UNE BORNE SUR LES DEGRES POUR LE THéORèME DES ZéROS RéEL EFFECTIF

Henri LOMBARDI
Laboratoire de Mathématiques
UFR des Sciences et Techniques
Université de Franche-Comté
25030 BESANCON Cedex
FRANCE

Tel 81 66 63 40
e mail : TDNBESAC@FRGREN81

UNE BORNE SUR LES DEGRES POUR LE THéORèME DES ZéROS RéEL EFFECTIF

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

Résumé Nous donnons les idées et résultats essentiels d'un calcul d'une majoration des degrés pour le théorème des zéros réels effectif.

Abstract We give the main ideas and results concerning a computation of a degree majoration for the real nullstellensatz.

1) Introduction

Nous rendons compte dans cet article du calcul d'une borne sur les degrés accompagnant la preuve constructive du théorème des zéros réel et de ses variantes (cf. [**Lom d**]). Les preuves sans les majorations de degré peuvent être trouvées dans [**Lom b**] .

Les résultats obtenus

Une formulation générale du théorème des zéros réel et de ses variantes peut être la suivante (cf [**BCR**] théorème 4.4.2) : on considère un système d'égalités et inégalités portant sur des polynomes 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 semi-algébrique de $\mathbf{R}^n$; le théorème affirme que S est vide (fait géométrique) si et seulement si il y a une certaine identité algébrique construite à partir des polynomes donnés, identité qui donne une preuve de ce fait géométrique. Calculer une borne sur les degrés pour le théorème des zéros réels consiste à calculer une majoration sur les degrés des polynomes intervenant dans le résultat (l'identité algébrique construite) à partir de la taille de l'entrée (le système de conditions de signes portant sur la liste de polynomes donnée au départ). Les paramètres qui controlent la majoration des degrés dans le résultat sont en fait : le nombre k de polynomes dans l'entrée, le degré d des polynomes dans l'entrée, et le nombre n de variables.
Le calcul de majoration est obtenu en suivant pas à pas la preuve constructive d'existence de l'identité algébrique et en explicitant les majorations à chaque étape de la preuve.
C'est une majoration primitive récursive, donnée par une tour d'exponentielles : le nombre d'étages dans la tour est n+4 et en haut de la tour on trouve :

d.log(d) + loglog(k) + cte .

Ce résultat n'est pas trop mauvais, dans la mesure où la principale responsabilité de l'explosion est supportée par l'algorithme de Hörmander, à la base de la preuve effective. On peut espérer raisonnablement baser une autre preuve effective sur des algorithmes plus performants et obtenir en conséquence une majoration où le paramètre n interviendrait de manière moins catastrophique, comme dans les versions effectives du théorème des zéros de Hilbert.

La preuve constructive du théorème des zéros réels

De manière générale un «théorème des zéros» affirme que certains faits «géométriques» ont une preuve purement «algébrique».
Un exemple simple est fourni par la formule de Taylor. Par exemple pour un polynome de degré ≤ 4 , on a l'identité algébrique : (avec $\Delta = U - V$)

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

Cette identité algébrique rend manifeste le fait géométrique suivant : si en un point v le polynome P a toutes ses dérivées positives, alors pour tout $u > v$ on a $P(u) > P(v)$. Ce fait géométrique est un cas particulier du lemme de Thom et peut être rendu manifeste par un tableau de variation.
La construction du nullstellensatz réel utilise une version "identité algébrique" du lemme de Thom, donnée par ce que nous appelons les formules de Taylor mixtes et les formules de Taylor généralisées.

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 polynomes 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), 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 polynome sur un intervalle où il change de signe.
Les ...-stellensatz réels effectifs doivent donc pouvoir être obtenus si on arrive à "algébriser" les arguments de base de la preuve d'incompatibilité et les méthodes de déduction impliquées.
Un pas important a déjà été réalisé avec la version algébrique du théorème des accroissements finis pour les polynomes (cf [**LR**]), qui a été à l'origine des formules de Taylor mixtes et généralisées.
Un autre pas a consisté à traduire sous forme de *constructions d'identités algébriques* 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*.

Remarques sur l'article présent

Nous intoduisons dans cet article une problématique où le role central est tenu par les constructions d'identités algébriques (appelées «incompatibilités fortes») à

partir d'autres identités algébriques, alors que dans les versions précédentes c'étaient plutôt les identités algébriques elles-mêmes qui jouaient le role central. Ce changement de point de vue a été motivé par le calcul de majoration lui-même. Ce qui, dans [**Lom d**], apparaissait sous l'appellation peu plaisante d'«implication forte vue comme existence potentielle», s'appelle désormais «implication dynamique». Quant aux anciennes implications fortes, elles ne jouent pratiquement plus aucun role. Nous donnons dans ce nouveau cadre un traitement unifié pour les preuves cas par cas («disjonction dynamique»), l'implication («implication dynamique») et l'existence («existence potentielle»).

