ ]\ \Rightarrow\ 1 = 0\ )\ \big)^*.$$

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

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 $Q_i(\mathbf{X}) \in \mathcal{C}p(F_\geq \cup F_>)$ 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 :

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

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

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 :

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

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:

$$^*\left(U \neq 0 \Rightarrow \exists\ T \quad 1 = U.T \right)^*$$

preuve> Mêmes notations qu'au théorème précédent. On veut expliciter la construction: $^*\left([\ \mathbb{H},\ 1 - U.T = 0\ ] \Rightarrow 1 = 0 \right)^* \ \vdash_{\overline{cons}}\ ^*\left([\ \mathbb{H},\ U \neq 0\ ] \Rightarrow 1 = 0 \right)^*$.
L'hypothèse correspond à une équation :

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

Informellement : 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.
Plus précisément : multiplions par une puissance U^{2m} convenable ($m \geq \deg_T(V_i)$ et $2m \geq \deg_T(W_j)$), puis remplaçons chaque $U^k.T^k$ dans un V_i ou W_j par 1 modulo $(1 - U.T)$. On obtient :

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

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:

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

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:

$$^*\left(U > 0 \Rightarrow \exists\ T \quad 1 = U.T^2 \right)^*$$

preuve> $^*\left(U \geq 0 \Rightarrow \exists\ Z \quad U = Z^2 \right)^*$ d'après le théorème 19 .
Par ailleurs $^*\left([\ U > 0,\ U = Z^2\ ] \Rightarrow Z \neq 0 \right)^*$ donc par transitivité :
$^*\left(U > 0 \Rightarrow \exists\ Z \quad [\ U = Z^2\ ,\ Z \neq 0\ ] \right)^*$
Par ailleurs $^*\left(Z \neq 0 \Rightarrow \exists\ T \quad 1 = Z.T \right)^*$ d'après le théorème 20, donc par transitivité : $^*\left(U > 0 \Rightarrow \exists\ Z, T \quad [\ U = Z^2\ ,\ Z \neq 0\ ,\ 1 = Z.T\ ] \right)^*$
Enfin $^*\left([\ U = Z^2\ ,\ 1 = Z.T\ ] \Rightarrow 1 = U.T^2 \right)^*$ donc par transitivité :
$^*\left(U > 0 \Rightarrow \exists\ Z, T \quad [\ U = Z^2\ ,\ Z \neq 0\ ,\ 1 = Z.T\ ,\ 1 = U.T^2\ ] \right)^*$
et a fortiori $^*\left(U > 0 \Rightarrow \exists\ T \quad 1 = U.T^2 \right)^*$ ❑

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

K. Alors, pour tout système de csg portant sur des polynômes de **K**[**X**], l'impossibilité dans **R** implique l'incompatibilité forte dans **K**.

preuve> Considérons un système de csg portant sur des polynômes de **K**[**X**]. Si on a une csg $P \geq 0$ 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:
$^*(U \geq 0 \Rightarrow \exists\ T\ \ U = T^2\ )^*$ permet de remplacer $P - T_P^2 = 0$ par $P \geq 0$ (théorème 19)
$^*(U > 0 \Rightarrow \exists\ T\ \ 1 = U.T^2\ )^*$ permet de remplacer $1 - Q.T_Q^2 = 0$ par $Q > 0$ (corollaire 1)
$^*(U \neq 0 \Rightarrow \exists\ T\ \ 1 = U.T\ )^*$ permet de remplacer $1 - R.T_R = 0$ par $R \neq 0$ (théorème 20) ❑

Remarques 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. Par ailleurs le corollaire 1 peut être prouvé directement (même méthode que les théorèmes 19 et 20). Il s'ensuit que le corollaire 2 peut être prouvé directement, sans théorie générale de l'existence potentielle, comme dans le cas de la théorie des corps algébriquement clos.

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, en notant P(U) pour P(**X**,U) : $^*(\ P(U).P(V) \leq 0 \Rightarrow \exists\ Z\ \ P(Z) = 0)^*$

preuve> Nous faisons une preuve par récurrence[1] sur le degré s 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 Z, d'expliciter la construction:

$$^*(\ [\ \mathbb{H}, P(\mathbf{X},Z) = 0\ ] \Rightarrow 1 = 0\ )^* \ \ |\!\!\sim_{cons}\ ^*(\ [\ \mathbb{H}, P(\mathbf{X},U).P(\mathbf{X},V) \leq 0\ ] \Rightarrow 1 = 0\ )\ )^*$$

qui peut se relire :

$$^*(\ \mathbb{H} \Rightarrow P(\mathbf{X},Z) \neq 0\ )^* \ \ |\!\!\sim_{cons}\ ^*(\ \mathbb{H} \Rightarrow P(\mathbf{X},U).P(\mathbf{X},V) > 0\ )^*$$

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

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

avec $Q_i(\mathbf{X}) \in Cp(F_{\geq} \cup F_{>})$ et $N_j(\mathbf{X}) \in F_{=}$. Les polynômes $B_i(\mathbf{X},Z)$ et $C_j(\mathbf{X},Z)$ peuvent être pris modulo P en Z (parce que P est unitaire), auquel cas : $deg_Z(G) \leq deg_Z(P) - 2$.
La même égalité se relit de plusieurs manières:

$$^*(\ \mathbb{H} \Rightarrow G(\mathbf{X},Z) \neq 0\ )^*\ (1),\quad ^*(\ \mathbb{H} \Rightarrow P(\mathbf{X},Z).G(\mathbf{X},Z) > 0\ )^*\ (2).$$

On déduit par substitution:

---

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 .

$$^*(\mathbb{H} \Rightarrow P(\mathbf{X},U).G(\mathbf{X},U) > 0)^* \quad , \quad ^*(\mathbb{H} \Rightarrow P(\mathbf{X},V).G(\mathbf{X},V) > 0)^*$$

D'où : $$^*(\mathbb{H} \Rightarrow P(\mathbf{X},U).G(\mathbf{X},U).P(\mathbf{X},V).G(\mathbf{X},V) > 0)^*$$

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

Enfin, on a trivialement:

$$^*([P(\mathbf{X},U).G(\mathbf{X},U).P(\mathbf{X},V).G(\mathbf{X},V) > 0,\ G(\mathbf{X},U).G(\mathbf{X},V) > 0] \Rightarrow P(\mathbf{X},U).P(\mathbf{X},V) > 0)^*$$

On conclut par transitivité des implications fortes.

Voyons maintenant le cas où P n'est pas unitaire.

Soit $C(\mathbf{X})$ son coefficient dominant en Z.

Soit $R(\mathbf{X},Z) = P(\mathbf{X},Z) - C(\mathbf{X}).Z^s$. (donc $\deg_Z(R) < s = \deg_Z(P)$).

Démontrons l'existence potentielle en raisonnant cas par cas, selon le signe de C(X).

1er cas : $C(\mathbf{X}) = 0$

On a : $$^*(C(\mathbf{X}) = 0 \Rightarrow R(\mathbf{X},Z) = P(\mathbf{X},Z))^*$$

et donc : $$^*([\ P(\mathbf{X},U).P(\mathbf{X},V) \le 0\ ,\ C(\mathbf{X}) = 0\ ] \Rightarrow R(\mathbf{X},U).R(\mathbf{X},V) \le 0)^*$$

et par hypothèse de récurrence, on a:

$$^*(R(\mathbf{X},U).R(\mathbf{X},V) \le 0 \Rightarrow \exists\, Z\ \ R(\mathbf{X},Z) = 0)^*$$

et comme : $$^*([\ R(\mathbf{X},Z) = 0,\ C(\mathbf{X}) = 0\ ] \Rightarrow P(\mathbf{X},Z) = 0)^*$$

on conclut par transitivité.

2ème cas : $C(\mathbf{X}) \neq 0$.

On considère une nouvelle variable T. Soit $P_1(\mathbf{X},T,Z) = T.R(\mathbf{X},Z) + Z^s$.

On a : $^*(C(\mathbf{X}) \neq 0 \Rightarrow \exists\, T\ \ 1 = C(\mathbf{X}).T)^*$, $^*(1 = C(\mathbf{X}).T \Rightarrow T.P(\mathbf{X},Z) = P_1(\mathbf{X},T,Z))^*$ et

$$^*(1 = C(\mathbf{X}).T \Rightarrow P(\mathbf{X},Z) = C(\mathbf{X}).P_1(\mathbf{X},T,Z))^*$$

et donc:

$$^*([\ P(\mathbf{X},U).P(\mathbf{X},V) \le 0\ ,\ C(\mathbf{X}) \neq 0\ ] \Rightarrow \exists\, T\ [\ 1 = C(\mathbf{X}).T\ ,\ P_1(\mathbf{X},T,U).P_1(\mathbf{X},T,V) \le 0])^*$$

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

$$^*(P_1(\mathbf{X},T,U).P_1(\mathbf{X},T,V) \le 0 \Rightarrow \exists\, Z\ \ P_1(\mathbf{X},T,Z) = 0)^*$$

Par transitivité :

$$^*([\ P(\mathbf{X},U).P(\mathbf{X},V) \le 0\ ,\ C(\mathbf{X}) \neq 0\ ] \Rightarrow \exists\, T,Z\ [\ 1 = C(\mathbf{X}).T\ ,\ P_1(\mathbf{X},T,Z) = 0\ ])^*$$

Donc : $$^*([\ P(\mathbf{X},U).P(\mathbf{X},V) \le 0\ ,\ C(\mathbf{X}) \neq 0\ ] \Rightarrow \exists\, T,Z\ \ P(\mathbf{X},Z) = 0)^*,$$

où on peut supprimer T. ❑

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, en notant P(U) pour $P(\mathbf{X},U)$:

$$^*([\ P(U).P(V) < 0\ ] \Rightarrow \exists\ Z\ [\ P(Z) = 0,\ P(U).P(V) < 0\ ,\ (Z - U).(Z - V) < 0\ ])^*$$

ou encore :

$$^*([\ P(U).P(V) < 0,\ U < V\ ] \Rightarrow \exists\ Z\ [\ P(Z) = 0,\ P(U).P(V) < 0\ ,\ U < Z < V\ ])^*$$

preuve> La deuxième forme résulte de la première : on a en effet facilement

$$^*([\ U < V,\ (Z - U).(Z - V) < 0\ ] \Rightarrow U < Z < V)^*.$$

Nous allons mimer le raisonnement classique qui dit : si z est hors de l'intervalle d'extrémités u et v, alors on considère le polynôme obtenu en divisant P(Z) par (Z – z), 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 s en Z de P(Z).

Si ce degré est 0, le théorème est trivial. Passons de s à s+1. Supposons le degré s+1.

D'après le théorème 21 et la proposition 13, on a déjà:

$$^{*}\big(\, P(U).P(V) < 0 \;\Rightarrow\; \exists\ Z\ [P(Z) = 0,\ P(U).P(V) < 0]\,\big)^{*}$$

Nous allons démontrer l'existence potentielle:

$$^{*}\big([P(U).P(V) < 0,\ P(Z) = 0] \Rightarrow \exists\ Z'\ [P(Z') = 0,\ P(U).P(V) < 0,\ (Z' - U).(Z' - V) < 0]\big)^{*}$$

cas par cas, selon le signe de $(Z - U).(Z - V)$.

Si $(Z - U).(Z - V) < 0$.

Tout va bien : l'existence (vérifiée par Z) implique l'existence potentielle (pour la nouvelle variable Z') .

Si $(Z - U).(Z - V) \geq 0$.

On considère une nouvelle variable T et le polynôme R défini par :

$$R(\mathbf{X},Z,T) := \big(\, P(\mathbf{X},T) - P(\mathbf{X},Z)\big) \,/\, (T - Z)\ .$$

Notons pour alléger R(T) pour $R(\mathbf{X},Z,T)$ et P(T) pour $P(\mathbf{X},T)$.

Notons $\mathbb{H}_1(\mathbf{X},Z)$ pour $[\ P(U).P(V) < 0\ ,\ P(Z) = 0,\ (Z - U).(Z - V) \geq 0\ ]$.

(c'est l'hypothèse de l'existence potentielle que nous voulons démontrer)

On a facilement l'implication forte:

$$^{*}\big(\, \mathbb{H}_1(\mathbf{X},Z) \;\Rightarrow\; P(T) = R(T).(T - Z)\,\big)^{*},\quad \text{et donc aussi :}$$

$$^{*}\big(\, \mathbb{H}_1(\mathbf{X},Z) \;\Rightarrow\; [\ R(U).(Z - U).R(V).(Z - V) = P(U).P(V) < 0,\ (Z - U).(Z - V) \geq 0\ ]\,\big)^{*}$$

et donc aussi

$$^{*}\big(\, \mathbb{H}_1(\mathbf{X},Z) \;\Rightarrow\; R(U).R(V) < 0\,\big)^{*}$$

Comme R(T) est de degré $\leq s$ en T on applique l'hypothèse de récurrence. On obtient :

$$^{*}\big(\, R(U).R(V) < 0 \;\Rightarrow\; \exists\ Z'\ [R(Z') = 0,\ R(U).R(V) < 0,\ (Z' - U).(Z' - V) < 0]\,\big)^{*}$$

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

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 Hörmander

Nullstellensatz réel en une variable

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

Proposition 23 : (Tableau et algorithme de Hörmander)

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 P la famille de polynômes engendrée par les éléments de L et par les opérations $P \to P'$, et $(P,Q) \to$ **Rst**(P,Q). Alors :

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

preuve> 1) A priori, pour construire P on prend la liste L et on applique systématiquement l'opération "reste de tous les couples de polynômes précédemment obtenus" ainsi que l'opération "dérivation de tous polynômes précédemment 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 P_m la sous-famille de P constituée des polynômes numérotés de 1 à m. Elle est évidemment stable par les opérations 'dérivation' et 'reste de division', qui abaissent le degré. Notons enfin T_m le tableau de Hörmander correspondant.

Montrons, par récurrence sur le numéro m du polynôme, qu'on peut établir le tableau complet des signes des polynômes de la famille P_m, en utilisant les seules informations autorisées. Tant que les polynômes sont de degré 0, c'est clair.

Supposons vrai jusqu'à m. Soit P le polynôme de numéro $m + 1$ dans P. Sur chacun des intervalles du tableau T_m, le polynôme P est strictement monotone, d'après le théorème des accroissements finis. Chacun des points ξ du tableau T_m est ou bien $+\infty$, ou bien $-\infty$, ou bien une racine d'un certain polynôme Q de numéro $\leq m$, et dans ce cas, si R = **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 T_m le polynôme P reste de signe constant, en quels points déjà introduits s'annule P et sur quels intervalles ouverts de T_m sont les racines de P dans **R** qui ne figuraient pas encore dans T_m. Soit ζ une racine de P sur l'un de ces intervalles ouverts $I =]\xi,\xi'[$. Si Q est un polynôme de numéro $\leq m$ dans P, son

---

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

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 P_{m+1} à partir des informations autorisées et du tableau complet des signes pour P_m. ❑

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'(ξ), P"(ξ), 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 Hörmander 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 P une famille de polynômes de **K**[X] et $\mathbb{H}(X)$ un système de csg portant sur des éléments de P. Alors :

ou bien $\mathbb{H}(x)$ est impossible dans **R** et alors $^*(\mathbb{H}(X) \Rightarrow 1 = 0)^*$ 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 $^*(\exists X \ \mathbb{H}(X))^*$ dans **K** et dans toute extension ordonnée de **K**.

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

Nous commençons par considérer le cas où le corps **K** est réel clos, qui est beaucoup plus simple à traiter.

---

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

Lorsque le corps K est réel clos

preuve du théorème dans ce cas > On a donc **R** = **K**. Soient $\upsilon_1, \upsilon_2, ..., \upsilon_k$ la liste ordonnée des points finis du tableau de Hörmander de la famille P. On peut calculer υ_0 et υ_{k+1} dans **R** tels que l'évidence forte des signes de tous les $P \in P$ soit facile à établir en $x \leq \upsilon_0$ et en $x \geq \upsilon_{k+1}$.
La possibilité dans **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 **R** pour une système $\mathbb{H}$ de csg est également lisible sur le tableau de Hörmander, 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 **R** (puisque $\upsilon_i \in$ **R**). Sur un intervalle $]\upsilon_i, \upsilon_{i+1}[$, les signes, constants et non nuls, des $P \in P$ sont tous fortement évidents à partir des signes aux bords modulo une formule de Taylor mixte convenable (cf. théorème 10 (5)).

Dans le corps des coefficients

Nous voulons établir, pour tous les faits lisibles sur le tableau de Hörmander, incompatibilité forte et existence potentielle dans **K**.
Il nous faut cette fois-ci suivre l'algorithme de Hörmander pas à pas, c.-à-d. en introduisant les points du tableau de Hörmander un à un.
Nous commençons par calculer a et b dans **K**, au delà desquels les signes des polynômes de P sont fortement évidents. Ces 2 éléments de **K** remplaceront pour nous $-\infty$ et $+\infty$ dans le tableau de Hörmander.

Lemme 26 : (évidence forte et existence potentielle pour les faits élémentaires lisibles sur un tableau de Hörmander)
Soit **K** un corps ordonné et **R** sa clôture réelle. Soit P une famille de polynômes de **K**[X] stable par les opérations "reste" et "dérivation", soit T son tableau de Hörmander.

1) les points du tableau de Hörmander, définis à la Thom par leur construction même, vérifient l'existence potentielle pour leur codage à la Thom [(1)].
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.

---

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.

preuve du lemme> Nous démontrons le lemme pour la famille P_m et le tableau T_m, par récurrence sur m. En suivant pas à pas la preuve de la proposition 23. Le lemme est évident lorsque la famille P_m ne contient que des constantes.
Passons de m à m+1. Si λ est un point de T_m, 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 **R** vérifiant $\mathbb{H}_\lambda(\lambda)$. Soit alors P le polynôme numéroté m+1, non constant, de degré p.
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 $+\infty$.
Pour chaque point λ de T, nous introduisons une nouvelle variable X_λ. Pour rendre la preuve plus lisible, nous écrivons λ à la place de X_λ. Les instances de λ valant pour X_λ sont claires d'après le contexte.

Voyons le point 1) Seuls les points introduits à l'étape m+1, c.-à-d. les racines de P non racines d'un polynôme de numéro $\leq$ m, posent a priori problème. Il est clair que le signe de P en un point λ de T_m est fortement évident à partir du signe de **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 T_m. On a donc :

$$^*(\mathbb{H}_\alpha(\alpha) \Rightarrow P(\alpha) > 0)^* \text{ et } ^*(\mathbb{H}_\beta(\beta) \Rightarrow P(\beta) < 0)^* \text{ ou vice-versa.}$$

Et l'hypothèse de récurrence (2) donne :

$$^*([\mathbb{H}_\alpha(\alpha) , \mathbb{H}_\beta(\beta)] \Rightarrow \alpha < \beta)^*$$

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

$$^*([\mathbb{H}_\alpha(\alpha) , \mathbb{H}_\beta(\beta)] \Rightarrow \exists Z [\alpha < Z < \beta, P(Z) = 0])^*$$

Par ailleurs, par hypothèse de récurrence (4), il y a des $\tau_i \in \{ <, > \}$ (i = 1, ..., p) tels que l'on ait :

$$^*([\mathbb{H}_\alpha(\alpha) , \mathbb{H}_\beta(\beta) , \alpha < Z < \beta] \Rightarrow [P^{(i)}(Z) \ \tau_i \ 0 \quad (i = 1, ..., p)])^*$$

Et comme on a déjà :

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

On en déduit par transitivité:

$$^*(\exists Z [P(Z) = 0, P^{(i)}(Z) \ \tau_i \ 0 \quad (i = 1, ..., p)])^*$$

que nous réécrivons pour plus de lisibilité:

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

Voyons le point 2) Appelons τ'_i le signe $\leq$ ou $\geq$ associé à τ_i.
On a les implications fortes:

$$^*(\mathbb{H}_\alpha(\alpha) \Rightarrow P(\alpha) > 0)^* \text{ (si } \tau_1 \text{ est } < \text{, } P(\alpha) < 0 \text{ si } \tau_1 \text{ est } >)$$

$$^*(\mathbb{H}_\alpha(\alpha) \Rightarrow P^{(i)}(\alpha) \ \tau'_i \ 0)^* \text{ (i = 1, ..., p – 1), et } ^*(\mathbb{H}_\alpha(\alpha) \Rightarrow P^{(p)}(\alpha) \ \tau_p \ 0)^*$$

Donc via le théorème 10 (2,b) :

$$^*([\mathbb{H}_\alpha(\alpha) , \mathbb{H}_\zeta(\zeta)] \Rightarrow \alpha < \zeta)^* \quad \text{(idem pour } \beta > \zeta)$$

Le point 2) pour T_{m+1} se déduit alors du point 2) pour T_m : si par exemple $\lambda \in T_m$ avec $\lambda < \alpha$ on a par hypothèse de récurrence :

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

Donc :

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

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

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

Voyons le point 3) On a déjà vu que le signe de P en tout point λ de T_m est fortement évident à partir du codage à la Thom de λ. Il reste à voir que le signe de $Q \in P_m$ 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 :

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

Par ailleurs, vue l'hypothèse de récurrence (3), les signes de Q et de ses dérivées en α et β sont fortement évidents à partir de $\mathbb{H}_\alpha(\alpha)$ et $\mathbb{H}_\beta(\beta)$. Ils sont en outre compatibles (c.-à-d. que les signes en α et β d'un même polynôme ne sont ni " $= 0$ et $= 0$ ", ni " > 0 et < 0 " ni " < 0 et > 0 ")[1]. Donc, en appliquant de nouveau le théorème 10 (5) et la transitivité, on obtient :

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

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

on obtient le résultat voulu :

$$^*(\mathbb{H}_\zeta(\zeta)\,] \Rightarrow Q(\zeta)\ \tau\ 0)^* \text{ avec } \tau \in \{ <, > \}$$ [2]

Voyons le point 4) Notons $\mathbb{H}_{\lambda,\mu}(X)$ le codage à la Thom d'un intervalle ouvert minimal de T_{m+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 (2) on obtient:

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

Si maintenant Q est un polynôme arbitraire de P_{m+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 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... ❑

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 Hörmander, ont été établis sans supposer l'existence d'une clôture réelle de **K**. Pour ce qui concerne l'algorithme de Hörmander 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 Hörmander "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.

---

[1] Ceci est clair d'après l'existence de la clôture réelle, mais résulte également de la construction itérative des implications fortes et existences potentielles donnée dans ce lemme : cette remarque nous permet par la suite d'utiliser la preuve de la proposition 25 comme nouveau moyen d'établir constructivement l'existence de la clôture réelle d'un corps ordonné ; elle nous permet également de relire le lemme 26 lorsque les coefficients des polynômes dépendent de paramètres, dans la preuve du théorème 28.

[2] 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 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 **K** .

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 :

$$^*(\mathbb{H} \Rightarrow Q(X) \equiv \sigma)^*$$

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 Hörmander 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) Nulltellensatz réel effectif et variantes

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.

Nous commençons par rappeler le théorème concernant les tableaux de Hörmander paramétrés. (cf. [**BCR**] chap. 1).

Proposition 27 : (Tableau de Hörmander 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 $\mathbf{K}[X_1, X_2,..., X_n][Y]$.

On peut construire une famille finie F de polynômes de $\mathbf{K}[X_1, X_2,..., X_n]$ telle que, pour tous $x_1, x_2,..., x_n$ dans **R**, en posant $P_i(Y) = Q_i(x_1, x_2,..., x_n;Y)$, le tableau complet des signes pour $L = [P_1, P_2, ..., P_k]$ est calculable à partir des signes des $S(x_1, x_2,..., x_n)$ pour $S \in F$.

preuve> On remarque que les constantes de *l'algorithme de Hörmander* (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 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 $x_1, x_2,..., x_n$ donnée de $X_1, X_2,..., X_n$, dépend de l'annulation de certains polynômes en les coefficients des polynômes de la liste initiale L. On met donc dans la famille F tous les polynômes apparaissant au numérateur ou dénominateur d'un coefficient d'un polynôme de la famille P, pour toutes les familles P possibles. ❑

Nous sommes maintenant en mesure de démontrer le :

Théorème 28 : (Tableau de Hörmander 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 $\mathbf{K}[X_1,X_2,...,X_n][Y]$.
On construit la famille finie F de polynômes de $\mathbf{K}[X_1,X_2,...,X_n]$ comme à la proposition 27.
Soit $\mathbb{H}(X_1,X_2,...,X_n,Y)$ un système de csg portant sur des polynômes de la liste L. Soit un élément $\Sigma = (\sigma_S)_{S \in F}$ de $\{-1, 0, +1\}^F$. On note $\mathbb{H}_\Sigma(X_1,X_2,...,X_n)$ le système de conditions de signes $[\, S(X_1,X_2,...,X_n) \equiv \sigma_S \,;\, S \in F\,]$. On suppose qu'il existe $x_1,x_2,...,x_n \in \mathbf{R}$ vérifiant $\mathbb{H}_\Sigma(x_1,x_2,...,x_n)$. Alors :
ou bien $\forall\, x_1,x_2,...,x_n \in \mathbf{R}\ \big(\, \mathbb{H}_\Sigma(x_1,x_2,...,x_n) \Rightarrow \exists\, y \in \mathbf{R}\ \mathbb{H}(x_1,x_2,...,x_n,y)\big)$
et alors : ${}^*\big(\, \mathbb{H}_\Sigma(X_1,X_2,...,X_n) \Rightarrow \exists\ Y\ \mathbb{H}(X_1,X_2,...,X_n,Y)\,\big)^*$ (lu dans **K**)
ou bien $\forall\, x_1,x_2,...,x_n,y \in \mathbf{R}\ \big(\ \mathbb{H}_\Sigma(x_1,x_2,...,x_n)$ et $\mathbb{H}(x_1,x_2,...,x_n,y)\,\big) \Rightarrow 1 = 0$ et alors :
${}^*\big(\, [\, \mathbb{H}_\Sigma(X_1,X_2,...,X_n)\, ,\, \mathbb{H}(X_1,X_2,...,X_n,Y)\,] \ \Rightarrow\ 1 = 0\,\big)^*$ (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 Hörmander de la famille. Pour ne pas avoir à utiliser des fractions rationnelles en $X_1,X_2,...,X_n$ 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 $\mathbf{K}[X_1,X_2,...,X_n]$, 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. ❑

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[2])
Soit **K** un corps ordonné, sous-corps d'un corps réel clos **R**.
Soit $\mathbb{H}(X_1,X_2,...,X_n)$ un système de csg portant sur une famille finie de polynômes de $\mathbf{K}[X_1,X_2,...,X_n]$. Ce système est impossible dans **R** si et seulement si il est fortement incompatible dans **K**. En termes plus formalisés :
Si $\forall\, x_1,x_2,...,x_n \in \mathbf{R}$ $\mathbb{H}(x_1,x_2,...,x_n)$ est absurde,
alors : ${}^*\big(\, \mathbb{H}(X_1,X_2,...,X_n) \ \Rightarrow\ 1 = 0\,\big)^*$ (dans **K**).

---

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.

2 "effectifs" parce que toutes nos preuves sont constructives et réfèrent à des algorithmes

Si $^*(\mathbb{H}(X_1,X_2,...,X_n) \Rightarrow 1 = 0)^*$ (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 Y la $n+1^{ème}$ 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 F. Soit donc Σ un élément arbitraire de $\{-1, 0, +1\}^F$.

Nous voulons construire l'implication forte:

$$^*([\mathbb{H}_\Sigma(X_1,X_2,...,X_n) , \mathbb{H}(X_1,X_2,...,X_n,Y)] \Rightarrow 1 = 0)^*.$$

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

$$^*(\mathbb{H}_\Sigma \Rightarrow 1 = 0)^* \quad \text{et a fortiori} \quad ^*([\mathbb{H}_\Sigma , \mathbb{H}] \Rightarrow 1 = 0)^*.$$

Sinon, on applique le théorème 28, c'est forcément la deuxième alternative qui se présente puisque $\mathbb{H}(x_1,x_2,...,x_n,y)$ 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 $\mathbb{H}(X_1,X_2,...,X_n)$ un système de csg portant sur une famille finie de polynômes de $\mathbf{K}[X_1,X_2,...,X_n]$. 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 $^*(\mathbb{H} \Rightarrow 1 = 0)^*$ (lue 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 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:

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

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

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

Théorème 32 :

Soit **K** un corps réel discret et $T_2(\mathbf{K})$ la théorie formelle intuitionniste des corps réels clos discrets, avec les éléments **K** pour constantes et les axiomes explicitant la structure de corps de **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 **K**. Si $c_1, c_2,..., c_n$ sont les éléments de **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 $P_i(X_1, X_2,..., X_n) \in \mathbb{Q}[X_1, X_2,..., X_n]$ $i = 1, 2, ..., k$ (un axiome traduisant la structure de **K** du type $c \neq 0$ peut être remplacé par $c.c' = 1$ où c' est l'inverse de c dans **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:

$(P_1(X_1, X_2,..., X_n) = 0$ et ... 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 $\mathbb{Q}[X_1, X_2,..., X_n]$. En remplaçant les X_i par les c_i dans cette identité algébrique, on obtient que le corps **K** n'est pas réel. ❑

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 ordonné, donc contenu dans un corps réel clos.

Remarque 12 : Les mêmes méthodes, simplifiées, s'appliqueraient en théorie des corps (avec les seules conditions de signe $= 0$ et $\neq 0$). On obtiendrait ainsi les analogues des théorèmes 30 et 32, c.-à-d. plus précisément :

Primo, le théorème des zéros de Hilbert explicité par un algorithme uniformément primitif récursif, avec une preuve directe et entièrement constructive (pour le cas des corps discrets[2]), sans avoir à développer la théorie constructive de la noethériannité.

Secundo, une preuve constructive que la théorie intuitionniste des corps algébriquement clos discrets, avec constantes dans un corps discret donné, est complète et non contradictoire.

---

[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 **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, $\exists x$ x ou -x est un carré, tout polynôme de degré impair admet une racine. Le tiers exclu restreint est alors formulé: $\exists x$ $x=0$ ou $x>0$. Si on adopte ce point de vue, la théorie formelle $T_1(\mathbf{K})$ contient, pour chaque élément positif a de **K** l'axiome $\exists x$ $x^2 = a$.

[2] Constructivement, un ensemble est dit discret lorsqu'on dispose d'un test effectif pour l'égalité de deux éléments.

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.

[Kri] Krivine, J. L. :Anneaux préordonnés. Journal d'analyse mathématique, t.12, 1964, p. 307-326

[Loma] Lombardi H. :Théorème effectif des zéros réel et variantes. Publications Mathématiques de l'Université (Besançon). 88-89. Fascicule 1.

[Lomb] Lombardi H. :Effective real nullstellensatz and variants, à paraître dans les compte rendus de MEGA 90, chez Birkhaüser. (Version anglaise plus courte)

[Lomc] Lombardi H. : Nullstellensatz réel effectif et variantes.
C.R.A.S. Paris, t. 310, Série I, p 635-640, 1990.

[LR] Lombardi H., Roy M.-F. :Théorie constructive élémentaire des corps ordonnés. 1989. A paraître aux Publications Mathématiques de Besançon.
Version anglaise moins détaillée «Constructive elementary theory of ordered fields» à paraître dans les comptes rendus de MEGA 90, chez Birkhauser.

[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 principe du calcul de majoration primitif récursif

Nous expliquons dans cette annexe comment peut être mené un calcul de majorations primitives récursives pour le théorème des zéros réels. En d'autres termes nous donnons une preuve un peu plus détaillée du théorème 30.

Position du problème:

Les données sont trois entiers d, n, k qui majorent, dans une incompatibilité $\mathbb{H} \Rightarrow 1 = 0$, respectivement les degrés des polynômes, le nombre des variables et le nombre de csg.
Le calcul doit aboutir à 3 fonctions primitives récursives explicites $\delta(d,n,k)$, $\sigma(d,n,k)$ et $\psi(d,n,k)$ qui donnent des majorants pour, dans une implication forte $^{*}(\mathbb{H} \Rightarrow 1 = 0)^{*}$,

respectivement le degré maximum, le nombre de termes dans la somme, et le nombre d'opérations arithmétiques dans **K** nécessaires pour calculer les coefficients dans l'implication forte à partir des coefficients donnés au départ.

Démarche générale:

En fait chacune des affirmations de chacun des théorèmes ou propositions de l'article précédent peut être accompagnée d'une majoration primitive récursive du même type que celle souhaitée pour le théorème 29, et affirmée dans le théorème 30.
Ces majorations s'enchainent les unes les autres, sans difficulté majeure. Il nous a néanmoins semblé utile d'expliquer plus en détail les mécanismes de ce calcul, notamment en ce qui concerne les existences potentielles, les tableaux de Hörmander, et la récurrence sur le nombre de variables.
En fait le calcul de majoration s'appuie beaucoup plus sur la notion d'existence potentielle que sur celle d'implication forte. Ceci traduit à notre avis le caractère crucial de la notion d'existence potentielle dans une compréhension du véritable mécanisme de cet algorithme.
Comme le calcul est très fastidieux, nous nous en tenons aux majorations de degrés, laissant au lecteur courageux les deux autres majorations.
On notera que l'usage de l'algorithme de Hörmander 'sans raccourci', à la base de notre méthode, rend a priori les majorations obtenues sans intérêt pratique.

Les calculs fastidieux:

Nous reprenons donc les énoncés de l'article, un à un, (si du moins ils sont utilisés dans la preuve du résultat final), et indiquons l'enchaînement des majorations.
Nous manipulons des incompatibilités fortes écrites *sous forme normale*, (c.-à-d. la forme (2), avec exposants pairs), c.-à-d. :

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

Le degré considéré, sauf précision contraire, est le degré total maximum.
Lorsqu'il s'agit d'une implication forte, nous l'appelons *le degré de l'implication forte*, et il est au moins égal à 1.
Par exemple, si nous avons une implication forte :

$$^{*}([\ A > 0, B > 0, C \geq 0, D \geq 0, E = 0, F = 0\ ] \Rightarrow\ 1 = 0)^{*}$$

explicitée sous forme d'une identité algébrique :

$$A^2.B^6 + C.\sum_{i=1}^{h} p_i.P_i^{\,2} + A.B.D.\sum_{j=1}^{k} q_j.Q_j^{\,2} + E.U + F.V = 0$$

le degré de l'implication forte est :

$$\sup(\ d(A^2.B^6)\ ,\ d(C.P_i^{\,2})\ (i = 1,...,h)\ ,\ d(A.B.D.Q_j^{\,2})\ (j = 1,...,k)\ ,\ d(E.U)\ ,\ d(F.V)\ ).$$

Notons enfin que nous utilisons la forme normale (à exposants pairs) des implications fortes pour faciliter le calcul de majoration, mais un peu de réflexion montre que si on veut pratiquer l'algorithme, on manipulera des objets moins gros si on n'impose pas cette condition.
Quand nous ne mettons aucun commentaire, les calculs sont faciles.

Incompatibilités, évidences et implications fortes

Proposition et majorations 2 : On a les implications fortes qui suivent.

$$^{*}([\ U > 0, V > 0\ ] \quad \Rightarrow \quad [\ U+V > 0, U.V > 0\ ])^{*}$$

$$^{*}([\ U+V \geq 0, U.V > 0\ ] \quad \Rightarrow \quad [\ U > 0, V > 0\ ])^{*} \quad \text{etc...} \ \text{(cf. p. 5)}$$

Dans chacune de ces implications fortes (17 en tout), le degré est majoré par 4, sauf dans l'implication forte :

$$^*(\ U = V \quad \Rightarrow \quad P(\mathbf{X},U) = P(\mathbf{X},V)\ )^*$$

où le degré est majoré par 2.deg(P).

Proposition et majorations 3 : (principe de substitution) .

Si, dans une implication forte $\mathfrak{I}$: $^*(\ \mathbb{H} \Rightarrow 1 = 0\ )^*$, on remplace toute occurrence d'une variable par un polynôme P fixé, on obtient encore une implication forte.

Le degré de la nouvelle implication forte est majoré par le produit deg($\mathfrak{I}$).sup(1,deg(P)).

Plus généralement, si le degré de l'implication forte initiale est d_1 et si on remplace simultanément plusieurs variables par différents polynômes de degrés majorés par d_2, alors le degré de l'implication forte construite est majoré par :

$$\delta_3(d_1,d_2) = d_1.\sup(1,d_2)$$

Lemme et majorations 5 : Soit $\mathbb{H}$ un système de csg portant sur des polynômes de $\mathbf{K}[\mathbf{X}]$, Q un élément de $\mathbf{K}[\mathbf{X}]$.

Alors toute implication forte du type $^*(\ \mathbb{H} \Rightarrow Q\ \tau\ 0\ )^*$ (où τ est $=$, $<$ ou $>$) fournit par relecture toute implication forte "plus faible" $^*(\ \mathbb{H} \Rightarrow Q\ \tau'\ 0\ )^*$. Par exemple, on a :

$$^*(\ \mathbb{H} \Rightarrow Q > 0\ )^* \ \vdash_{cons}\ ^*(\ \mathbb{H} \Rightarrow Q \geq 0\ )^*.$$

Le degré de la nouvelle implication forte est inchangé.

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

$$[\ ^*(\ \mathbb{H} \Rightarrow Q \leq 0\ )^* \text{ et } ^*(\ \mathbb{H} \Rightarrow Q \geq 0\ )^*\ ] \ \vdash_{cons}\ ^*(\ \mathbb{H} \Rightarrow Q = 0\ )^* \quad (a)$$

$$[\ ^*(\ \mathbb{H} \Rightarrow Q < 0\ )^* \text{ et } ^*(\ \mathbb{H} \Rightarrow Q > 0\ )^*\ ] \ \vdash_{cons}\ ^*(\ \mathbb{H} \Rightarrow 1 = 0\ )^* \quad (a')$$

De même :

$$[\ ^*(\ \mathbb{H} \Rightarrow Q \leq 0\ )^* \text{ et } ^*(\ \mathbb{H} \Rightarrow Q \neq 0\ )^*\ ] \ \vdash_{cons}\ ^*(\ \mathbb{H} \Rightarrow Q < 0\ )^* \quad (b)$$

$$[\ ^*(\ \mathbb{H} \Rightarrow Q = 0\ )^* \text{ et } ^*(\ \mathbb{H} \Rightarrow Q \neq 0\ )^*\ ] \ \vdash_{cons}\ ^*(\ \mathbb{H} \Rightarrow 1 = 0\ )^* \quad (c)$$

$$[\ ^*(\ \mathbb{H} \Rightarrow Q \leq 0\ )^* \text{ et } ^*(\ \mathbb{H} \Rightarrow Q > 0\ )^*\ ] \ \vdash_{cons}\ ^*(\ \mathbb{H} \Rightarrow 1 = 0\ )^* \quad (d).$$

Dans chacun de ces cas, notons d_1 et d_2 les degrés des deux implications fortes données dans l'hypothèse, le degré de l'implication forte construite est respectivement majoré par :

$$\delta_{6,a}(d_1,d_2) = \delta_{6,a'}(d_1,d_2) = d_1 + d_2$$

$$\delta_{6,b}(d_1,d_2) = d_1.d_2$$

$$\delta_{6,c}(d_1,d_2) = d_1.d_2$$

$$\delta_{6,d}(d_1,d_2) = d_1.d_2 + d_2$$

Nous posons :

$$\delta_6(d_1,d_2) = d_1.d_2 + \sup(d_1,d_2) \text{ (symétrique et majore les 4 précédents).}$$

preuve> On se reporte à la preuve et aux notations de la proposition 6. Dans le cas a) ou a'), on réécrit les deux identités en isolant les termes en Q dans un membre, on les multiplie, et on réécrit le résultat. Donc le nouveau degré est majoré par $d_1 + d_2$.

Dans les cas b) ou c) on a $Q^{2m}.S_1$ dans la première identité et $Q.Y_3$ dans la seconde. On doit réécrire les deux identités, élever la deuxième à la puissance 2m et la multiplier par S_1 (d'où degré $\leq 2md_2 + d_1 - 2m = d_1 + 2m.(d_2 - 1)$), on doit enfin multiplier la première identité par

Y_3^{2m} (d'où degré $\le d_1 + 2m.(d_2 - 1)$) et terminer par une manipulation qui n'augmente pas les degrés.
Le cas d) peut être traité en faisant b) puis a') ❑

Remarque : Le fait que ci-dessus le a') est beaucoup moins coûteux que le d) est en soi un phénomène intéressant, qu'on pourrait traduire par : tout se paye.

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

Soit Q 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 chaque cas.

Notons d_1, d_2 et d_3 les degrés des trois implications fortes données dans l'hypothèse, le degré de l'implication forte construite est majoré par :

$$\delta_{7,a}(d_1,d_2,d_3) = (d_1+ d_2).d_3$$

Nous posons :

$$\delta_7(d_1,d_2,d_3) = d_1.d_2+ d_1.d_3+ d_2.d_3$$ (symétrique et majore le précédent)

Corollaire et majorations 7bis : (raisonnements cas par cas, en cascade ou en parallèle)

En cascade : Soient $(A_i)_{i=1,...,h}$ des variables. Pour démontrer que $\mathbb{H}$ est fortement incompatible, on peut raisonner en séparant selon les $2.h+1$ cas :

$$Q = A_i \ (i=1,...,h)\ ,\ Q < A_1\ ,\ Q > A_h\ ,\ A_i < Q < A_{i+1}\ \ (i=1,...,h-1)$$

et en construisant une incompatibilité forte dans chaque cas.

Supposons que d_3 majore les degrés des implications fortes avec les hypothèses $Q = A_i$, et que d_1 majore les degrés des autres implications fortes (intervalles ouverts), alors le degré de l'implication forte construite est majoré par $\delta_{7,b}(d_1,d_3,h)$ donné par les relations récurrentes :

$$\delta_{7,b}(d_1,d_3,1) = \delta_{7,a}(d_1,d_1,d_3)$$
$$\delta_{7,b}(d_1,d_3,h+1) = \delta_{7,a}(\delta_{7,b}(d_1,d_3,h),d_1,d_3)$$

En parallèle : Soient $(Q_i)_{i=1,...,h}$ des polynômes. Pour démontrer que $\mathbb{H}$ est fortement incompatible, on peut raisonner en séparant selon les 3^h cas obtenus en fixant le signe de chaque Q_i, et en construisant une incompatibilité forte dans chaque cas.

Supposons que d_1 majore les degrés des implications fortes (cas par cas), alors le degré de l'implication forte construite est majoré par $\delta_{7,c}(d_1,h)$ donné par les relations récurrentes :

$$\delta_{7,c}(d_1,1) = \delta_{7,a}(d_1,d_1,d_1)\ ,\quad \delta_{7,c}(d_1,h+1) = \delta_{7,c}(\delta_{7,c}(d_1,h),1).$$

Remarque : On notera que dans la majoration en cascade, il n'est pas nécessaire d'avoir les conditions de signes $A_i < A_{i+1}$ dans $\mathbb{H}$, ni même comme conséquence de $\mathbb{H}$. On notera également que les polynômes $Q - A_i$ pourraient être remplacés par des polynômes Q_i arbitraires.

Théorème et majorations 8 : (transitivité des implications fortes)

Soient $\mathbb{H}$, $\mathbb{H}'$, $\mathbb{H}''$ trois systèmes de csg portant sur des polynômes de $\mathbf{K}[\mathbf{X}]$.
Alors: $[\ {}^*(\mathbb{H} \Rightarrow \mathbb{H}')^*$ et ${}^*([\mathbb{H}, \mathbb{H}'] \Rightarrow \mathbb{H}'')^*\ ] \ |\!\!-_{\text{cons}}\ {}^*(\mathbb{H} \Rightarrow \mathbb{H}'')^*$

Notons d_1 et d_2 les degrés des deux implications fortes données dans l'hypothèse, et k le nombre de csg contenues dans $\mathbb{H}'$, alors le degré de l'implication forte construite est

majoré par $\delta_8(d_1,d_2,k)$ qui obéit à la définition récurrente suivante :

$\delta_8(d_1,d_2,1) = \delta_6(d_1,d_2)$

$\delta_8(d_1,d_2,k+1) = \delta_6(d_1,\delta_8(d_1,d_2,k))$

Si $\mathbb{H}'$ ne contient que des conditions du type $Q = 0$ ou $Q \neq 0$, le degré de l'implication forte construite est majoré par $\delta_8(d_1,d_2,k)$ qui obéit à la définition récurrente suivante :

$\delta_{8,a}(d_1,d_2,1) = \delta_{6,c}(d_1,d_2)$

$\delta_{8,a}(d_1,d_2,k+1) = \delta_{6,c}(d_1,\delta_{8,a}(d_1,d_2,k))$.

Existences potentielles

Fonction Δ d'une existence potentielle et d'une implication forte. Fonctionnelle attachée à une manipulation d'existences potentielles

Une existence potentielle $^*(\mathbb{H}_1(\mathbf{X}) \Rightarrow \exists\ \mathbf{T}\ \mathbb{H}_2(\mathbf{X},\mathbf{T}))^*$ signifie par définition un algorithme fournissant la construction :

$^*([\ \mathbb{H}_2(\mathbf{X},\mathbf{T}),\ \mathbb{H}(\mathbf{X},\mathbf{Y})\ ] \Rightarrow 1 = 0)^*$ $\vdash_{cons}$ $^*([\ \mathbb{H}_1(\mathbf{X}),\ \mathbb{H}(\mathbf{X},\mathbf{Y})\ ] \Rightarrow 1 = 0)^*$.

Chaque fois que nous établissons une existence potentielle particulière, nous devons établir des 'majorations primitives récursives de degré' pour cette construction d'implications fortes : le degré de l'implication forte construite est majoré par une fonction $\Delta(d,..;k,...)$ où d est le degré de l'implication forte initiale, k le nombre de csg dans $\mathbb{H}_2$ etc.... (le point-virgule isole les 'variables', qui dépendent de l'implication forte initiale, des 'paramètres', qui ne dépendent que de $\mathbb{H}_1$ et $\mathbb{H}_2$).

Nous disons qu'il s'agit d'une fonction Δ acceptable pour l'existence potentielle considérée, ou encore, (par abus) nous parlons de *la* fonction Δ attachée à l'existence potentielle.

Par ailleurs, puisque toute implication forte peut être vue comme une existence potentielle (proposition 14), nous parlerons également de fonction Δ acceptable pour une implication forte donnée.

Lorsqu'un théorème énonce qu'une existence potentielle résulte d'autres existences potentielles, nous devons préciser comment la fonction Δ de l'implication potentielle déduite se calcule à partir des fonctions Δ^i des existences potentielles supposées. Ce calcul est donné par une *fonctionnelle* $\Phi : (\Delta^i)_{i=1,2,...} \rightarrow \Delta$, fonctionnelle qui doit conserver la classe des fonctions primitives récursives. En fait, nous ne rencontrerons que des fonctionnelles uniformément primitives récursives très simples.

Lemme et majorations 12 : Une existence potentielle $^*(\mathbb{H}_1(\mathbf{X}) \Rightarrow \exists\ \mathbf{T}\ \mathbb{H}_2(\mathbf{X},\mathbf{T}))^*$ reste vraie, avec la même fonction Δ, si on affaiblit la conclusion, si on renforce l'hypothèse, ou si on supprime ou rajoute derrière $\exists$ des variables ne figurant pas dans $\mathbb{H}_2(\mathbf{X},\mathbf{T})$.

Proposition et majorations 13 :

(renforcement simultané de l'hypothèse et de la conclusion)

Si $^*(\mathbb{H}_1(\mathbf{X}) \Rightarrow \exists\ \mathbf{T}\ \mathbb{H}_2(\mathbf{X},\mathbf{T}))^*$ **alors**

$^*([\ \mathbb{H}_1(\mathbf{X})\ ,\ \mathbb{H}_3(\mathbf{X})\ ] \Rightarrow \exists\ \mathbf{T}\ [\ \mathbb{H}_2(\mathbf{X},\mathbf{T}),\ \mathbb{H}_3(\mathbf{X})\ ])^*$

Un cas particulier est le rappel de l'hypothèse dans la conclusion.

Dans les deux cas la fonction Δ est inchangée.

Proposition et majorations 14 :

(existence potentielle comme généralisation de l'implication forte)

Supposons que les systèmes de csg $\mathbb{H}_1$ et $\mathbb{H}_2$ portent sur les seules variables $\mathbf{X}$.
Alors $^*(\ \mathbb{H}_1(\mathbf{X}) \Rightarrow \exists\ \mathbf{T}\ \mathbb{H}_2(\mathbf{X}))^*$ **si et seulement si** $^*(\ \mathbb{H}_1(\mathbf{X}) \Rightarrow \mathbb{H}_2(\mathbf{X}))^*$.
Si k est le nombre de csg dans $\mathbb{H}_2(\mathbf{X})$ et d_1 le degré de $^*(\ \mathbb{H}_1(\mathbf{X}) \Rightarrow \mathbb{H}_2(\mathbf{X}))^*$, une fonction Δ acceptable pour l'existence potentielle $^*(\ \mathbb{H}_1(\mathbf{X}) \Rightarrow \exists\ \mathbf{T}\ \mathbb{H}_2(\mathbf{X}))^*$ est :

$$\Delta_{14}(d;d_1,k) = \delta_8(d_1,d,k)$$

En particulier $\Delta_{14}(d;d_1,1) = \delta_6(d_1,d)$

Plus précisément, si $d_1, d_2, ..., d_k$ sont des majorations pour les degrés des k identités qui donnent l'implication forte, une fonction Δ acceptable pour l'existence potentielle est :

$$\Delta_{14,a}(d;[d_1,d_2, ...,d_k]) = \delta_6(d_1,(\delta_6(d_2,...(\delta_6(d_k,d))...))$$

De même, si $\mathbb{H}_2$ ne contient que des conditions du type $Q = 0$ ou $Q \neq 0$, une fonction Δ acceptable pour l'existence potentielle est :

$$\Delta_{14,b}(d;[d_1,d_2, ...,d_k]) = \delta_{6,c}(d_1,(\delta_{6,c}(d_2,...(\delta_{6,c}(d_k,d))...))$$

Réciproquement, si une implication forte $^*(\ \mathbb{H}_1(\mathbf{X}) \Rightarrow \mathbb{H}_2(\mathbf{X})\ )^*$ admet Δ^1 pour fonction Δ et si δ majore le degré d'une csg ' $P\ \sigma\ 0$ ' dans $\mathbb{H}_2(\mathbf{X})$, alors on peut expliciter l'implication forte $^*(\ \mathbb{H}_1(\mathbf{X}) \Rightarrow P\ \sigma\ 0\ )^*$ de manière que son degré soit majoré par $\Delta^1(\sup(1,2.\delta))$.

preuve> On a au départ une implication forte $^*(\ [\ \mathbb{H}_2(\mathbf{X}),\ \mathbb{H}(\mathbf{X},\mathbf{Y})\ ] \Rightarrow 1 = 0\ )^*$ qui peut être considérée comme un cas particulier pour une implication forte :

$$^*(\ [\ \mathbb{H}_1(\mathbf{X}),\ \mathbb{H}_2(\mathbf{X}),\ \mathbb{H}(\mathbf{X},\mathbf{Y})\ ] \Rightarrow 1 = 0\ )^*$$

On peut alors éliminer une à une les k csg de $\mathbb{H}_2(\mathbf{X})$ en utilisant les k implications fortes élémentaires contenues dans $^*(\ \mathbb{H}_1(\mathbf{X}) \Rightarrow \mathbb{H}_2(\mathbf{X})\ )^*$, ce qui donne le même raisonnement que lorsqu'on a calculé la fonction δ_8 au sujet de la transitivité des implications fortes.
Pour la réciproque, relire la preuve de la partie directe de la proposition 14. ❑

Remarques : 1) Le $\exists\ \mathbf{T}$ dans la proposition 14 est là uniquement pour signaler qu'on veut considérer l'implication forte en tant qu'existence potentielle. Dans le corps de l'article, la proposition 14 peut donc être vue comme justifiant a posteriori le fait qu'on a utilisé deux notations analogues pour l'existence potentielle et l'implication forte. Dans cette annexe, la majoration donnée explicite la fonction Δ de l'existence potentielle à partir du degré de l'implication forte, et donc précise l'énoncé.
2) Considérer une implication forte en tant qu'existence potentielle est au coeur de la preuve constructive du théorème des zéros réel et conduit à un déplacement de point de vue tout à fait intéressant. En fait, même lorsque le quantificateur $\exists$ n'est pas présent, l'existence potentielle est une notion plus subtile que l'implication forte. Par exemple, il se peut que, étant données deux csg $\mathbb{A}$ et $\mathbb{B}$, et un système de csg $\mathbb{H}$, les deux existences potentielles :

$$^*(\ [\ \mathbb{H}, \mathbb{A}\ ] \Rightarrow \mathbb{B})^*,\ ^*(\ [\ \mathbb{H}, \neg\ \mathbb{B}] \Rightarrow \neg\ \mathbb{A}\ )^*$$

soient vérifiées avec des algorithmes plus rapides que ceux donnés par la proposition 14, mais sensiblement différents, et donc avec des fonctions Δ différentes elles aussi. (cf. l'exemple qui suit la définition 14.1 infra)
3) En fait, de nombreuses implications fortes admettent une fonction Δ bien meilleure que celle fournie par le résultat de la proposition 14. Ceci est précisé dans quelques définitions et propositions 14.n. qui suivent la majoration 17 infra (paragraphe : implications triviales et implications simples).

Proposition et majorations 15 : (raisonnement cas par cas)

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

$^*(\mathbb{H}_1(\mathbf{X}) \Rightarrow \exists\ \mathbf{T}\ \mathbb{H}_2(\mathbf{X},\mathbf{T}))^*$ il suffit de démontrer chacune des existences potentielles $^*([\ \mathbb{H}_1(\mathbf{X}),\ Q\ \sigma\ 0\ ] \Rightarrow \exists\ \mathbf{T}\ \mathbb{H}_2(\mathbf{X},\mathbf{T}))^*$ pour les 3 signes σ possibles.

i) Si Δ^i (i = 1,2,3) sont les trois fonctions Δ des existences potentielles supposées, une fonction Δ pour l'existence potentielle déduite est donnée par :

$\Delta = \Phi_{15}(\Delta^1,\Delta^2,\Delta^3)$ où $\Delta = \delta_7$ o $(\Delta^1,\Delta^2,\Delta^3)$

ii) Dans le cas où on démontre une existence potentielle cas par cas avec deux signes généralisés opposés $=$ et $\neq$, on obtient :

$\Delta = \Phi_{15,c}(\Delta^1,\Delta^2)$ où $\Delta = \delta_{6,c}$ o $(\Delta^1,\Delta^2) = \Delta^1.\Delta^2$

iii) Dans le cas où on démontre une existence potentielle cas par cas avec deux signes généralisés opposés $>$ et $\leq$ on obtient :

$\Delta = \Phi_{15,d}(\Delta^1,\Delta^2)$ où $\Delta = \delta_{6,d}$ o (Δ^1,Δ^2)

iv) Enfin, dans le cas où on démontre une existence potentielle cas par cas avec deux signes généralisés $\geq$ et $\leq$ on obtient :

$\Delta = \Phi_{15,a}(\Delta^1,\Delta^2)$ où $\Delta = \delta_{6,a}$ o $(\Delta^1,\Delta^2) = \Delta^1 + \Delta^2$

Théorème et majorations 16 : (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

$^*(\mathbb{H}_1(\mathbf{X}) \Rightarrow \exists\ \mathbf{T}\ \mathbb{H}_2(\mathbf{X},\mathbf{T}))^*$ et $^*(\mathbb{H}_2(\mathbf{X},\mathbf{T}) \Rightarrow \exists\ \mathbf{U}\ \mathbb{H}_3(\mathbf{X},\mathbf{T},\mathbf{U}))^*$

alors on a aussi :

$^*(\mathbb{H}_1(\mathbf{X}) \Rightarrow \exists\ \mathbf{T}, \mathbf{U}\ \ \mathbb{H}_3(\mathbf{X},\mathbf{T},\mathbf{U}))^*$

Supposons que la première existence potentielle fournisse une majoration primitive récursive $\Delta^1(d;\mathbf{p})$ où d est le degré de $^*([\ \mathbb{H}_2(\mathbf{X},\mathbf{T}),\ \mathbb{H}(\mathbf{X},\mathbf{Y})\ ] \Rightarrow 1 = 0)^*$ et $\mathbf{p}$ représente certains paramètres dépendant de $\mathbb{H}_1(\mathbf{X})$ et $\mathbb{H}_2(\mathbf{X},\mathbf{T})$, supposons de même une majoration primitive récursive $\Delta^2(d;\mathbf{q})$ fournie par la deuxième existence potentielle, alors une fonction Δ pour l'existence potentielle construite est donnée par :

$\Delta = \Phi_{16}(\Delta^1,\Delta^2)$: $\Delta(d;\mathbf{p},\mathbf{q}) = \Delta^1(\Delta^2(d;\mathbf{q});\mathbf{p})$

Remarques: 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. La fonction Δ de la nouvelle existence potentielle est alors obtenue en appliquant les majorations 14 et 16.

Nous avons ici donné un énoncé du théorème 16 légèrement plus faible que dans l'article. On récupèrera la forme "forte" en combinant avec la proposition 13.

Proposition et majorations 17 : (l'existence implique l'existence potentielle)

Soient $P_1,P_2,...,P_m \in \mathbf{K}[\mathbf{X}]$ et notons $\mathbf{P}(\mathbf{X})$ pour $P_1(\mathbf{X})$, ..., $P_m(\mathbf{X})$. Si δ majore les degrés des P_i, l'existence potentielle : $^*(\mathbb{H}_2(\mathbf{X},\mathbf{P}(\mathbf{X})) \Rightarrow \exists\ \mathbf{T}\ \mathbb{H}_2(\mathbf{X},\mathbf{T}))^*$ accepte pour fonction Δ : $\Delta_{17}(d;\delta) = d.\sup(1,\delta)$

Corollaire :

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

Si Δ^1 est une fonction Δ acceptable pour l'implication forte de l'hypothèse, une fonction Δ acceptable pour la conclusion est donnée par :

$\Delta = \Phi_{17}(\Delta^1;\delta)$ où $\Delta = \Delta^1(d.\sup(1,\delta))$ où δ majore les degrés des P_i.

Implications triviales et implications simples

Définition 14.1 : (**implications triviales**)

Une implication $\mathbb{H}_1(\mathbf{X}) \Rightarrow \mathbb{H}_2(\mathbf{X})$ est dite triviale lorsque toute implication forte $^*([\ \mathbb{H}_2(\mathbf{X}),\ \mathbb{H}(\mathbf{X},\mathbf{Y})\ ] \Rightarrow 1 = 0)^*$ fournit par simple relecture l'implication forte $^*([\ \mathbb{H}_1(\mathbf{X}),\ \mathbb{H}(\mathbf{X},\mathbf{Y})\ ] \Rightarrow 1 = 0)^*$. L'implication forte $^*(\mathbb{H}_1(\mathbf{X}) \Rightarrow \mathbb{H}_2(\mathbf{X}))^*$ accepte donc pour fonction Δ : $\Delta_0(d) = d$.

Exemples : On a l'implication triviale $[\ A > 0\ ,\ B > 0\ ] \Rightarrow A.B > 0$ mais l'implication 'contrapposée' : $[\ A > 0\ ,\ A.B \leq 0\ ] \Rightarrow B \leq 0$ ne l'est pas. Ceci, bien que les implications fortes soient exactement les mêmes dans les deux cas.
De même, l'implication $B = 0 \Rightarrow A.B = 0$ est triviale, tandis que la contrapposée ne l'est pas.

On a l'implication triviale $[\ A \geq 0\ ,\ A \neq 0\ ] \Rightarrow A > 0$, tandis que $[\ A \geq 0\ ,\ A \leq 0\ ] \Rightarrow A = 0$ ne l'est pas.

Définitions 14.2 : (**implications simples**)

a) Une implication : $\mathbb{H}_1(\mathbf{X}) \Rightarrow T(\mathbf{X}) = 0$ est dite simple lorsqu'elle est donnée par une égalité $T = \Sigma\ N_i.V_i$ où les N_i sont les polynômes supposés nuls dans $\mathbb{H}_1$.
On appelle degré absolu d'une telle implication simple l'entier : $\sup(\ d(N_i.V_i)\ ) - d(T)$, et degré relatif le rationnel $\sup(\ d(N_i.V_i)\ ) / d(T)$

b) Une implication : $\mathbb{H}_1(\mathbf{X}) \Rightarrow T(\mathbf{X}) \geq 0$ est dite simple lorsqu'elle est donnée par une égalité $T = \Sigma\ P_h.(\Sigma\ u_{h,j}\ U_{h,j}^{\ 2}\ ) + \Sigma\ N_i.V_i$ avec les mêmes hypothèses qu'en a), et où en outre les P_h sont des produits de polynômes supposés > 0, ou ≥ 0 , dans $\mathbb{H}_1$. (les $u_{h,j}$ sont des positifs de $\mathbf{K}$).
On appelle degré absolu d'une telle implication simple la différence :

$\sup(\ d(N_i.V_i)\ ,\ d(P_h.U_{h,j}^{\ 2})\ ) - d(T)$, et degré relatif leur rapport.

c) Une implication : $\mathbb{H}_1(\mathbf{X}) \Rightarrow T(\mathbf{X}) > 0$ est dite simple lorsqu'elle est donnée par une égalité $T = S.R^2 + \Sigma\ P_h.(\Sigma\ u_{h,j}\ U_{h,j}^{\ 2}\ ) + \Sigma\ N_i.V_i$ avec les mêmes hypothèses qu'en b), et où en outre S (resp. R) est un produit de polynômes supposés > 0 (resp $\neq 0$) dans $\mathbb{H}_1$.
On appelle degré relatif d'une telle implication simple le rationnel :
$\sup(\ d(S.R^2), d(N_i.V_i)\ ,\ d(P_h.U_{h,j}^{\ 2})\ ) / d(T)$

d) Une implication : $\mathbb{H}_1(\mathbf{X}) \Rightarrow T(\mathbf{X}) \neq 0$ est dite simple lorsqu'elle est donnée par une égalité $T = S.R + \Sigma\ N_i.V_i$ avec les mêmes hypothèses qu'en c). On appelle degré relatif

d'une telle implication simple le rationnel : $\sup(d(S.R), d(N_i.V_i)) / d(T)$

e) Une implication $\mathbb{H}_1(\mathbf{X}) \Rightarrow \mathbb{H}_2(\mathbf{X})$ est dite simple lorsque chacune des csg du second membre résulte de $\mathbb{H}_1(\mathbf{X})$ par une implication simple. On appelle degré relatif le sup des degrés relatifs des implications simples considérées.

Il y a un algorithme particulièrement simple pour expliciter l'existence potentielle correspondant à une implication simple donnée du type :

$$\mathbb{H}_1(\mathbf{X}) \Rightarrow T(\mathbf{X}) = 0$$

Dans l'implication forte :

$$^*([\mathbb{H}(\mathbf{X},\mathbf{Y}), T(\mathbf{X}) = 0] \Rightarrow 1 = 0)^*$$

on remplace T par $\Sigma N_i.V_i$.

Par exemple si T apparaissait sous forme $T.W$, on aura maintenant une somme $\Sigma N_i.(W.V_i)$ où chaque terme a un rôle autonome dans la nouvelle implication forte :

$$^*([\mathbb{H}(\mathbf{X},\mathbf{Y}), \mathbb{H}_1(\mathbf{X})] \Rightarrow 1 = 0)^* .$$

On voit que le degré de cette dernière a augmenté au plus de δ = degré absolu de l'implication simple, et on en déduit qu'il a été multiplié au plus par δ' = degré relatif de l'implication simple. Des considérations du même genre s'appliquent aux autres cas d'implications simples et on obtient :

Proposition 14.3 : (implications simples en tant qu'existences potentielles)

a) Une implication simple : $\mathbb{H}_1(\mathbf{X}) \Rightarrow T(\mathbf{X}) = 0$ ou $\mathbb{H}_1(\mathbf{X}) \Rightarrow T(\mathbf{X}) \geq 0$ accepte pour fonction Δ : $\Delta_{14,3,a}(d;\delta) = d + \delta$ où δ est le degré absolu de l'implication simple.

b) Une implication simple : $\mathbb{H}_1(\mathbf{X}) \Rightarrow \mathbb{H}_2(\mathbf{X})$ accepte pour fonction Δ : $\Delta_{14,3}(d;\delta') = d.\delta'$ où δ' est le degré relatif de l'implication simple.

Remarque : Souvent, une implication simple a un degré absolu nul et un degré relatif égal à 1, ce qui signifie que l'implication forte considérée ne coûte rien pour ce qui concerne les degrés. Nous dirons indifféremment ‘implication simple de degré relatif égal à 1’ ou ‘implication simple qui ne coûte rien’. Ce sont surtout ces implications là qu'il est utile de traiter directement (plutôt que par la proposition 14) pour améliorer le résultat du calcul de majoration. Dans une éventuelle mise en oeuvre de l'algorithme, il est *toujours* plus économique de traiter une implication simple en tant que telle.

Trois exemples :

Subsitution d'égaux :

L'implication $U = V \Rightarrow P(\mathbf{X},U) = P(\mathbf{X},V)$ est une implication simple qui ne coûte rien.

Somme de deux positifs :

L'implication $[A > 0, B \geq 0] \Rightarrow A + B > 0$ est simple de degré relatif $\delta' = \sup(d(A),d(B))/d(A+B)$ et accepte la fonction $\Delta : d \rightarrow d.\delta'$.

L'implication $[A \geq 0, B \geq 0] \Rightarrow A + B \geq 0$ est simple de degré absolu $\delta = \sup(d(A),d(B)) - d(A+B)$ et accepte la fonction $\Delta : d \rightarrow d + \delta$.

Point où un polynôme unitaire a le signe de son coefficient dominant :

Soit Q un polynôme, unitaire en la variable U distincte des X_i :

$$Q(\mathbf{X},U) = U^s + C_{s-1}(\mathbf{X}).U^{s-1} + ... + C_1(\mathbf{X}).U + C_0(\mathbf{X})$$

Soit $V(\mathbf{X}) = s + C_{s-1}(\mathbf{X})^2 + ... + C_1(\mathbf{X})^2 + C_0(\mathbf{X})^2$.

Alors on a des implications simples simultanées qui ne coûtent rien :

$$[\ ] \Rightarrow Q(\mathbf{X},V(\mathbf{X})) > 0$$
$$[\ ] \Rightarrow Q^{(i)}(\mathbf{X},V(\mathbf{X})) > 0 \qquad \text{(dérivées par rapport à U)}$$

preuve> Il s'agit d'écrire $Q(\mathbf{X},V(\mathbf{X}))$ comme une somme de carrés et d'une constante strictement positive. Ce n'est pas trop difficile en utilisant l'égalité :

$$(1 + C + C^2) = 3/4 + (1/2 + C)^2 \qquad ❑$$

Proposition 14.4 : (fonctions Δ de quelques implications particulières)

a) L'implication $[A > 0 , A.B \geq 0] \Rightarrow B \geq 0$ accepte pour fonction Δ : $\Delta_{14,4,a}(d;\delta) = d + 2.\delta$ où $\delta = d(A)$. Même chose avec $=$ à la place de $\geq$.

b) L'implication $[A > 0 , A.B > 0] \Rightarrow B > 0$ accepte pour fonction Δ : $\Delta_{14,4,b}(d;\delta,\delta') = \sup(d.\delta', d + 2.\delta)$ où $\delta = d(A)$, $\delta' = d(A.B) / d(B)$.

c) L'implication $[A \geq 0 , A.B > 0] \Rightarrow B \geq 0$ accepte pour fonction Δ : $\Delta_{14,4,c}(d;\delta) = d + 2.\delta$ où $\delta = d(A.B)$.

d) L'implication $[A \geq 0 , A.B > 0] \Rightarrow B > 0$ accepte pour fonction Δ : $\Delta_{14,4,d}(d;\delta,\delta') = \sup(d.\delta', d + 2.\delta)$ où $\delta = d(A.B)$, $\delta' = d(A.B) / d(B)$.

e) L'implication $[A.B > 0 , A+B > 0] \Rightarrow [A > 0 , B > 0]$ accepte pour fonction Δ : $\Delta_{14,4,e}(d;\delta,\delta') = d.\delta' + 2\delta$ où $\delta' = d(AB)/\inf(d(A),d(B))$, $\delta = \sup(d(A),d(B))$.

f) L'implication $A^{2k} \leq 0 \Rightarrow A = 0$ accepte pour fonction Δ : $\Delta_{14,4,f}(d;k) = 2k.d$

De même l'implication $[A \geq 0 , A \leq 0] \Rightarrow A = 0$ accepte pour fonction Δ : $d \rightarrow 2d$.

g) L'implication $P(\mathbf{X},U) \neq P(\mathbf{X},V) \Rightarrow U \neq V$ accepte pour fonction Δ : $\Delta_{14,4,g}(d;\delta') = d.\delta'$ où $\delta' = d(P(\mathbf{X},U) - P(\mathbf{X},V)) / d(U - V)$

preuve> Pour le a) : on multiplie, terme à terme, l'implication forte par A^2, en prenant soin de remplacer les $B.A^2$ par $(BA).A$.
Pour le b). Si, dans l'implication forte, B n'apparaît qu'en tant que ≥ 0, on applique le a). Si B apparaît en tant que > 0 avec l'exposant 2h, on doit tout multiplier par A^{2h}, remplacer $A^{2h}.B^{2h}$ par $(AB)^{2h}$ dans le terme > 0 et, dans les termes ≥ 0, $B.A^{2h}$ par $(BA).A.(A^{h-1})^2$
Pour le c). On multiplie, terme à terme, l'implication forte par $(AB)^2$, en prenant soin de remplacer les $B.(AB)^2$ par $(BA).A.B^2$.
Pour le d). Si, dans l'implication forte, B n'apparaît qu'en tant que ≥ 0, on fait comme en c) Sinon : comme en b) 2ème cas.
Pour le e). Si A et B apparaissent en tant que > 0 avec des exposants 2h et 2k, avec par exemple $h > k$, on commence par tout multiplier par B^{2h-2k}, ce qui fait apparaître $(AB)^{2h}$ dans le terme > 0. Si A et B apparaissent maintenant (sans exposant) de manière séparée dans les termes ≥ 0 sous forme $A.U + B.V$ on remarque qu'après multiplication par $(A+B)^2$ on peut remplacer $(A+B)^2(AU+BV)$ par $(A+B).A^2.U + (A+B).B^2.V + (A+B).(AB).(U+V)$. Ainsi toutes les occurrences isolées de A ou B ont été supprimées.
Pour le f) : on isole le terme en A au second membre, on élève à la puissance 2k, on réécrit le premier membre, on remet le second membre dans le premier en tant que $A^{2k} \leq 0$ ❑

Théorème et majorations 10 : (évidence forte du lemme de Thom)

Soit T une variable distincte des X_i.Soit $P \in \mathbf{K}[\mathbf{X}][T]$, de degré s en T et de degré total δ, $\sigma_1, \sigma_2,..., \sigma_s$ une liste formée de $<$ ou $>$. On note $\mathbb{H}(\mathbf{X},T)$ ou $\mathbb{H}(T)$ le système de csg : $P'(\mathbf{X},T)\ \sigma_1\ 0$, ..., $P^{(i)}(\mathbf{X},T)\ \sigma_i\ 0$, ..., $P^{(s)}(\mathbf{X},T)\ \sigma_s\ 0$ (les dérivées sont par rapport à T).
Soit $\mathbb{H}'(T)$ le système de csg obtenu à partir de $\mathbb{H}(T)$ en relachant toutes les conditions de

signe sauf celle relative à $P^{(s)}$.

Soit $\mathbb{H}_1(T)$ le système de csg : $P^{(s)}(\mathbf{X},T) > 0$, $P^{(i)}(\mathbf{X},T) \geq 0$, i = 1, ..., s–1 .

Soient enfin trois variables U , V , Z distincte des X_i .

On a alors les évidences fortes suivantes :

$^*([\, \mathbb{H}'(U),\ \mathbb{H}'(V),\ P(U) = P(V)\,] \ \Rightarrow\ U = V)^*$ (1)

$^*([\, \mathbb{H}'(U),\ \mathbb{H}'(V)\ ,\ U\ \sigma_1\ V\,] \ \Rightarrow\ P(U) > P(V))^*$ (2,a)

$^*([\, \mathbb{H}'(U),\ \mathbb{H}'(V)\ ,\ P(U)\ \sigma_1\ P(V)\,] \ \Rightarrow\ U > V)^*$ (2,b)

$^*([\, \mathbb{H}_1(U),\ V > U\,] \ \Rightarrow\ P(V) > P(U))^*$ (2,c)

$^*([\, \mathbb{H}_1(U),\ P(U) > P(V)\,] \ \Rightarrow\ U > V)^*$ (2,d)

$^*([\, \mathbb{H}'(U)\ ,\ \mathbb{H}'(V),\ U < Z < V\,] \ \Rightarrow\ \mathbb{H}(Z))^*$ (5)

Les implications fortes (2,a), (2,c) et (5) sont des implications simples qui ne coûtent rien et acceptent donc pour fonction Δ : $\Delta_0(d) = d$

Les degrés des implications fortes (2,b) et (2,d) sont majorés par : $\delta_{10,b}(\delta) = 2.\delta$ donc acceptent pour fonction Δ : $\Delta_{10}(d;\delta) = \delta_6(d,2\delta)$.

preuve> Les implications fortes (2,a), (2,b) résultent de formules de Taylor mixtes de degrés majorés par δ. Les implication fortes (2,c) et (2,d) résultent de la formule de Taylor ordinaire au point U. Les formules établies pour l'implication forte (5) résultent des formules de Taylor mixtes et sont aussi a priori de degrés majorés par δ.
Dans les cas (2,a), (2,c) et (5) on constate qu'il s'agit d'implications simples qui ne coûtent rien. Dans les cas (2,b) et (2,d), pour passer à une implication forte sous forme "normale", il faut multiplier par un polynôme de degré au plus δ . D'où la majoration $2.\delta$. ❑

Remarques:
1) Supposons pour simplifier que σ_1 est $>$. On a, comme pour (2,a) une implication simple qui ne coûte rien :

$$^*([\, \mathbb{H}'(U),\ \mathbb{H}'(V)\ ,\ U \geq V\,] \ \Rightarrow\ P(U) \geq P(V))^*$$

Par contre l'implication forte suivante est donnée par (2,b) (permuter U et V) et "coûte quelque chose" (en tant qu'existence potentielle) :

$$^*([\, \mathbb{H}'(U),\ \mathbb{H}'(V)\ ,\ P(U) < P(V)\,] \ \Rightarrow\ U < V)^*$$

Pourtant, en tant qu'implications fortes, on a écrit deux fois la même chose.
2) Si U, V, Z sont des polynômes de degrés majorés par δ_1 et si δ désigne maintenant le degré en **X** de P, on obtient sans peine les majorations de degrés suivantes pour les implications fortes du théorème 10 :

– (2,a) , (2,c) , (5) : $2\delta + (s+1).\delta_1$
– (2,b) , (2,d) : $2\delta + 2s.\delta_1$
– (1) : $4\delta + 2(s+1).\delta_1$

et on peut en déduire des fonctions Δ acceptables en appliquant le proposition 14 : plus générales, elles sont moins bonnes que celles données dans le théorème 10.

L'existence potentielle de l'inverse d'un non nul, et la fonction Δ attachée à cette existence potentielle

Théorème et majorations 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:

$$^*(U(\mathbf{X}) \neq 0 \ \Rightarrow\ \exists\ T\quad 1 = U(\mathbf{X}).T)^*$$

Soit δ le degré de U, une fonction Δ acceptable pour l'existence potentielle est

$$\Delta_{20}(d;\delta) = d + d.\delta + \delta$$

preuve> Soit système de csg $\mathbb{H}(\mathbf{X},\mathbf{Y})$, on a :

$$^*([U(\mathbf{X}).T = 1,\ \mathbb{H}(\mathbf{X},\mathbf{Y})] \Rightarrow 1 = 0)^* \ \ |\overline{\ }_{cons}\ ^*([U(\mathbf{X}) \neq 0,\ \mathbb{H}(\mathbf{X},\mathbf{Y})] \Rightarrow 1 = 0)^*$$

Soit δ le degré de U, t le degré en T et d le degré total de la première implication forte ci-dessus. On multiplie cette identité par U^{2m} avec $2m = t$ ou $t+1$, les degrés sont alors majorés par $d + \delta.(t+1)$, on remplace ensuite des $U^i.T^i$ $(i \leq 2m)$ par 1 modulo $(1 - U.T)$, ce qui abaisse les degrés, sauf éventuellement celui du facteur de $(1 - U.T)$, et a posteriori, ce terme de la somme ne peut être de degré supérieur aux autres. Le degré de l'implication forte construite est donc majoré par : $d + \delta.(d+1)$.

On notera que si $d < \delta$, l'identité initiale ne fait pas usage de $1 - U.T$, et donc en remplaçant T par 0 on obtient $^*(\mathbb{H}(\mathbf{X},\mathbf{Y}) \Rightarrow 1 = 0)^*$.

On notera également que si $\delta = 0$ on peut simplifier l'algorithme en : «remplacer T par le scalaire 1/U». ❑

Corollaire et majorations 20 bis :

On a l'existence potentielle d'un point où un polynôme P donné a le signe de son coefficient dominant supposé non nul.

Plus précisément, en notant $P(\mathbf{X},U)$ le polynôme et $C(\mathbf{X})$ son coefficient dominant :

$$^*(C(\mathbf{X}) > 0 \Rightarrow \exists\ U\ [\ P(\mathbf{X},U) > 0\ ;\ P^{(i)}(\mathbf{X},U) > 0\ ,\ i = 1, ..., s\ ])^*$$

Si δ majore le degré de P en $\mathbf{X}$ et s le degré en U, l'existence potentielle accepte pour fonction Δ :

$$\Delta_{20,a}(d;0,s) = \Delta_{20,a}(d;\delta,0) = d \quad \text{et pour } s \text{ et } \delta > 0$$
$$\Delta_{20,a}(d;\delta,s) = \Delta_{20}(\ d.(\delta+1).(1+2s\delta)\ ;\ \delta\ )$$

preuve> Les cas avec $\delta = 0$ ou $s = 0$ sont faciles.

On a : $P(\mathbf{X},U) = C(\mathbf{X}).U^s + C_{s-1}(\mathbf{X}).U^{s-1} + ... + C_1(\mathbf{X}).U + C_0(\mathbf{X})$.

Par l'existence potentielle de l'inverse d'un non nul, on a :

$$^*(C(\mathbf{X}) > 0 \Rightarrow \exists\ T\ [\ 1 = C(\mathbf{X}).T\ ,\ C(\mathbf{X}) > 0\ ])^* \qquad (1)$$

acceptant pour fonction Δ : $\Delta_{20}(d;\delta)$.

On a une implication simple de degré relatif 1

$$1 = C(\mathbf{X}).T \Rightarrow C(\mathbf{X}).T > 0$$

et par la proposition 14.4.b, l'implication : $[\ C(\mathbf{X}) > 0,\ C(\mathbf{X}).T > 0\ ] \Rightarrow T > 0$ accepte pour fonction Δ : $\sup(d.(\delta+1),\ d+2\delta)$. Donc l'implication forte :

$$^*([\ C(\mathbf{X}) > 0,\ 1 = C(\mathbf{X}).T\ ] \Rightarrow [\ C(\mathbf{X}) > 0,\ 1 = C(\mathbf{X}).T,\ T > 0\ ])^* \qquad (2)$$

accepte pour fonction Δ : $\sup(d.(\delta+1),\ d+2\delta)$.

Par transitivité :

$$^*(C(\mathbf{X}) > 0 \Rightarrow \exists\ T\ [\ 1 = C(\mathbf{X}).T,\ C(\mathbf{X}) > 0,\ T > 0\ ])^* \qquad (3)$$

accepte pour fonction Δ : $\Delta_{20}(\ \sup(d.(\delta+1),\ d+2\delta)\ ;\ \delta\ )$.

Soit $Q(\mathbf{X},V) = V^s + C_{s-1}.V^{s-1} + C_{s-2}.C.V^{s-1} + ... + C_1.C^{s-2}.V + C_0.C^{s-1}$
$= V^s + D_{s-1}(\mathbf{X}).V^{s-1} + ... + D_1(\mathbf{X}).V + D_0(\mathbf{X})$

avec les degrés des D_i majorés par $s.\delta$.

On a : $P(\mathbf{X},T.V) \equiv T^{s-1}\ Q(\mathbf{X},V) \quad (\mod 1 - C.T) \qquad (\alpha)$

Plus précisément $P(\mathbf{X},T.V) = T^{s-1}\ Q(\mathbf{X},V) + R(\mathbf{X},T,V).(1 - C.T) \qquad (\beta)$

Soit $V(\mathbf{X}) = s + D_{s-1}(\mathbf{X})^2 + ... + D_1(\mathbf{X})^2 + D_0(\mathbf{X})^2$ de degré $\leq 2s\delta$.

Alors, dans la ligne (β), les degrés des deux termes du second membre sont non supérieurs à celui du premier membre, puisque le degré total de P est égal à celui de son terme $C.T^s.V(\mathbf{X})^s$.

En se référant à l'exemple qui suit la proposition 14.3, on peut écrire $Q(\mathbf{X},V(\mathbf{X}))$ comme une somme de carrés, sans augmenter les degrés dans la réécriture.
L'égalité (β) , après qu'on ait remplacé $Q(\mathbf{X},V(\mathbf{X}))$ par une somme de carrés fournit donc une implication simple qui ne coûte rien :

$$[\ 1 = C.T,\ T > 0\ ] \Rightarrow\ P(\mathbf{X},T.V(\mathbf{X})) > 0 \qquad (4)$$

Par ailleurs (l'existence implique l'existence potentielle, prop. 17) :

$$^{*}(\ P(\mathbf{X},T.V(\mathbf{X})) > 0 \Rightarrow\ \exists\ U\ \ P(\mathbf{X},U) > 0\ )^{*} \qquad (5)$$

En composant (4) avec (5) on obtient l'existence potentielle:

$$^{*}(\ [\ C > 0,\ 1 = C.T,\ T > 0\ ] \Rightarrow\ \exists\ U\ \ P(\mathbf{X},U) > 0\ )^{*} \qquad (6)$$

acceptant pour fonction Δ : $d.(2s\delta+1)$.
Par transitivité (3) et (6) donnent :

$$^{*}(\ C(\mathbf{X}) > 0\ \Rightarrow\ \exists\ U\ \ P(\mathbf{X},U) > 0\ )^{*}$$

acceptant pour fonction Δ : $\Delta_{20,a}(d;\delta,s) = \Delta_{20}(\ d.(2s\delta+1).(\delta+1)\ ;\ \delta\ )$.
La même majoration fonctionne pour :

$$^{*}(\ C(\mathbf{X}) > 0\ \Rightarrow\ \exists\ V\ [\ P(\mathbf{X},V) > 0;\ P^{(i)}(\mathbf{X},V) > 0\ ,\ i = 1, ...,\ s\ ]\ )^{*}$$

puisque la nouvelle forme de (4) est encore donnée par une implication simple qui ne coûte rien. ❑

L'existence potentielle d'une racine d'un polynôme, et la fonction Δ attachée à cette existence potentielle.

Théorème et majorations 21 : (autorisation de rajouter une racine à un polynôme qui change de signe).

Soient des variables distinctes $X_1, X_2,..., X_n$, Z, U et V, soit $P(\mathbf{X},Z)$ un polynôme de $\mathbf{K}[X_1, X_2,..., X_n][Z]$. Notons $P(Z)$ pour $P(\mathbf{X},Z)$, on a l'existence potentielle :

$$^{*}(\ P(U).P(V) \le 0\ \Rightarrow\ \exists\ Z\ \ P(Z) = 0)^{*}\ .$$

Dans le cas où le polynôme P, de degré s, ne contient que la variable Z, l'existence potentielle accepte la fonction $\Delta_{21,0}(d;s)$ définie par les relations récurrentes :

$\Delta_{21,0}(d;0) = 1$

$\Delta_{21,0}(d;1) = d$

$\Delta_{21,0}(d;s+2) = \Delta_{14,a}(\ 2d\ ;\ [\Delta_{21,0}(d;s),d,d]\ )$

Dans le cas général, supposons le degré total de $P(\mathbf{X},Z)$ égal à δ et son degré en Z égal à s. Alors une fonction Δ acceptable pour l'existence potentielle, notée $\Delta_{21}(d;\delta,s)$ (avec $d \ge \delta$) peut être calculée au moyen des formules récurrentes suivantes (qui font intervenir des fonctions auxiliaires):

$\Delta_{21}(d;\delta,0) = 2d$

$\Delta_{21}(d;\delta,1) = \delta_{6,c}(2d,\Delta_{20}(d.(\delta+1);\delta - 1))$

$\delta_1(d,\delta,s+2) = (d - s - 1).(\delta - s - 2) + d$ que nous notons δ_1 ci-dessous

$\Delta_{21,u}(d;\delta,s+2) = \Delta_{14,a}(\ 4\delta_1\ ;\ [\Delta_{21}(\delta_1;\delta_1,s),\delta_1,\delta_1]\ )$

$\Delta_{21,a}(d;\delta,s+2) = \Delta_{21}(d;\delta,s+1) + 2\delta$

$\Delta_{21,b}(d;\delta,s+2) = \Delta_{20}(\ \Delta_{21,u}(d;\delta,s+2) + 2(\delta - s - 2))\ ;\ \delta\ )$

$\Delta_{21}(d;\delta,s+2) = \delta_{6,c}(\ \Delta_{21,a}(d;\delta,s+2)\ ,\ \Delta_{21,b}(d;\delta,s+2)\ )$

preuve> Nous renvoyons le cas $n = 0$ à la fin de la preuve.
Voyons le cas général.

Tout d'abord, si $s = 0$, l'implication forte $^*(P^2 \le 0 \Rightarrow P = 0)^*$ admet pour fonction Δ la fonction $d \to 2.d$ (prop. 14.4.f)) et elle se relit :

$$^*(P(U).P(V) \le 0 \Rightarrow P(Z) = 0)^* .$$

Si $s = 1$, $P(\mathbf{X},U) = C(\mathbf{X}).U - D(\mathbf{X})$. On raisonne selon le signe de $C(\mathbf{X})$.

Avec $C(\mathbf{X}) = 0$:

On a une implication simple qui ne coûte rien : $[C(\mathbf{X}) = 0, P(U).P(V) \le 0] \Rightarrow P(Z)^2 \le 0$ obtenue en écrivant $P(Z)^2 \equiv P(U).P(V) \pmod{C(\mathbf{X})}$. Puis, comme pour $s = 0$, l'implication $P(Z)^2 \le 0 \Rightarrow P(Z) = 0$, qui accepte pour fonction Δ la fonction $d \to 2d$.

Avec $C(\mathbf{X}) \neq 0$:

On a tout d'abord l'existence potentielle $^*(C(\mathbf{X}) \neq 0 \Rightarrow \exists\ T\ \ 1 = C(\mathbf{X}).T)^*$

avec pour fonction Δ : $\Delta_{20}(d;\delta-1)$

L'implication simple $1 = C(\mathbf{X}).T \Rightarrow P(\mathbf{X},T.D(\mathbf{X})) = 0$, ne coûte rien.

Elle fournit donc (prop. 17) l'existence potentielle :

$$^*(1 = C(\mathbf{X}).T \Rightarrow \exists\ Z\ \ P(\mathbf{X},Z) = 0)^*$$

avec pour fonction Δ la fonction $d.(\delta+1)$.

En combinant ces deux existences potentielles, on obtient :

$^*(C(\mathbf{X}) \neq 0 \Rightarrow \exists\ T , Z\ \ P(\mathbf{X},Z) = 0)^*$ avec la fonction $\Delta : \Delta_{20}(d.(\delta+1);\delta-1)$

Il ne reste plus qu'à regrouper les deux cas $C(\mathbf{X}) = 0$ et $C(\mathbf{X}) \neq 0$ (majoration 15,c).

Nous passons à la partie "récurrence sur s " de la preuve. Nous supposons P de degré $s+2$ en Z.

Nous cherchons tout d'abord une majoration $\Delta_{21,u}(d ; \delta , s+2)$ *valable pour le cas où* P *est unitaire*. Il s'agit, pour tout système $\mathbb{H}$ de csg où ne figure pas la variable Z, d'expliciter la majoration correspondant à la construction:

$$^*(\mathbb{H} \Rightarrow P(\mathbf{X},Z) \neq 0)^* \ \ |\!\!\sim_{cons}\ ^*(\mathbb{H} \Rightarrow P(\mathbf{X},U).P(\mathbf{X},V) > 0)^*$$

L'implication forte de l'hypothèse, supposée de degré $d \ge \delta$, (sinon, P n'y figure pas explicitement) s'écrit :

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

avec $Q_i(\mathbf{X}) \in \mathcal{C}p(F_{\ge} \cup F_{>})$ et $N_j(\mathbf{X}) \in F_{=}$. Les polynômes $B_i(\mathbf{X},Z)$ et $C_j(\mathbf{X},Z)$ peuvent être pris modulo P en Z (parce que P est unitaire), auquel cas $\deg_Z(G) \le s$. Après cette réduction modulo P nous obtenons une implication forte $\mathbb{I}$ dont le degré est majoré par :

$\delta_1(d,\delta,s+2) = (d-s-1).(\delta-s-2) + d$ que nous notons δ_1 dans la suite

L'implication forte $\mathbb{I}$ se relit tout d'abord :

$$^*(\mathbb{H} \Rightarrow G(\mathbf{X},Z) \neq 0)^*$$ de degré majoré par δ_1

Ce qui fournit, par hypothèse de récurrence, une implication forte:

$$^*(\mathbb{H} \Rightarrow G(\mathbf{X},U).G(\mathbf{X},V) > 0)^*$$ de degré majoré par $\Delta_{21}(\delta_1;\delta_1,s)$

En remplaçant Z par U et V l'implication forte $\mathbb{I}$ se relit

$$^*(\mathbb{H} \Rightarrow P(\mathbf{X},U).G(\mathbf{X},U) > 0)^* \ , \ ^*(\mathbb{H} \Rightarrow P(\mathbf{X},V).G(\mathbf{X},V) > 0)^*$$

de degrés majorés par δ_1. On obtient donc l'implication forte:

$$^*(\mathbb{H} \Rightarrow [G(\mathbf{X},U).G(\mathbf{X},V) > 0, P(\mathbf{X},U).G(\mathbf{X},U) > 0, P(\mathbf{X},V).G(\mathbf{X},V) > 0])^* \qquad (1)$$

acceptant pour fonction Δ : $d' \to \Delta_{14,a}(d';[\Delta_{21}(\delta_1;\delta_1,s)),\delta_1,\delta_1])$.

En combinant l'implication triviale $[A.C > 0, B.D > 0] \Rightarrow A.B.C.D > 0$ avec l'implication : $[A.B.C.D > 0, A.B > 0] \Rightarrow C.D > 0$ (cf.14.4.c) on obtient une implication forte :

$$^*([A.B > 0, A.C > 0, B.D > 0] \Rightarrow C.D > 0)^* \qquad (2)$$

Avec pour A, B, C, D : $G(\mathbf{X},U)$, $G(\mathbf{X},V)$, $P(\mathbf{X},U)$, $P(\mathbf{X},V)$, une fonction Δ acceptable est : $d' \to \sup(d'.\delta_1/\delta , d'+2(\delta_1-\delta))$ (majoration 14,4,b)

Il reste à combiner par transitivité (1) et (2) pour obtenir :

$$^{*}\big(\ \mathbb{H} \Rightarrow P(\mathbf{X},U).P(\mathbf{X},V) > 0\ \big)^{*}$$

avec pour fonction Δ : $\Delta_{14,a}(\ \sup(d'.\delta_1/\delta, d'+2(\delta_1-\delta))\ ;\ [\Delta_{21}(\delta_1;\delta_1,s)),\delta_1,\delta_1]\ )$, et donc de degré majoré par : $\Delta_{14,a}(4\delta_1;[\Delta_{21}(\delta_1;\delta_1,s)),\delta_1,\delta_1])$ (partie réciproque dans la proposition 14 : remplacer d' par 4δ).

En définitive, nous avons obtenu, pour P unitaire de degré s+2 en Z, l'existence potentielle:

$$^{*}\big(\ P(U).P(V) \le 0\ \Rightarrow\ \exists\ Z\ \ P(Z) = 0\big)^{*}$$

avec pour fonction Δ : $\Delta_{21,u}(d;\delta,s+2) = \Delta_{14,a}(\ 4\delta_1\ ;\ [\Delta_{21}(\delta_1;\delta_1,s),\delta_1,\delta_1]\ )$.

Nous passons maintenant au cas non unitaire, et nous raisonnons selon le signe de $C(\mathbf{X})$, coefficient dominant en Z de $P(\mathbf{X},Z)$: $P(\mathbf{X},Z) = C(\mathbf{X}).Z^{s+2} + R(\mathbf{X},Z)$

Avec $C(\mathbf{X}) = 0$:

On a l'implication simple, de degré absolu $\le 2.\delta$

$$^{*}\ [C(\mathbf{X}) = 0,\ P(U).P(V) \le 0]\ \Rightarrow\ R(U).R(V) \le 0 \qquad (3)$$

obtenue en écrivant $R(U).R(V) \equiv P(U).P(V)\ (\mathrm{mod}\ C(\mathbf{X}))$. avec donc pour fonction Δ la fonction $d \to d + 2\delta$.

Par ailleurs on a l'existence potentielle (hypothèse de récurrence) :

$$^{*}\big(\ R(U).R(V) \le 0\ \Rightarrow\ \exists\ Z\ \ R(Z) = 0\big)^{*} \qquad (4)$$

qui admet pour fonction Δ : $\Delta_{21}(d;\delta,s+1)$.

Enfin on a l'implication simple qui ne coûte rien :

$$[C(\mathbf{X}) = 0,\ R(Z) = 0]\ \Rightarrow\ P(Z) = 0 \qquad (5)$$

Par transitivité de ces trois existences potentielles, on obtient :

$$^{*}\big(\ [C(\mathbf{X}) = 0,\ P(U).P(V) \le 0]\ \Rightarrow\ \exists\ Z\ \ P(Z) = 0\big)^{*} \qquad (6)$$

avec pour fonction Δ : $\Delta_{21,a}(d;\delta,s+2) = \Delta_{21}(d;\delta,s+1) + 2\delta$

Avec $C(\mathbf{X}) \neq 0$: on pose $P_1(\mathbf{X},T,Z) = T.R(\mathbf{X},Z) + Z^{s+2}$.

On a tout d'abord l'existence potentielle

$$^{*}\big(\ C(\mathbf{X}) \neq 0\ \Rightarrow\ \exists\ T\ \ 1 = C(\mathbf{X}).T\ \big)^{*}$$

avec pour fonction Δ : $\Delta_{20}(d;\delta)$

Par renforcement simultané de l'hypothèse et de la conclusion, on obtient l'existence potentielle ;

$$^{*}\big(\ [\ C(\mathbf{X}) \neq 0\ ,\ P(U).P(V) \le 0]\ \Rightarrow\ \exists\ T\ \ [1 = C(\mathbf{X}).T,\ P(U).P(V) \le 0]\ \big)^{*} \qquad (7)$$

avec la même fonction Δ : $\Delta_{20}(d;\delta)$

On a l'implication simple, de degré absolu $\le 2.(\delta - s - 2)$

$$[1 = C(\mathbf{X}).T,\ P(U).P(V) \le 0]\ \Rightarrow\ P_1(U).P_1(V) \le 0 \qquad (8)$$

obtenue en écrivant : $P_1(U).P_1(V) \equiv P(U).P(V)\ \ (\mathrm{mod}\ 1 - C(\mathbf{X}).T)$.

Par ailleurs l'existence potentielle (cas unitaire) :

$$^{*}\big(\ P_1(U).P_1(V) \le 0\ \Rightarrow\ \exists\ Z\ \ P_1(Z) = 0\big)^{*} \qquad (9)$$

a pour fonction Δ : $\Delta_{21,u}(d;\delta,s+2)$.

En combinant (8) et (9) on obtient une existence potentielle avec pour fonction Δ : $\Delta_{21,u}(d;\delta,s+2)+2(\delta - s - 2)$.

Et on peut rappeler l'hypothèse $1 = C(\mathbf{X}).T$ dans la conclusion :

$$^{*}\big(\ [1 = C(\mathbf{X}).T,\ P(U).P(V) \le 0] \Rightarrow\ \exists\ Z\ \ [1 = C(\mathbf{X}).T,\ P_1(Z) = 0]\ \big)^{*} \qquad (10)$$

(même fonction Δ)

Enfin on a l'implication simple qui ne coûte rien :

$$^{*}\big(\ [1 = C(\mathbf{X}).T,\ P_1(Z) = 0]\ \Rightarrow\ P(Z) = 0\big)^{*} \qquad (11)$$

Par transitivité des existences potentielles (7), (10) et (11), on obtient :

$$^{*}\big(\ [C(\mathbf{X}) \neq 0,\ P(U).P(V) \le 0]\ \Rightarrow\ \exists\ Z\ \ P(Z) = 0\big)^{*} \qquad (12)$$

avec pour fonction Δ :

$$\Delta_{21,b}(d;\delta,s+2) = \Delta_{20}(\Delta_{21,u}(d;\delta,s+2) + 2(\delta - s - 2)) ; \delta)$$

Il ne reste plus qu'à regrouper les deux cas $C(\mathbf{X}) = 0$ (6) et $C(\mathbf{X}) \neq 0$ (12) au moyen de la majoration 15,c) pour obtenir la majoration finale :

$$\Delta_{21}(d;\delta,s+2) = \delta_{6,c}(\Delta_{21,a}(d;\delta,s+2) , \Delta_{21,b}(d;\delta,s+2))$$

Voyons pour terminer le cas $n = 0$. Les initialisations sont faciles. La récurrence s'obtient par relecture du cas général. Le calcul est simplifié parce qu'il n'y a pas à raisonner selon le signe ($= 0$ ou $\neq 0$) du coefficient dominant de P et l'inverse du coefficient dominant est dans $\mathbf{K}$ donc ne nécessite pas d'existence potentielle. En particulier, contrairement au cas général, la récurrence n'introduit pas de nouvelle variable. ❑

Théorème et majorations 22 : (autorisation de rajouter une racine sur l'intervalle où le signe change) Hypothèses et notations comme au théorème 21.

On a l'existence potentielle :

$$^*([P(U).P(V) < 0] \Rightarrow \exists Z [P(Z) = 0, P(U).P(V) < 0 , (Z - U).(Z - V) < 0])^*$$

et une fonction Δ acceptable, notée $\Delta_{22,a}(d;\delta,s)$, peut être calculée au moyen des formules récurrentes suivantes:

$$\Delta_{22,a}(d;\delta,0) = 2.\delta , \ \Delta_{22,a}(d;\delta,1) = \Delta_{21}((d+4).\delta ; \delta , 1)$$

$$\Delta_{22,a}(d;\delta,s+1) = \Delta_{21}(\delta_{6,a}(d.\delta , (\Delta_{22,a}(d;\delta–1,s)+4) . \delta) ; \delta , s+1).$$

On a également les existences potentielles :

$$^*([P(U) < 0 < P(V), U < V] \Rightarrow \exists Z [P(Z) = 0, P(U) < 0 < P(V), U < Z < V])^*$$

$$^*([P(U) > 0 > P(V), U < V] \Rightarrow \exists Z [P(Z) = 0, P(U) > 0 > P(V), U < Z < V])^*$$

Et une fonction Δ acceptable est donnée par :

$$\Delta_{22}(d;\delta,s) = \Delta_{22,a}(2.d+2 ; \delta , s).$$

preuve> Voyons tout d'abord la première existence potentielle, qui se démontre par récurrence sur s.

Si $s = 0$ on a l'implication forte $^*([P(U).P(V) < 0] \Rightarrow 1 = 0)^*$ de degré $2.\delta$ ce qui montre que $\Delta_{22,a}(d;\delta,0) = 2.\delta$.

Avec $s+1$: tout d'abord, le théorème 21, avec renforcement de l'hypothèse puis rappel de l'hypothèse dans la conclusion fournit l'existence potentielle :

$$^*(P(U).P(V) < 0 \Rightarrow \exists Z [P(U).P(V) < 0 , P(Z) = 0])^* \qquad (1)$$

avec pour fonction Δ : $\Delta_{21}(d ; \delta , s+1)$.

Si $s+1 = 1$, notons A le coefficient de Z dans $P(Z)$, l'implication forte :

$$^*([P(Z) = 0, P(U).P(V) < 0] \Rightarrow [P(Z) = 0, P(U).P(V) < 0 , (Z - U).(Z - V) < 0])^*$$

obtenue en écrivant : $A^2.(Z - U).(Z - V) \equiv P(U).P(V) \mod P(Z)$, accepte pour fonction Δ : $d \rightarrow d\delta+4\delta$ (comme 14.4.d).

Supposons $s \geq 1$. Nous démontrons maintenant l'existence potentielle :

$$^*([P(U).P(V) < 0, P(Z) = 0] \Rightarrow \exists Z' [P(Z') = 0, P(U).P(V) < 0, (Z' - U).(Z' - V) < 0])^*$$

cas par cas, selon le signe de $(Z - U).(Z - V)$.

Si $(Z - U).(Z - V) \leq 0$.

L'implication : $[P(U).P(V) \neq 0, \ P(Z) = 0] \Rightarrow (Z - U).(Z - V) \neq 0$ admet pour fonction $\Delta : d \rightarrow d.\delta$. (petit calcul sans difficulté)

Et l'implication $[(Z - U).(Z - V) \leq 0, \ (Z - U).(Z - V) \neq 0] \Rightarrow (Z - U).(Z - V) < 0$ est triviale. Donc l'implication :

$$[P(U).P(V) < 0, \ P(Z) = 0, \ (Z - U).(Z - V) \leq 0] \Rightarrow (Z - U).(Z - V) < 0$$

admet pour fonction $\Delta : d \rightarrow d.\delta$.

Si $(Z - U).(Z - V) \geq 0$.

On considère une nouvelle variable T et le polynôme R défini par :

$$R(\mathbf{X},Z,T) := \big(P(\mathbf{X},T) - P(\mathbf{X},Z)\big) / (T - Z)$$

qui est de degré total $\leq \delta-1$, et de degré $\leq s$ en T.

Notons pour alléger R(T) pour $R(\mathbf{X},Z,T)$ et P(T) pour $P(\mathbf{X},T)$.

Notons $\mathbb{H}_1(\mathbf{X},Z)$ pour [$P(U).P(V) < 0$, $P(Z) = 0$, $(Z - U).(Z - V) \geq 0$] .

(c'est l'hypothèse de l'existence potentielle que nous voulons démontrer)

On a une implication forte :

$$^*\big(\mathbb{H}_1(\mathbf{X},Z) \Rightarrow R(U).R(V) < 0 \big)^* \qquad (2)$$

obtenue en écrivant : $\big(R(U).R(V)\big).\big((Z - U).(Z - V)\big) \equiv P(U).P(V) \pmod{P(Z)}$

ce qui fournit la fonction $\Delta : d \to (d+4).\delta$ (comme 14.4.d)

Comme R(T) est de degré $\leq s$ en T on applique l'hypothèse de récurrence. On obtient :

$$^*\big(R(U).R(V) < 0 \Rightarrow \exists\ Z'\ [R(Z') = 0, R(U).R(V) < 0, (Z' - U).(Z' - V) < 0] \big)^* \qquad (3)$$

avec pour fonction $\Delta : \Delta_{22,a}(d;\delta-1,s)$.

En combinant (2) et (3) et en rappelant une hypothèse dans la conclusion, on obtient :

$$^*\big(\mathbb{H}_1(\mathbf{X},Z) \Rightarrow \exists\ Z'\ [R(Z') = 0, P(Z) = 0, (Z' - U).(Z' - V) < 0] \big)^* \qquad (4)$$

avec pour fonction $\Delta : (\Delta_{22,a}(d;\delta-1,s)+4) . \delta$.

L'implication

$$^*\big([R(Z') = 0, P(Z) = 0, (Z' - U).(Z' - V) < 0] \Rightarrow [P(Z') = 0, (Z' - U).(Z' - V) < 0]\big)^* \qquad (5)$$

est une implication simple qui ne coûte rien.

En combinant (4) et (5) on obtient :

$$^*\big(\mathbb{H}_1(\mathbf{X},Z) \Rightarrow \exists\ Z'\ [P(Z') = 0,\ (Z' - U).(Z' - V) < 0]\big)^*$$

avec pour fonction $\Delta : (\Delta_{22,a}(d;\delta-1,s)+4) . \delta$.

En regroupant les deux cas $(Z - U).(Z - V) \leq 0$ et $(Z - U).(Z - V) \geq 0$ on obtient :

$$^*\big([P(U).P(V) < 0, P(Z) = 0] \Rightarrow \exists\ Z'[P(Z') = 0, P(U).P(V) < 0, (Z' - U).(Z' - V) < 0]\big)^*$$

avec pour fonction Δ :

$$\Delta_{22,b}(d;\delta,s) = \delta_{6,a}(d.\delta , (\Delta_{22,a}(d;\delta-1,s)+4) . \delta).$$

Enfin en combinant le dernier résultat avec (1) :

$$^*\big(P(U).P(V) < 0 \Rightarrow \exists\ Z' [P(Z') = 0, P(U).P(V) < 0, (Z' - U).(Z' - V) < 0]\big)^* \qquad (6)$$

avec pour fonction $\Delta : \Delta_{21}(\Delta_{22,b}(d;\delta,s) ; \delta , s+1)$. Ceci fournit la relation récurrente cherchée.

Il nous reste à calculer Δ_{22} .

D'après la proposition 14.4.e (en prenant pour A et B : $(Z - U)$ et $(V - Z)$)

$$[P(Z) = 0, P(U).P(V) < 0 , (Z - U).(Z - V) < 0, U < V] \Rightarrow [P(Z) = 0, P(U).P(V) < 0 , U < Z < V]$$

accepte pour fonction $\Delta : d \to 2.d+2$.

Par ailleurs, on a l'implication triviale : $P(U) < 0 < P(V) \Rightarrow P(U).P(V) < 0$

D'où, par transitivité avec (6) : $\Delta_{22}(d;\delta,s) = \Delta_{22,a}(2.d+2 ; \delta , s)$. ❑

Tableaux de Hörmander et C^ie

Proposition et majorations 23 : (Tableau et algorithme de Hörmander)

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**[Y].

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

1) P est finie.

2) On peut établir le tableau complet des signes pour P en utilisant les seules informations suivantes : le degré de chaque polynôme de la famille; les diagrammes des opérations $P \to P'$, et $(P,Q) \to Rst(P,Q)$ (où $deg(P) \geq deg(Q)$) dans P ; et les signes des constantes de P.

Si s majore les degrés des P_i, le nombre de coefficients d'éléments de P, et donc aussi le nombre de points du tableau de Hörmander est majoré par : $\Lambda_{23}(s,k) = (k+1)^{2^s}$

preuve> D'après la preuve le la proposition 23, pour obtenir P, il suffit de répéter s fois les deux opérations "dérivation" et "reste". Un calcul précis ne donnerait guère mieux que la majoration $\Lambda_{27}(s,k)$ qui sera obtenue plus loin, et à laquelle nous renvoyons. ❑

Pseudo-restes : Dans un tableau de Hörmander paramétré, on a intérêt à remplacer les restes par des psudo-restes. Rappelons que le pseudo-reste de $P(\mathbf{X},Y)$ par $Q(\mathbf{X},Y)$, de degrés respectifs en Y égaux à p et $q \leq p$ est défini comme égal au déterminant polynomial de la matrice ayant pour lignes les polynômes :

$Q, Q.Y, ..., Q.Y^{p-q}, P$ écrits sur la base $Y^p, ..., Y, 1$ (on est dans $\mathbf{K}[\mathbf{X}][Y]$).

On a alors une égalité : $S(\mathbf{X})^{p-q+1}.P(\mathbf{X},Y) = Q(\mathbf{X},Y).T(\mathbf{X},Y) + R(\mathbf{X},Y)$ où $S(\mathbf{X})$ est le coefficient dominant de Q. Nous appellerons *degré de la pseudo-division de* P *par* Q le plus grand des degrés totaux des trois polynômes $S(\mathbf{X})^{p-q+1}.P(\mathbf{X},Y)$, $Q(\mathbf{X},Y).T(\mathbf{X},Y)$ et $R(\mathbf{X},Y)$. (il suffit de prendre le plus grand de deux d'entre eux)

Lemme et majorations 26, avec paramètres : (évidence forte et existence potentielle pour les faits élémentaires lisibles sur un tableau de Hörmander paramétré)

Soit $\mathbf{K}$ un corps ordonné. Soit P une famille de polynômes de $\mathbf{K}[X_1,X_2,...,X_n][Y]$ stable par les opérations "pseudo-reste" et "dérivation", modulo un système de conditions de signes $\mathbb{H}_\Sigma(X_1,X_2,...,X_n)$, système qui fixe également la forme précise du tableau de Hörmander de la famille P (les polynômes figurant dans $\mathbb{H}_\Sigma$ sont d'une part les polynômes constants, c.-à-d. sans Y, de la famille P, d'autre part les polynômes dont l'annulation garantit le degré d'un pseudo-reste).

1) les points du tableau de Hörmander, définis à la Thom par leur construction même, vérifient l'existence potentielle pour leur codage à la Thom, sous l'hypothèse $\mathbb{H}_\Sigma$.
2) la comparaison (pour l'ordre) de 2 points consécutifs du tableau est fortement évidente à partir de $\mathbb{H}_\Sigma$ et 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 de $\mathbb{H}_\Sigma$ et du codage à la Thom du point considéré.
4) sur chaque intervalle ouvert minimal du tableau les signes de tous les polynômes de la famille sont fortement évidents à partir de $\mathbb{H}_\Sigma$, du codage à la Thom des extrémités de l'intervalle (si l'intervalle est non borné, seule l'extrémité finie intervient) et du fait que le point est situé entre les extrémités.

Soient, pour la famille P, m le nombre de polynômes non constants (en Y), m_1 le nombre de polynômes de degré 1 (en Y), δ une majoration des degrés (totaux) des éléments de P et des degrés des pseudo-divisions, et s une majoration des degrés en Y, soit enfin h le nombre de points du tableau de Hörmander. Les fonctions Δ correspondant aux points 1 , 2 , 3 , 4 du lemme sont données par les formules récurrentes suivantes :

Initialisations :

$\Delta_{26,1}(d;\delta,s,m_1) = \Delta_{21}(\Delta_{21}(d ; \delta , 1) ; \delta , 1)$

$\delta_{26,2}(\delta,s,m_1) = \delta_{26,3}(\delta,s,m_1) = \delta_{26,4}(\delta,s,m_1) = 4\delta$

$\Delta_{26,2}(d;\delta,s,m_1) = \Delta_{26,3}(d;\delta,s,m_1) = \Delta_{26,4}(d;\delta,s,m_1) = \Delta_{26,4,a}(d;\delta,s,m_1) = \delta_6(d; 4\delta)$;

Récurrences : $m \geq m_1$

$\Delta_{26,1,a}(d;\delta,s,m) = \Delta_{26,3}(\delta_6(d , 2.\delta) ; \delta,s,m)$

$\Delta_{26,1,b}(d;\delta,s,m) = \Delta_{26,1,a}(\Delta_{26,1,a}(\Delta_{26,2}(d;\delta,s,m) ;\delta,s,m) ;\delta,s,m)$

$\Delta_{26,1,b'}(d;\delta,s,m) = \Delta_{26,1,a}(\Delta_{10}(d;\delta) ; \delta,s,m)$

$\Delta_{26,1,c}(d;\delta,s,m) = \Delta_{26,1}(\Delta_{26,1,b}(\Delta_{22}(\Delta_{26,4}(d;\delta,s,m) ; \delta,s) ; \delta,s,m) ; \delta,s,m)$

$\Delta_{26,1,c'}(d;\delta,s,m) = \Delta_{26,1}(\Delta_{20,a}(\Delta_{26,1,b'}(\Delta_{22}(\Delta_{26,4,a}(d;\delta,s,m);\delta,s);\delta,s,m);\delta,s);\delta,s,m)$

$\Delta_{26,1}(d;\delta,s,m+1) = \sup(\Delta_{26,1,c}(d;\delta,s,m) , \Delta_{26,1,c'}(d;\delta,s,m))$

$\Delta_{26,2}(d;\delta,s,m+1) = \Delta_{10}(\Delta_{26,1,a}(\Delta_{26,3}(d;\delta,s,m) ; \delta,s,m) ; \delta)$

$\Delta_{26,3,a}(d;\delta,s,m+1) = \Delta_{26,1,a}(\Delta_{26,3}(d ; \delta,s,m) ; \delta,s,m)$

$\Delta_{26,3,a'}(d;\delta,s,m+1) = \Delta_{26,1}(\Delta_{26,2}(\Delta_{26,2}(\Delta_{26,4}(d;\delta,s,m) ; \delta,s,m+1); \delta,s,m+1); \delta,s,m)$

$\Delta_{26,3}(d;\delta,s,m+1) = \sup(\Delta_{26,3,a}(d;\delta,s,m+1) , \Delta_{26,3,a'}(d;\delta,s,m+1))$

$\Delta_{26,4,a}(d;\delta,s,m+1) = \Delta_{26,3}(d;\delta,s,m+1)$

$\Delta_{26,4}(d;\delta,s,m+1) = \Delta_{26,3}(\Delta_{26,3}(d;\delta,s,m+1) ; \delta,s,m+1)$

Quelques résultats supplémentaires:

$\delta_{26,2}(\delta,s,m) = \Delta_{26,2}(2\delta;\delta,s,m)$

$\delta_{26,3}(\delta,s,m) = \Delta_{26,3}(2\delta;\delta,s,m)$

$\delta_{26,4}(\delta,s,m) = \Delta_{26,4}(2\delta;\delta,s,m)$

Enfin, l'existence potentielle simultanée de tous les points du tableau de Hörmander, pour leur codage à la Thom, sous l'hypothèse $\mathbb{H}_\Sigma$, accepte pour fonction Δ :

$\Delta_{26}(d;\delta,s,m,h)$ = itérée h fois de la fonction $d \rightarrow \Delta_{26,1}(d;\delta,s,m)$

preuve du lemme>

Précisons tout d'abord la signification exacte des fonctions : $\Delta_{26,1}$, $\Delta_{26,2}$, $\Delta_{26,3}$, $\Delta_{26,4}$, $\Delta_{26,4,a}$.

– La fonction $\Delta_{26,1}(d;\delta,s,m)$ est une fonction Δ pour toute existence potentielle :

$$^*(\mathbb{H}_\Sigma \Rightarrow \exists\, \alpha,\beta \ [\mathbb{H}_\alpha(\alpha) , \mathbb{H}_\beta(\beta)])^*$$

où α et β sont 2 points consécutifs d'un tableau T_m.

– La fonction $\Delta_{26,2}(d;\delta,s,m)$ est une fonction Δ acceptable pour l'implication forte :

$$^*([\mathbb{H}_\Sigma, \ \mathbb{H}_\alpha(\alpha), \ \mathbb{H}_\beta(\beta)] \Rightarrow \ \alpha < \beta \ )^*$$

où α et β sont 2 points consécutifs d'un tableau T_m.

– La fonction $\Delta_{26,3}(d;\delta,s,m)$ est une fonction Δ acceptable pour l'implication forte :

$$^*([\mathbb{H}_\Sigma, \ \mathbb{H}_\alpha(\alpha)] \Rightarrow P^{(i)}(\alpha) \ \tau_i \ 0)^* \ (i = 0, 1, ..., \deg(P) - 1)$$

où α est un point d'un tableau T_m, et P un polynôme de numéro $\leq m$.

– La fonction $\Delta_{26,4}(d;\delta,s,m)$ est une fonction Δ acceptable pour l'implication forte :

$$^*([\mathbb{H}_\Sigma, \ \mathbb{H}_\alpha(\alpha), \ \mathbb{H}_\beta(\beta), \alpha < Z < \beta] \Rightarrow [\ P^{(i)}(Z) \ \tau_i \ 0 \quad (i = 0, 1, ..., \deg(P) - 1) \ ])^*$$

où α et β sont 2 points consécutifs d'un tableau T_m, et P un polynôme de numéro $\leq m$.

La fonction $\Delta_{26,4,a}(d;\delta,s,m)$ est la fonction Δ analogue lorsqu'il s'agit d'un Z au delà d'une extrémité du tableau.

Remarque : dans les trois derniers cas, on peut récupérer une majoration des degrés des implications fortes considérées en appliquant la réciproque dans la proposition 14 :

$\delta_{26,i}(\delta,s,m) = \Delta_{26,i}(2\delta;\delta,s,m)$: i = 2, 3, 4.

Pour l'initialisation, on considère uniquement les polynômes de degré 1, et on n'a pas besoin de récurrence.
Une existence potentielle $^*(\mathbb{H}_\Sigma \Rightarrow \exists\, \alpha \;\; \mathbb{H}_\alpha(\alpha)])^*$
se réduit à : $^*(\mathbb{H}_\Sigma \Rightarrow \exists\, \alpha \;\; P(\alpha) = 0])^*$ (avec P de degré 1)
qui admet pour fonction Δ : $\Delta_{21}(d;\delta,1)$. Et donc par transitivité :

$$^*(\mathbb{H}_\Sigma \Rightarrow \exists\, \alpha,\beta \;\; [\mathbb{H}_\alpha(\alpha) , \mathbb{H}_\beta(\beta)])^*$$

avec pour fonction Δ : $\Delta_{21}(\Delta_{21}(d;\delta,1);\delta,1)$.
Les majorations de degrés $\delta_{26,2}(\delta,s,m_1) = \delta_{26,3}(\delta,s,m_1) = \delta_{26,4}(\delta,s,m_1) = 4\delta$ sont faciles. A partir de là on obtient les fonctions Δ par la proposition 14. (on note que dans le cas 26.4, une seule des deux inégalités est utilisée).

La récurrence :
On introduit ensuite les polynômes de degré ≥ 1 de P un à un, par degrés croissants. Une étape de la récurrence consiste donc à introduire les racines (non déjà présentes) d'un polynôme P. On fait donc une preuve par récurrence sur m. Nous supposons donc que P a le numéro m+1 parmi les polynômes non constants rangés en ordre de degrés croissants. Nous posons p = deg(P). On a alors $m \geq m_1$ et $2 \leq p \leq s$.

Nous commençons par calculer une majoration de degré pour l'implication forte donnant le signe de P *en un point de* T_m. C'est un point λ codé à la Thom par $\mathbb{H}_\lambda(\lambda)$ à partir d'un polynôme $Q_\lambda(\mathbf{X},Y)$ de coefficient dominant $S(\mathbf{X})$. On a donc la condition de signe $S(\mathbf{X})\ \sigma\ 0$ dans $\mathbb{H}_\Sigma(\mathbf{X})$, et la condition $Q_\lambda(\mathbf{X},\lambda) = 0$ dans $\mathbb{H}_\lambda(\lambda)$. Soit R le pseudo-reste de la pseudo-division de P par Q_λ.
Par hypothèse de récurrence (3), on a une implication forte

$$^*([\mathbb{H}_\Sigma , \mathbb{H}_\lambda(\lambda)] \Rightarrow R(\mathbf{X},\lambda)\ \tau\ 0)^* \text{ avec la fonction } \Delta : \Delta_{26,3}(d;\delta,s,m)$$

On a une égalité :

$$S(\mathbf{X})^i.P(\mathbf{X},Y) = Q_\lambda(\mathbf{X},Y).T(\mathbf{X},Y) + R(\mathbf{X},Y) \text{ avec les degrés} \leq \delta$$

Ceci donne lieu, après multiplication par $R(\mathbf{X},Y)$ ou après élévation au carré, à une implication forte sous forme normale, assurant le signe de $P(\mathbf{X},\lambda)$, et de degré majoré par $2.\delta$:

$$^*([R(\mathbf{X},\lambda)\ \tau\ 0 , Q_\lambda(\mathbf{X},\lambda) = 0 , S(\mathbf{X})\ \sigma\ 0] \Rightarrow P(\mathbf{X},\lambda)\ \tau'\ 0)^*$$

D'où par transitivité :

$$^*([\mathbb{H}_\Sigma , \mathbb{H}_\lambda(\lambda)] \Rightarrow P(\mathbf{X},\lambda)\ \tau'\ 0)^*$$

acceptant pour fonction Δ : $\Delta_{26,1,a}(d;\delta,s,m) = \Delta_{26,3}(\delta_6(d , 2.\delta) ; \delta,s,m)$.

Nous passons au point 1 du lemme .
Soit ζ une racine de P située sur l'intervalle ouvert minimal $]\alpha,\beta[$ de T_m. On a donc :
$^*([\mathbb{H}_\Sigma , \mathbb{H}_\alpha(\alpha)] \Rightarrow P(\alpha) > 0)^*$ et $^*([\mathbb{H}_\Sigma , \mathbb{H}_\beta(\beta)] \Rightarrow P(\beta) < 0)^*$ ou vice-versa,
avec la fonction Δ : $\Delta_{26,1,a}(d;\delta,s,m)$
Et l'hypothèse de récurrence (2) donne :

$$^*([\mathbb{H}_\Sigma , \mathbb{H}_\alpha(\alpha) , \mathbb{H}_\beta(\beta)] \Rightarrow \alpha < \beta)^* \text{ avec la fonction } \Delta : \Delta_{26,2}(d;\delta,s,m)$$

On a donc :

$$^*([\mathbb{H}_\Sigma , \mathbb{H}_\alpha(\alpha) , \mathbb{H}_\beta(\beta)] \Rightarrow [P(\alpha) > 0 , P(\beta) < 0 , \alpha < \beta])^* \qquad \text{(i)}$$

avec la fonction Δ : $\Delta_{26,1,b}(d;\delta,s,m) = \Delta_{26,1,a}(\Delta_{26,1,a}(\Delta_{26,2}(d;\delta,s,m) ;\delta,s,m) ;\delta,s,m)$
Le théorème 22 donne :

$$^*([P(\alpha) > 0 , P(\beta) < 0 , \alpha < \beta] \Rightarrow \exists\, Z\ [\alpha < Z < \beta, P(Z) = 0])^*$$

avec pour fonction Δ : $\Delta_{22}(d;\delta,s)$. Et par transitivité on obtient :

$$^*([\mathbb{H}_\Sigma , \mathbb{H}_\alpha(\alpha) , \mathbb{H}_\beta(\beta)] \Rightarrow \exists\, Z\ [\alpha < Z < \beta, P(Z) = 0])^* \qquad \text{(ii)}$$

avec pour fonction Δ : $\Delta_{26,1,b}(\Delta_{22}(d;\delta,s) ; \delta,s,m)$
Par ailleurs, par hypothèse de récurrence 4, il y a des $\tau_i \in \{ <, > \}$ (i = 1, ..., p) tels que :

$^*([\ \mathbb{H}_\Sigma,\ \mathbb{H}_\alpha(\alpha),\ \mathbb{H}_\beta(\beta),\ \alpha < Z < \beta\ ] \Rightarrow [\ P^{(i)}(Z)\ \tau_i\ 0\ \ (i = 1, ..., p-1)\ ])^*$ (iii)

avec pour fonction Δ : $\Delta_{26,4}(d;\delta,s,m)$.

Notons aussi que $P^{(p)}(Z)\ \tau_p\ 0$ est dans $\mathbb{H}_\Sigma$.

Enfin, on a, par hypothèse de récurrence (1) :

$$^*(\mathbb{H}_\Sigma \Rightarrow \exists\ \alpha,\beta\ [\ \mathbb{H}_\alpha(\alpha)\ ,\ \mathbb{H}_\beta(\beta)\ ]\ )^* \qquad \text{(iv)}$$

acceptant pour fonction Δ : $\Delta_{26,1}(d;\delta,s,m)$.

Enfin par transitivité (iv), (ii) et (iii) donnent :

$$^*(\mathbb{H}_\Sigma \Rightarrow \exists\ Z,\alpha,\beta\ [\ \mathbb{H}_\zeta(Z)\ ,\ \mathbb{H}_\alpha(\alpha)\ ,\ \mathbb{H}_\beta(\beta)\ ]\ )^* \qquad \text{(v)}$$

acceptant pour fonction Δ :

$\Delta_{26,1,c}(d;\delta,s,m) = \Delta_{26,1}(\ \Delta_{26,1,b}(\ \Delta_{22}(\ \Delta_{26,4}(d;\delta,s,m)\ ;\ \delta,s\ )\ ;\ \delta,s,m\ )\ ;\ \delta,s,m\ )$.

Voyons ce que nous modifions à l'argument précédent lorsqu'on rajoute une racine de P sur un intervalle extrémal, par exemple $]\alpha,\infty[$, en supposant par exemple que $P(\alpha) > 0$ et que le coefficient dominant de P, soit $C(\mathbf{X})$, est affirmé < 0 dans $\mathbb{H}_\Sigma$. La notation $\mathbb{H}_\beta(\beta)$ signifie maintenant $[\ P(\mathbf{X},\beta) < 0;\ P^{(i)}(\mathbf{X},\beta) < 0\ ,\ i = 1, ..., s\ ]$. L'existence potentielle d'un tel β est assurée par le corollaire 20bis (majoration 20,c).

La ligne (iv) accepte donc maintenant pour fonction Δ : $\Delta_{26,1}(\ \Delta_{20,a}(d;\delta,s)\ ;\ \delta,s,m\ )$.

La ligne (i) peut maintenant être obtenue à partir de :

$$^*([\ \mathbb{H}_\Sigma\ ,\ \mathbb{H}_\alpha(\alpha)\ ]\ \Rightarrow\ P(\alpha) > 0\ )^*$$

et de $^*([\ P(\alpha) > 0\ ,\ \mathbb{H}_\beta(\beta)\ ]\ \Rightarrow\ \beta > \alpha\ )^*$ (théorème 10 (2,d)

La ligne (i) accepte donc maintenant pour fonction Δ :

$\Delta_{26,1,b'}(d;\delta,s,m) = \Delta_{26,1,a}(\ \Delta_{10}(d;\delta)\ ;\ \delta,s,m)$

Ce qui donne pour la ligne (ii) la fonction Δ : $\Delta_{26,1,b'}(\Delta_{22}(d;\delta,s);\delta,s,m)$

Enfin, la fonction Δ pour la ligne (iii) est maintenant : $\Delta_{26,4,a}(d;\delta,s,m)$.

Finalement la ligne (v) accepte maintenant pour fonction Δ :

$\Delta_{26,1,c'}(d;\delta,s,m) = \Delta_{26,1}(\Delta_{20,a}(\Delta_{26,1,b'}(\Delta_{22}(\Delta_{26,4,a}(d;\delta,s,m)\ ;\ \delta,s\ );\delta,s,m);\delta,s);\delta,s,m\ )$

Nous concluons $\Delta_{26,1}(d;\delta,s,m+1) = \sup(\ \Delta_{26,1,c}(d;\delta,s,m)\ ,\ \Delta_{26,1,c'}(d;\delta,s,m)\ )$.

Voyons le point 2 du lemme :

Il nous suffit de calculer une majoration pour un nouveau couple tel que (α,ζ).

Appelons τ'_i le signe $\leq$ ou $\geq$ associé à τ_i. Supposons par exemple que τ_1 est $<$.

On a les implications fortes :

$$^*([\ \mathbb{H}_\Sigma,\ \mathbb{H}_\alpha(\alpha)\ ] \Rightarrow P(\alpha) > 0\ )^* \text{ et}$$

$$^*([\ \mathbb{H}_\Sigma,\ \mathbb{H}_\alpha(\alpha)\ ]\ \Rightarrow [P^{(i)}(\alpha)\ \tau'_i\ 0\ ,\ (i = 1, ..., p-1)\ ]\ )^*$$

avec les fonctions Δ : $\Delta_{26,1,a}(d;\delta,s,m)$ et $\Delta_{26,3}(d;\delta,s,m)$.

Par ailleurs $P^{(s)}(\alpha)\ \tau_s\ 0$ est dans $\mathbb{H}_\Sigma$.

Donc via le théorème 10 (2,b) : $^*([\ \mathbb{H}_\Sigma,\ \mathbb{H}_\alpha(\alpha),\ \mathbb{H}_\zeta(\zeta)\ ] \Rightarrow \alpha < \zeta\ )^*$

avec pour fonction Δ : $\Delta_{26,2}(d;\delta,s,m+1) = \Delta_{10}(\ \Delta_{26,1,a}(\ \Delta_{26,3}(d;\delta,s,m)\ ;\ \delta,s,m\ )\ ;\ \delta\ )$

Voyons le point 3 du lemme :

Nous avons déjà la fonction Δ : $\Delta_{26,1,a}(d;\delta,s,m)$ pour une évidence forte assurant le signe de P en un point quelconque α de T_m. En combinant avec l'évidence forte déjà obtenue pour le signe des dérivées de P on obtient :

$$^*([\ \mathbb{H}_\Sigma,\ \mathbb{H}_\alpha(\alpha)\ ]\ \Rightarrow [P^{(i)}(\alpha)\ \tau_i\ 0\ ,\ (i = 0, 1, ..., p-1)\ ]\ )^*$$

avec pour fonction Δ : $\Delta_{26,3,a}(d;\delta,s,m+1) = \Delta_{26,1,a}(\ \Delta_{26,3}(\ d\ ;\ \delta,s,m\ )\ ;\ \delta,s,m\ )$

Il nous faut en outre la majoration de degré pour l'implication forte :

$$^*([\ \mathbb{H}_\Sigma,\ \mathbb{H}_\zeta(\zeta)\ ] \Rightarrow [Q^{(i)}(\zeta)\ \sigma_i\ 0\ ,\ (i = 0, 1, ..., \deg(Q)-1)\ ]\ )^*$$

avec Q dans P_m et ζ une racine de P rajoutée dans la tableau.

On a : $^*([\mathbb{H}_\Sigma , \mathbb{H}_\alpha(\alpha) , \mathbb{H}_\beta(\beta), \mathbb{H}_\zeta(\zeta)] \Rightarrow \alpha < \zeta < \beta)^*$
avec pour fonction Δ : $\Delta_{26,2}(\Delta_{26,2}(d ; \delta,s,m+1) ; \delta,s,m+1)$
et : $^*([\mathbb{H}_\Sigma , \mathbb{H}_\alpha(\alpha) , \mathbb{H}_\beta(\beta), \alpha < \zeta < \beta] \Rightarrow [Q^{(i)}(\zeta)\ \sigma_i\ 0 , (i = 0, 1, ..., \deg(Q) - 1)])^*$
avec pour fonction Δ : $\Delta_{26,4}(d ; \delta,s,m)$
donc : $^*([\mathbb{H}_\Sigma , \mathbb{H}_\alpha(\alpha), \mathbb{H}_\beta(\beta), \mathbb{H}_\zeta(\zeta)] \Rightarrow [Q^{(i)}(\zeta)\ \sigma_i\ 0 , (i = 0, 1, ..., \deg(Q) - 1)])^*$
avec pour fonction Δ : $\Delta_{26,2}(\Delta_{26,2}(\Delta_{26,4}(d ; \delta,s,m) ; \delta,s,m+1) ; \delta,s,m+1)$.
Comme : $^*(\mathbb{H}_\Sigma \Rightarrow \exists\ \alpha,\beta\ [\mathbb{H}_\alpha(\alpha) , \mathbb{H}_\beta(\beta)])^*$
qui accepte pour fonction Δ : $\Delta_{26,1}(d;\delta,s,m)$
on obtient : $^*([\mathbb{H}_\Sigma , \mathbb{H}_\zeta(\zeta)] \Rightarrow [Q^{(i)}(\zeta)\ \sigma_i\ 0 , (i = 0, 1, ..., \deg(Q) - 1)])^*$
avec pour fonction Δ :
$\Delta_{26,3,a'}(d;\delta,s,m+1) = \Delta_{26,1}(\Delta_{26,2}(\Delta_{26,2}(\Delta_{26,4}(d ; \delta,s,m) ; \delta,s,m+1) ; \delta,s,m+1) ; \delta,s,m)$.
Il reste à poser :

$$\Delta_{26,3}(d;\delta,s,m+1) = \sup(\Delta_{26,3,a}(d;\delta,s,m+1) , \Delta_{26,3,a'}(d;\delta,s,m+1))$$

Voyons le point 4 du lemme :
Il se déduit du point 3 en utilisant le théorème 10 (5), et cela donne la fonction Δ :

$$\Delta_{26,4}(d;\delta,s,m+1) = \Delta_{26,3}(\Delta_{26,3}(d;\delta,s,m+1) ; \delta,s,m+1)$$

Pour un point au delà d'une extrémité du tableau on utilise 10 (2,c) , et cela donne la fonction Δ :

$$\Delta_{26,4,a}(d;\delta,s,m+1) = \Delta_{26,3}(d;\delta,s,m+1).$$

Enfin la majoration concernant l'existence potentielle simultanée des points du tableau de Hörmander s'obtient par la transitivité des existences potentielles. ❑

Proposition et majorations 27 : (Tableau de Hörmander 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 $\mathbf{K}[X_1, X_2,..., X_n][Y]$.

On peut construire une famille finie F de polynômes de $\mathbf{K}[X_1, X_2,..., X_n]$ telle que, pour tous $x_1, x_2,..., x_n$ dans **R**, en posant $P_i(Y) = Q_i(x_1, x_2,..., x_n;Y)$, le tableau complet des signes pour $L = [P_1, P_2, ..., P_k]$ est calculable à partir des signes des $S(x_1, x_2,..., x_n)$ pour $S \in F$.

Supposons que la liste L possède k éléments de degré en **X** majoré par δ et de degré en Y majoré par s. Considérons la famille G , formée de tous les coefficients de tous les polynômes de tous les tableaux de Hörmander possibles, construits sur L, en remplaçant l'opération "reste" par l'opération "pseudo-reste". Une famille F convenable peut être extraite de G. Alors :

le degré de chaque polynôme de G et de chaque pseudo-division est majoré par :

$\delta_{27}(\delta,s) = \delta.(s+1)!$, sauf si $n = 0$ (donc $\delta = 0$) et alors $\delta_{27}(0,s) = s$.

le nombre d'éléments de la famille G est majoré par : $\Lambda_{27}(s,k) = (k+1)^{2^s}$

preuve>
Voyons d'abord le nombre d'éléments de G. Pour cela considérons l'ensemble des *polynômes formels*, dont les éléments sont des couples (P,p) où $P \in \mathbf{K}[X_1, X_2,..., X_n][Y]$ et p est supérieur ou égal au degré en Y de P. On dit que p est le degré formel du polynôme formel

(P,p)[1]. On a aussi la notion, claire sans plus de précision, de coefficient formellement dominant d'un polynôme formel.
Sur cet ensemble des polynômes formels sont définis les trois opérations suivantes :
– dérivation (no problem)
– troncature (on remplace p par $p-1$ et on supprime dans P le coefficient de degré p)
– pseudo-reste formel : le pseudo-reste formel de (P,p) et de (Q,q) est sans intérêt (ou encore trivial) si $P = Q$ ou si $p < q$ (on le prend alors nul), et dans le cas contraire, il est égal au déterminant polynomial de la matrice ayant pour lignes les polynômes $Q, Q.Y, ..., Q.Y^{p-q}, P$ écrits sur la base $Y^p, ..., Y, 1$ (son degré formel étant pris égal à $q-1$).
Il est alors clair que la famille G est la famille des coefficients formellement dominants de la famille obtenue à partir de la liste L en la saturant pour les trois opérations ci-dessus.
Dans la définition de cette "famille saturée" nous pouvons introduire une notion de profondeur. Un polynôme de L a la profondeur 0. Un polynôme de profondeur h donne par dérivation ou troncature un polynôme de profondeur $h+1$. Et un pseudo-reste formel non trivial de deux polynômes de profondeurs $\le h$, l'une des deux au moins étant h, est de profondeur $h+1$.
On voit qu'un polynôme de profondeur h est de degré formel $\le s-h$. D'autre part un polynôme de profondeur $\le h+1$ est ou bien un élément de L ou bien obtenu à partir d'un ou deux polynômes de profondeur $\le h$ par dérivation, troncature ou pseudo-reste formel non trivial. Si on note $\varphi(s,k,h)$ le nombre de polynômes de profondeur $\le h$, on a donc la majoration :

$$\varphi(s,k,h+1) \le k + 2.\varphi(s,k,h) + (\varphi(s,k,h)^2 - \varphi(s,k,h)) = k + \varphi(s,k,h) + \varphi(s,k,h)^2$$

Il ne reste plus qu'à vérifier par un petit calcul de récurrence sur h la majoration :

$$\varphi(s,k,h) \le (k+1)^{2^h} - 1$$

Voyons maintenant la question du degré. L'opération dérivation ne change pas les degrés des coefficients. Les coefficients du pseudo-reste de P et Q de degrés en Y s' et $s" \le s'$ sont des déterminants extraits d'une matrice à $s'-s"+2$ lignes, et dont les entrées sont des coefficients de P et Q. Dans le calcul de pseudo-restes successifs, les degrés en Y des diviseurs successifs sont strictement décroissants, et le degré en $\mathbf{X}$ est au plus multiplié par $s'-s"+2$ à chaque étape. D'où (petit calcul) la majoration $\delta_{27}(\delta,s) = \delta.(s+1)!$.❑

Remarque : Une majoration pour $\Lambda_{23}(s,k)$ peut être obtenue en répétant grosso modo le raisonnement ci-dessus, sans le mot 'formel' et en supprimant l'opération troncature, ce qui donnerait à la place φ une fonction ψ vérifiant $\psi(s,k,h+1) \le k + \psi(s,k,h)^2$

Théorème et majorations 28 : (Tableau de Hörmander paramétré, implications fortes et existences potentielles) Soit $\mathbf{K}$ un corps ordonné, sous-corps d'un corps réel clos $\mathbf{R}$.
Soit $L = [Q_1, Q_2, ..., Q_k]$ une liste de polynômes de $\mathbf{K}[X_1,X_2,...,X_n][Y]$.
On construit la famille finie F de polynômes de $\mathbf{K}[X_1,X_2,...,X_n]$ comme à la proposition 27.
Soit $\mathbb{H}(X_1,X_2,...,X_n,Y)$ un système de csg portant sur des polynômes de la liste L. Soit un élément $\Sigma = (\sigma_S)_{S \in F}$ de $\{-1, 0, +1\}^F$. On note $\mathbb{H}_\Sigma(X_1,X_2,...,X_n)$ le système de conditions de signes $[\, S(X_1,X_2,...,X_n) \equiv \sigma_S \,;\, S \in F\,]$. On suppose qu'il existe $x_1,x_2,...,x_n \in \mathbf{R}$ vérifiant $\mathbb{H}_\Sigma(x_1,x_2,...,x_n)$. Alors :
ou bien $\forall\, x_1,x_2,...,u_n \in \mathbf{R}\ \big(\, \mathbb{H}_\Sigma(x_1,x_2,...,x_n) \Rightarrow \exists\, y \in \mathbf{R}\ \mathbb{H}(x_1,x_2,...,x_n,y)\big)$ et alors :
$^*\big(\, \mathbb{H}_\Sigma(X_1,X_2,...,X_n) \Rightarrow \exists\ Y\ \mathbb{H}(X_1,X_2,...,X_n,Y)\,\big)^*$ (lu dans $\mathbf{K}$)

---

[1] Il serait plus correct, mais plus lourd, d'appeler 'polynôme avec degré formel' ce que nous appelons polynôme formel dans ce calcul.

ou bien $\forall\, x_1,x_2,...,x_n,y \in \mathbf{R}\ \big(\ \mathbb{H}_\Sigma(x_1,x_2,...,x_n)$ et $\mathbb{H}(x_1,x_2,...,x_n,y)\ \big) \Rightarrow 1 = 0$ et alors :

$^*\big(\ [\ \mathbb{H}_\Sigma(X_1,X_2,...,X_n)\ ,\ \mathbb{H}(X_1,X_2,...,X_n,Y)\ ]\ \Rightarrow\ 1 = 0\ \big)^*$ (dans **K**)

Dans ce dernier cas, avec (δ,s,k) comme à la proposition précédente, le degré de l'implication forte construite est majoré par :

$\delta_{28}(\delta,s,k) = \Delta_{26}(\ \delta_{28,a}(\delta,s,k)\ ;\ d_1,s,k_0,k_2\ )$ où :

$d_1 = \delta_{27}(\delta,s)$, $k_0 = \Lambda_{23}(s,1)$, $k_1 = \Lambda_{23}(s,2)$, $k_2 = \Lambda_{23}(s,k)$, et

$\delta_{28,a}(\delta,s,k) = \delta_{7,b}(\ \delta_{26,4}(d_1,s,k_1)\ ,\ \delta_{26,3}(d_1,s,k_1)\ ,\ k_2\ )$

preuve>

Nous cherchons une majoration de degré pour l'implication forte :

$$^*\big(\ [\ \mathbb{H}_\Sigma(X_1,X_2,...,X_n)\ ,\ \mathbb{H}(X_1,X_2,...,X_n,Y)\ ]\ \Rightarrow\ 1 = 0\ \big)^*$$

Le degré et le nombre de csg dans $\mathbb{H}_\Sigma$ sont majorés par $\delta_{27}(\delta,s)$ et $\Lambda_{27}(s,k)$.

En fait, les conditions de signes vraiment utilisées pour fixer un tableau de Hörmander particulier n'excèdent pas $\Lambda_{23}(s,k)$ (il suffit en effet d'assurer les degrés des pseudo-restes et les signes des constantes)[1].

Nous posons donc $d_1 = \delta_{27}(\delta,s)$ et $k_2 = \Lambda_{23}(s,k)$.

Le nombre de points dans le tableau de Hörmander est aussi majoré par k_2.

Si α est un point du tableau de Hörmander, on a l'implication forte :

$$^*\big(\ [\ \mathbb{H}_\Sigma(X_1,X_2,...,X_n)\ ,\ \mathbb{H}_\alpha(\alpha)\ ,\ \mathbb{H}(X_1,X_2,...,X_n,\alpha)\ ]\ \Rightarrow\ 1 = 0\ \big)^*$$

de degré $\delta_{26,3}(d_1,s,k_1)$ avec $k_1 = \Lambda_{23}(s,2)$: il suffit en effet de considérer le sous-tableau de Hörmander obtenu à partir du polynôme P dont α est racine et du polynôme Q dans $\mathbb{H}(X_1,X_2,...,X_n,Y)$ qui fournit la contradiction.

Si $]\alpha,\beta[$ est un intervalle minimal du tableau de Hörmander, on a l'implication forte :

$$^*\big(\ [\ \mathbb{H}_\Sigma(X_1,X_2,...,X_n),\ \mathbb{H}_\alpha(\alpha),\ \mathbb{H}_\beta(\beta),\ \alpha < Y < \beta,\ \mathbb{H}(X_1,X_2,...,X_n,Y)\ ]\ \Rightarrow\ 1 = 0\ \big)^*$$

de degré $\delta_{26,4}(d_1,s,k_1)$. (même raisonnement, en se rappelant que ce qui se passe sur l'intervalle est contrôlé par ce qui se passe au borne, sans coût supplémentaire)

Donc, par une disjonction de cas en cascade :

$$^*\big(\ [\ \mathbb{H}_\Sigma\ ;\ (\ \mathbb{H}_{\alpha_i}(\alpha_i)\ ,\ i = 1,\ ....,\ h\ )\ ;\ \mathbb{H}\ ]\ \Rightarrow\ 1 = 0\ \big)^*$$

avec pour majoration de degré :

$$\delta_{28,a}(\delta,s,k) = \delta_{7,b}(\ \delta_{26,4}(d_1,s,k_1)\ ,\ \delta_{26,3}(d_1,s,k_1)\ ,\ k_2\ )$$

On a enfin l'existence potentielle :

$$^*\big(\ \mathbb{H}_\Sigma\ \Rightarrow\ \exists\ (\alpha_i)_i\ [\ \mathbb{H}_{\alpha_i}(\alpha_i)\ ,\ i = 1,\ ....,\ h\ ]\ \big)^*\quad (\text{avec } h \le k_2\ )$$

qui accepte pour fonction Δ : $\Delta_{26}(\ d\ ;\ d_1,s,k_0,k_2\ )$: en effet chaque existence potentielle séparée (i fixé) peut être établie sur le sous-tableau de Hörmander obtenu à partir du polynôme P dont α_i est racine.

Donc la majoration souhaitée est :

$\delta_{28}(\delta,s,k) = \Delta_{26}(\ \delta_{28,a}(\delta,s,k)\ ;\ d_1,s,k_0,k_2\ )$ ❑

---

[1] En fait, vues nos majorations, ce n'est pas une amélioration par rapport à $\Lambda_{27}(s,k)$.

Théorème et majorations 29 : (nullstellensatz, positivestellensatz et nichtnegativestellensatz réels effectifs) Soit **K** un corps ordonné, sous-corps d'un corps réel clos **R**.
Soit $\mathbb{H}(X_1,X_2,...,X_n)$ un système de csg portant sur une famille finie de polynômes de $\mathbf{K}[X_1,X_2,...,X_n]$. Ce système est impossible dans **R** si et seulement si il est fortement incompatible dans **K**. En termes plus formalisés :

Si $^*(\mathbb{H}(X_1,X_2,...,X_n) \Rightarrow 1 = 0)^*$ (dans **K**) , **alors** les csg $\mathbb{H}$ sont impossibles à réaliser dans n'importe quelle extension ordonnée de **K**.

Si $\forall\, x_1,x_2,...,x_n \in \mathbf{R}$ $\mathbb{H}(x_1,x_2,...,x_n)$ est absurde,
alors : $^*(\mathbb{H}(X_1,X_2,...,X_n) \Rightarrow 1 = 0)^*$ (dans **K**).

En outre, si k est le nombre de csg dans $\mathbb{H}(X_1,X_2,...,X_n)$ et d le degré maximum, alors on peut calculer une implication forte $^*(\mathbb{H}(X_1,X_2,...,X_n) \Rightarrow 1 = 0)^*$ (dans **K**) de degré majoré par $\delta_{29}(d,k,n)$ où δ_{29} est défini par les relations récurrentes :

$\delta_{29}(d,k,1) = \delta_{28}(0,d,k)$

$\delta_{29}(d,k,n+1) = \delta_{7,c}(\sup\{ \delta_{29}(\delta_{27}(d,d) , \Lambda_{23}(d,k) , n) , \delta_{28}(d,d,k) \} , \Lambda_{27}(d,k))$

preuve> La construction de l'implication forte se fait cas par cas, selon les signes des polynômes de la famille F, (disjonction de cas en parallèle). Par ailleurs, lorsque les signes de tous les polynômes de F sont mis dans l'hypothèse de l'implication forte, ou bien ces csg sont fortement incompatibles et on est ramené au cas d'une variable en moins (avec d et k remplacés par $\delta_{27}(d,d)$, $\Lambda_{23}(d,k)$), ou bien elles ne le sont pas et on fait appel à la majoration donnée à la proposition 28. ❑

Récapitulation, majorations plus grossières et plus lisibles

Nous donnons maintenant le récapitulatif des majorations obtenues, en établissant des formes plus visibles.

Quelques notations et remarques concernant la majoration d'une fonction itérée :

Si φ est une fonction qu'on peut itérer, nous noterons $\varphi^{[k]}$ la fonction obtenue en itérant k fois φ. Nous introduisons une notation particulière pour l'itérée de l'exponentielle:

$$\boxed{E(x,k) = \varphi^{[k]}(x) \text{ où } \varphi(x) = 2^x}$$

De même si τ est une bijection, nous noterons $\tau^{[-1]}$ la bijection réciproque. Nous notons lg(a) le logarithme en base 2, c.-à-d. $\varphi^{[-1]}(x)$ où $\varphi(x) = 2^x$.
Si une fonction ψ croissante est du même ordre de grandeur[1] qu'une fonction φ croissante, mais avec une expression plus compliquée, pour obtenir une majoration plus lisible de $\psi^{[k]}$ il suffit d'arriver à majorer ψ par une fonction de la forme : $\eta = \tau^{[-1]} \circ \varphi \circ \tau$ puisqu'alors $\psi^{[k]}$ est majorée par :

$$\eta^{[k]} = \tau^{[-1]} \circ \varphi^{[k]} \circ \tau$$

Exemples:

Exemple 1 : $\varphi(x) = x^2$, $\tau(x) = a.x$:

$$\psi(x) \le a.x^2 \Rightarrow \psi^{[k]}(x) \le (a.x)^{2^k}/a .$$

[1] notion informelle intuitive, non précisée.

Exemple 2 : $\varphi(x) = x^2$, $\tau(x) = a.x + b$:

$$\psi(x) \le a.x^2 + 2b.x + (b^2 - b)/a \;\Rightarrow\; \psi^{[k]}(x) \le (a.x + b)^{2^k}/a - b/a$$

Exemple 3 : $\varphi(x) = 2^x$, $\tau(x) = a.x + b$:

$$\psi(x) \le 2^{a.x + b - \lg(a)} - b/a \;\Rightarrow\; \psi^{[k]}(x) \le E(a.x+b,k)/a - b/a.$$

Exemple 4 : $\varphi(x) = 2^x$, $\tau(x) = a.x^\alpha + b$, $a \ge 1$, $b \ge 0$, $\alpha > 1$

$$\psi(x) \le \left(2^{a.x^\alpha + b - \lg(a)} - b/a\right)^{1/\alpha} \Rightarrow \psi^{[k]}(x) \le \left(E(a.x^\alpha+b,k)/a - b/a\right)^{1/\alpha} \le E(a.x^\alpha+b,k)$$

Dans la suite, nous parlerons de fonctions φ , τ et η en nous référant toujours implicitement au schéma développé ci-dessus.

<u>Les majorations</u> δ_6

$\delta_{6,a}(d_1,d_2) = d_1 + d_2$

$\delta_{6,b}(d_1,d_2) = d_1.d_2$

$\delta_{6,c}(d_1,d_2) = d_1.d_2$

$\delta_{6,d}(d_1,d_2) = d_1.d_2 + d_2$

$$\boxed{\delta_6(d_1,d_2) = d_1.d_2 + \sup(d_1,d_2) \le (d_1+1).(d_2+1) - 1}$$

<u>Les majorations</u> δ_7

$\delta_{7,a}(d_1,d_2,d_3) = (d_1+ d_2).d_3$

$\delta_7(d_1,d_2,d_3) = d_1.d_2+ d_1.d_3+ d_2.d_3$

$\delta_{7,b}(d_1,d_3,1) = \delta_{7,a}(d_1,d_1,d_3)$

$\delta_{7,b}(d_1,d_3,h+1) = \delta_{7,a}(\delta_{7,b}(d_1,d_3,h),d_1,d_3)$

La fonction $\delta_{7,b}$ est obtenue en itérant la fonction ψ: $(d_1,d_2,d_3) \to (\delta_{7,a}(d_1,d_2,d_3),d_2,d_3)$ puis en faisant $d_2 := d_1$.

Si $d_3 \ge 2$, on majore ψ par la fonction $\eta = \tau^{[-1]} \circ \varphi \circ \tau$ avec φ et τ définies par : $\varphi(d_1,d_2,d_3) = (d_1.d_3,d_2,d_3)$, $\eta(d_1,d_2,d_3) = (d_1+ 2.d_2,d_2,d_3)$, d'où :

$$\boxed{\delta_{7,b}(d_1,d_3,h) \le 3.d_1.d_3^{\,h} \text{ (sauf si } d_3 = 1\text{, et alors } \le (h+1).d_1\text{)}}\ .$$

$\delta_{7,c}(d_1,k) = \psi^{[k]}(d_1)$ avec $\psi(d_1) = \delta_{7,a}(d_1,d_1,d_1) \le 2.d_1^{\,2}$

$$\boxed{\delta_{7,c}(d_1,h) \le (2.d_1)^{2^h}}\ .\ \text{(cf. exemple 1 avec } \tau(d_1) = 2.d_1\text{)}$$

<u>Les majorations</u> δ_8

$\delta_8(d_1,d_2,1) = \delta_6(d_1,d_2)$

$\delta_8(d_1,d_2,k+1) = \delta_6(d_1,\delta_8(d_1,d_2,k))$

La majoration δ_8 est obtenue en itérant la fonction : $(d_1,d_2) \to (d_1,\delta_6(d_1,d_2))$. En considérant $\tau(d_1,d_2) = (1+d_1,1+ d_2)$ et $\varphi(d_1,d_2) = (d_1,d_1.d_2)$, on obtient : $\eta(d_1,d_2) = (d_1, (d_1+ d_2)^2 - d_1) \ge (d_1, \delta_6(d_1,d_2))$ (si d_1 et $d_2 \ge 2$) et donc :

$$\boxed{\delta_8(d_1,d_2,k) \le (1+d_1)^k.(1+d_2) - 1}$$

<u>Les majorations</u> Δ_{10}

(fonction Δ pour les évidences fortes résultant des formules de Taylor mixtes)

$\Delta_{10}(d;\delta) = \delta_6(d,2\delta)$

$\boxed{\Delta_{10}(d;\delta) \le (d+1).(2\delta+1) - 1}$

Les majorations Δ_{14} *(fonction Δ d'une implication forte)*

$\Delta_{14}(d;d_1,k) = \delta_8(d_1,d,k)$

$\Delta_{14,a}(d;[d_1,d_2, ...,d_k]) = \delta_6(d_1,...(\delta_6(d_k,d))...) \le (1+d_1).(1+d_2)...(1+d_k).(1+d) - 1$

$\boxed{\Delta_{14}(d;d_1,k) \le (1+d_1)^k.(1+d) - 1}$

$\boxed{\Delta_{14}(d;[d_1,d_2, ...,d_k]) \le (1+d_1).(1+d_2)...(1+d_k).(1+d) - 1}$

Les majorations Δ_{20}

(fonction Δ pour l'existence potentielle de l'inverse d'un non nul, et pour l'existence d'un point où un polynôme a le signe de son coefficient dominant)

$\Delta_{20}(d;\delta) = d + d.\delta + \delta$

$\Delta_{20,a}(d;0,s) = \Delta_{20,a}(d;\delta,0) = d$ et pour s et $\delta > 0$

$\Delta_{20,a}(d;\delta,s) = \Delta_{20}(d.(\delta+1).(1+2s\delta) ; \delta)$

$\boxed{\Delta_{20}(d;\delta) = (1+d).(1+\delta) - 1}$

$\boxed{\Delta_{20,a}(d;\delta,s) \le (d+1).(\delta+1)^2.(2s\delta+1) - 1}$

Les majorations Δ_{21} *(fonction Δ pour l'existence potentielle d'une racine d'un polynôme qui change de signe)*

sans paramètres

$\Delta_{21,0}(d;0) = 1$

$\Delta_{21,0}(d;1) = d$

$\Delta_{21,0}(d;s+2) = \Delta_{14,a}(2d ; [\Delta_{21,0}(d;s),d,d])$

C.-à-d. : $\Delta_{21,0}(d;s+2) \le (2d+1).(d+1)^2.(\Delta_{21,0}(d;s)+1) - 1$. On établit par récurrence :

$\boxed{\Delta_{21,0}(d;s) \le (d+1)^s.(2d+1)^{s \text{ div } 2} - 1 \quad \text{pour } s \ge 1}$

avec paramètres ($d \ge \delta$, sinon $\Delta_{21}(d;\delta,s) = d$)

$\Delta_{21}(d;\delta,0) = 2d$

$\Delta_{21}(d;\delta,1) = \delta_{6,c}(2d , \Delta_{20}(d.(\delta+1); \delta - 1))$

$\delta_1(d,\delta,s+2) = (d - s - 1).(\delta - s - 2) + d$ que nous notons δ_1 ci-dessous

$\Delta_{21,u}(d;\delta,s+2) = \Delta_{14,a}(4\delta_1 ; [\Delta_{21}(\delta_1;\delta_1,s),\delta_1,\delta_1])$

$\Delta_{21,a}(d;\delta,s+2) = \Delta_{21}(d;\delta,s+1) + 2\delta$

$\Delta_{21,b}(d;\delta,s+2) = \Delta_{20}(\Delta_{21,u}(d;\delta,s+2) + 2(\delta - s - 2)) ; \delta)$

$\Delta_{21}(d;\delta,s+2) = \delta_{6,c}(\Delta_{21,a}(d;\delta,s+2) , \Delta_{21,b}(d;\delta,s+2))$

On a : $\Delta_{21}(d;\delta,1) = 2\,d(d+1)\delta(\delta+1) - 2d\delta^2 - 1 \le 2\,(d+1)^2.(\delta+1)^2 - 2\delta$.
On majore δ_1 par $d\delta - 1$. En appliquant les formules de récurrence on trouve :

$$\Delta_{21}(d;\delta,2) \le 16\,(d+1)^6.(\delta+1)^7 - 2\delta$$

et on tente une majoration de la forme :

$$\Delta_{21}(d;\delta,s) \le 2^{\alpha(s)}\,(d+1)^{\beta(s)}\,(\delta+1)^{\gamma(s)} - 2\delta$$

On trouve alors que α, β, γ conviennent s'ils vérifient les formules récurrentes :

$\alpha(s+2) \le 2 + \alpha(s+1) + \alpha(s)$

$\beta(s+2) \le 3 + \beta(s+1) + \beta(s) + \gamma(s)$

$\gamma(s+2) \leq 4 + \gamma(s+1) + \beta(s) + \gamma(s)$

Ceci est vérifié, avec l'initialisation pour $s = 1$ et 2, si on prend :

$\alpha(s) = 2^s$, $\beta(s) = 2^{s+1} - (s+3) \text{ div } 2$, $\gamma(s) = 2^{s+1} + (s-4) \text{ div } 2$

d'où par exemple :

$$\Delta_{21}(d;\delta,s) \leq (2.(d+1).(\delta+1))^{2^{s+1}}.(\delta+1)^{s \text{ div } 2}$$

Les majorations Δ_{22} *(fonction Δ pour l'existence potentielle d'une racine d'un polynôme sur un intervalle où il change de signe)*

$\Delta_{22,a}(d;\delta,0) = 2.\delta$, $\Delta_{22,a}(d;\delta,1) = \Delta_{21}((d+4).\delta ; \delta , 1)$

$\Delta_{22,a}(d;\delta,s+1) = \Delta_{21}(\delta_{6,a}(d.\delta , (\Delta_{22,a}(d;\delta-1,s)+4) . \delta) ; \delta , s+1)$

$\Delta_{22}(d;\delta,s) = \Delta_{22,a}(2.d+2 ; \delta , s)$.

On a donc : $\Delta_{22,a}(d;\delta,s+1) = \Delta_{21}((\Delta_{22,a}(d;\delta-1,s) + 5) . \delta) ; \delta , s+1)$ avec à l'initialisation : $\Delta_{22,a}(d;\delta,1) \leq 2.(d+5)^2.\delta^2.(\delta+1)^2 - 2\delta \leq 2.(d+5)^2.(\delta+1)^4 - 5$ et on tente une majoration de la forme:

$$\Delta_{22,a}(d;\delta,s) \leq 2^{\alpha'(s)} (d+5)^{\beta'(s)} (\delta+1)^{\gamma'(s)} - 5$$

On trouve alors que α', β', γ', conviennent s'ils vérifient les formules récurrentes :

$\alpha'(s+1) \leq \alpha(s+1) + \alpha'(s).\beta(s+1)$

$\beta'(s+1) \leq \beta(s+1).\beta'(s)$

$\gamma(s+1) \leq \gamma(s+1) + \gamma'(s).\beta(s+1)$

On majore $\gamma(s)$ par $(\delta+1)^{2^{s+2}}$. On vérife que l'initialisation et les formules récurrentes sont vérifiées si on prend : $\beta'(s) = 2^{(s+1)(s+2)/2}$, $\alpha'(s) = 2^{-1+(s+2)^2/2}$, $\gamma'(s) = 2^{(s+2)^2/2}$.

En conclusion :

$$\Delta_{22,a}(d;\delta,s) \leq 2^{\alpha'(s)} (d+5)^{\beta'(s)} (\delta+1)^{\gamma'(s)} - 5 \quad \text{avec} \quad \alpha'(s) = 2^{-1+(s+2)^2/2}$$
$$\beta'(s) = 2^{(s+1)(s+2)/2}, \ \gamma'(s) = 2^{(s+2)^2/2}$$

et

$$\Delta_{22}(d;\delta,s) \leq 2^{\gamma'(s)} (d+3,5)^{\beta'(s)} (\delta+1)^{\gamma'(s)} - 5 \leq ((2d+7) (\delta+1))^{\gamma'(s)}$$

Problème : peut-on améliorer de manière sensible les majorations 21 et 22 pour l'existence potentielle de racines réelles ?

Ceci n'est pas certain.
Pour obtenir une telle amélioration, il semble qu'il faudrait "dérécursiver" la preuve d'existence de la clôture réelle d'un corps ordonné (telle que donnée dans [**LR**]). Ceci est peut-être possible sur la base d'une analyse approfondie des suites de Sturm-Habicht, ou de généralisations des formules de Taylor mixtes.

Il semble par contre que les majorations qui vont suivre, particulièrement mauvaises, soient directement imputables à l'algorithme de Hörmander, qui donne lieu à une explosion des degrés en $E(d,n)$. On peut donc sérieusement espérer les améliorer sur la base d'une stratégie qui serait inspirée des algorithmes qui testent “rapidement” si un semi-algébrique réel est vide.

La majoration Λ_{23} *(majoration du nombre de points d'un tableau de Hörmander)*

$\Lambda_{23}(s,k) = (k+1)^{2^s}$

Les majorations Δ_{26} et δ_{26} *(évidence forte et existence potentielle pour les faits élémentaires lisibles sur un tableau de Hörmander paramétré)*

Initialisations : $\Delta_{26,1}(d;\delta,s,m_1) = \Delta_{21}(\Delta_{21}(d;\delta,1);\delta,1)$

$\delta_{26,2}(\delta,s,m_1) = \delta_{26,3}(\delta,s,m_1) = \delta_{26,4}(\delta,s,m_1) = 4\delta$

$\Delta_{26,2}(d;\delta,s,m_1) = \Delta_{26,3}(d;\delta,s,m_1) = \Delta_{26,4}(d;\delta,s,m_1) = \Delta_{26,4,a}(d;\delta,s,m_1) = \delta_6(d;4\delta)$

Récurrences : $m \geq m_1$ (en ne mentionnant pas les δ,s dans les $\Delta_{26,...}(d;\delta,s,m)$

$\Delta_{26,1,a}(d;m) = \Delta_{26,3}(\delta_6(d,2\delta);m)$

$\Delta_{26,1,b}(d;m) = \Delta_{26,1,a}(\Delta_{26,1,a}(\Delta_{26,2}(d;m);m);m)$

$\Delta_{26,1,b'}(d;m) = \Delta_{26,1,a}(\Delta_{10}(d;\delta);m)$

$\Delta_{26,1,c}(d;m) = \Delta_{26,1}(\Delta_{26,1,b}(\Delta_{22}(\Delta_{26,4}(d;m);\delta,s);m);m)$

$\Delta_{26,1,c'}(d;m) = \Delta_{26,1}(\Delta_{20,a}(\Delta_{26,1,b'}(\Delta_{22}(\Delta_{26,4,a}(d;m);\delta,s);m);\delta,s);m)$

– $\Delta_{26,1}(d;m+1) = \sup(\Delta_{26,1,c}(d;m), \Delta_{26,1,c'}(d;m))$

– $\Delta_{26,2}(d;m+1) = \Delta_{10}(\Delta_{26,1,a}(\Delta_{26,3}(d;m);m);\delta)$

$\Delta_{26,3,a}(d;m+1) = \Delta_{26,1,a}(\Delta_{26,3}(d;m);m)$

$\Delta_{26,3,a'}(d;m+1) = \Delta_{26,1}(\Delta_{26,2}(\Delta_{26,2}(\Delta_{26,4}(d;m);m+1);m+1);m)$

– $\Delta_{26,3}(d;m+1) = \sup(\Delta_{26,3,a}(d;m+1), \Delta_{26,3,a'}(d;m+1))$

– $\Delta_{26,4,a}(d;m+1) = \Delta_{26,3}(d;m+1)$

– $\Delta_{26,4}(d;m+1) = \Delta_{26,3}(\Delta_{26,3}(d;m+1);m+1)$

– $\Delta_{26}(d;m,h)$ = itérée h fois de la fonction $d \to \Delta_{26,1}(d;m)$

$\delta_{26,2}(\delta,s,m) = \Delta_{26,2}(2\delta;\delta,s,m)$

$\delta_{26,3}(\delta,s,m) = \Delta_{26,3}(2\delta;\delta,s,m)$

$\delta_{26,4}(\delta,s,m) = \Delta_{26,4}(2\delta;\delta,s,m)$

Notons $\theta(d;\delta,s,m) = \sup(\Delta_{26,i}(d;\delta,s,m);\ i = 1, 2, 3)$. Considérons δ et s comme des paramètres fixés. On peut alors noter :

$\theta_m(d) = \theta(d;\delta,s,m)$, $\mu(d) = \delta_6(d,2\delta)$, $\Delta_{22}(d) = \Delta_{22}(d;\delta,s)$, $\Delta_{10}(d) = \Delta_{10}(d;\delta)$

Les formules récurrentes donnent alors les conditions suffisantes :

$\Delta_{26,1}(d;m+1) \leq \theta_m \circ \theta_m \circ \mu \circ \theta_m \circ \mu \circ \theta_m \circ \Delta_{22} \circ \theta_m \circ \theta_m\ (d)$

$\Delta_{26,2}(d;m+1) \leq \Delta_{10} \circ \theta_m \circ \mu \circ \theta_m$

$\Delta_{26,3}(d;m+1) \leq \theta_m \circ \Delta_{10} \circ \theta_m \circ \mu \circ \theta_m \circ \Delta_{10} \circ \theta_m \circ \mu \circ \theta_m \circ \theta_m\ (d)$

il suffit donc d'avoir :

$\theta_{m+1}(d) \leq \theta_m \circ \theta_m \circ \mu \circ \theta_m \circ \mu \circ \theta_m \circ \Delta_{22} \circ \theta_m \circ \theta_m\ (d)$ (1)

Si on prend :

$\theta_1(d) = \mu \circ \mu \circ \Delta_{22}\ (d)$, $\theta_{m+1} = \theta_m^{[7]}$, c.-à-d. $\theta_{m+1} = \theta_1^{[7^m]}$

alors l'inégalité (1) sera vérifiée.

On a $\theta_1(d) \leq (2\delta+2)^{2+\gamma'(s)}(d+4)^{\beta'(s)} - 4$.

On en déduit : $\theta_1^{[h]} \leq (2\delta+2)^{(2+\gamma').\beta'^{h+2}}(d+4)^{\beta'^{h+1}} - 4$

on en déduit : $\theta_m(d) \leq (2\delta+2)^{\gamma_1(s,m)}(d+4)^{\beta_1(s,m)} - 4$

où $\gamma_1(s,m) = 2^{7^m(s+2)^2/2}$, $\beta_1(s,m) = 2^{7^m(s+1)(s+2)/2}$

On en déduit : $\boxed{\delta_{26,i}(\delta,s,m) \leq \delta^{\alpha_1(s,m)}\ (i=2,3,4)\ \text{où}\ \alpha_1(s,m) = 2^{7^m(s+2)^2}\ (\delta \geq 2)}$

et $\boxed{\Delta_{26}(d;\delta,s,m,h) \leq (\delta.d)^{\alpha_2(s,m,h)}\ \text{où}\ \alpha_2(s,m,h) = 2^{h.7^m(s+2)^2}\ (d,\delta \geq 2)}$

Les majorations δ_{27} et Λ_{27} *(tableau de Hörmander paramétré)*

$\delta_{27}(d,s) = d.(s+1)!$, sauf $\delta_{27}(0,s) = s$

$\Lambda_{27}(s,k) = (k+1)^{2^s}$

Les majorations δ_{28}

(Tableau de Hörmander paramétré, implications fortes et existences potentielles)

$\delta_{28}(d,s,k) = \Delta_{26}(\delta_{28,a}(d,s,k) ; d_1,s,k_0,k_2)$ où :

$d_1 = \delta_{27}(d,s)$, $k_0 = \Lambda_{23}(s,1)$, $k_1 = \Lambda_{23}(s,2)$, $k_2 = \Lambda_{23}(s,k)$, et

$\delta_{28,a}(d,s,k) = \delta_{7,b}(\delta_{26,4}(d_1,s,k_1) , \delta_{26,3}(d_1,s,k_1) , k_2)$

Cela conduit à une majoration du type :

$\delta_{28}(d,s,k) \leq E(s+\lg(s)+\lg\lg(k+d)+cte , 5)$

Les majorations δ_{29} *(nullstellensatz et variantes, majoration des degrés)*

$\delta_{29}(d,k,1) = \delta_{28}(0,d,k)$

$\delta_{29}(d,k,n+1) = \delta_{7,c}(\sup\{ \delta_{29}(\delta_{27}(d,d) , \Lambda_{23}(d,k) , n) , \delta_{28}(d,d,k) \} , \Lambda_{27}(d,k))$

Cela conduit à une majoration du type :

$\delta_{29}(d,k,n) \leq E(d.\lg(d)+\lg\lg(k)+cte , 4+n)$