Significations de la preuve constructive pour différentes écoles philosophiques

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 réclamées dans la structure du corps des coefficients par le mathématicien constructif 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. En fait 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 :

si $(c_i)_{i=1,...,m}$ est la famille des coefficients et si $P \in \mathbb{Z}[(C_i)_{i=1,...,m}]$ l'oracle répond à la question « Quel est le signe de $P((c_i)_{i=1,...,m})$? ».

2) Incompatibilités fortes

Incompatibilités fortes : définitions et notations

Nous considérons un corps ordonné **K** , et une liste de variables X_1, X_2, ..., X_n désignée par **X** .
Nous notons donc **K**[**X**] l'anneau des polynomes $\mathbf{K}[X_1,X_2,...,X_n]$.
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 $M(F)$.

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 $Cp(F)$.

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

Définition et notation 1 : Etant donnés 4 parties finies de **K**[**X**] : $F_{>}$, $F_{\geq}$, $F_{=}$, $F_{\neq}$, contenant des polynomes 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 **K** si on a une égalité dans **K**[**X**] du type suivant :

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

Nous utiliserons la notation suivante pour une incompatibilité forte:

$$\downarrow [\, S_1 > 0, ..., S_i > 0, P_1 \geq 0, ..., P_j \geq 0, Z_1 = 0, ..., Z_k = 0, N_1 \neq 0, ..., N_h \neq 0 \,] \downarrow$$

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 polynomes 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.

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 polynomes 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.

Degré d'une incompatibilité forte

Si nous voulons préciser les majorations de degré fournis par notre preuve du théorème des zéros réel, nous devons préciser la terminologie.

Nous manipulons des incompatibilités fortes écrites *sous forme paire,,* c.-à-d.:

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

(la considération des formes paires d'implications fortes a pour unique utilité de faciliter un peu le calcul de majoration des degrés)
Quand nous parlons de degré, sauf précision contraire, il s'agit du degré total maximum.
Le degré d'une incompatibilité forte est par convention au moins égal à 1, c'est le degré maximum des polynomes qui «composent» l'incompatibilité forte.
Par exemple, si nous avons une incompatibilité forte :

$$\downarrow [\, A > 0 , B > 0 , C \geq 0 , D \geq 0 , E = 0 , F = 0 \,] \downarrow$$

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'incompatibilité forte est :

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

Le calcul de majoration

Nous allons expliquer dans cet article comment peut être mené un calcul de majorations primitives récursives pour le théorème des zéros réels. Les détails des calculs sont dans [**Lom d**].

Les données sont trois entiers d, n, k qui majorent, dans un système de csg incompatible $\mathbb{H}$, respectivement les degrés des polynomes, 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 incompatibilité forte $\downarrow \mathbb{H} \downarrow$, 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'incompatibilité forte à partir des coefficients donnés au départ.

En fait, chacun des théorèmes ou propositions qui conduit à la preuve constructive du théorème des zéros réel peut être accompagné d'une majoration primitive récursive du même type. Ces majorations s'enchainent les unes les autres, sans difficulté majeure.

Comme le calcul est très fastidieux, nous nous en sommes tenus 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.

Constructions d'incompatibilités fortes

Définition 2 : Nous parlerons de construction d'une incompatibilité forte à partir d'autres incompatibilités 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 incompatibilités fortes.

Notation 3 : Nous noterons cette implication logique (au sens constructif) par un signe de déduction "constructif" . La notation

$$(\downarrow \mathbb{H}_1 \downarrow \text{ et } \downarrow \mathbb{H}_2 \downarrow) \ \vdash_{\overline{\text{cons}}} \downarrow \mathbb{H}_3 \downarrow$$

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

Cela n'a d'intérêt que lorsque les incompatibilités fortes désignées en hypothèse et en conclusion comportent des éléments variables.

Un exemple fondamental aidera à mieux comprendre.

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

Nous donnons ici un énoncé détaillé des «raisonnements cas par cas», incluant la propagation des majorations de degrés.

Proposition 4 : Soit $\mathbb{H}$ un système de csg portant sur des polynomes de $\mathbf{K}[\mathbf{X}]$, Q un élément de $\mathbf{K}[\mathbf{X}]$, alors:

$[\downarrow(\mathbb{H}, Q<0)\downarrow$ et $\downarrow(\mathbb{H}, Q>0)\downarrow] \; \vdash_{\overline{\text{cons}}} \downarrow(\mathbb{H}, Q\neq 0)\downarrow$ (a)

$[\downarrow(\mathbb{H}, Q\leq 0)\downarrow$ et $\downarrow(\mathbb{H}, Q\geq 0)\downarrow] \; \vdash_{\overline{\text{cons}}} \downarrow\mathbb{H}\downarrow$ (a')

De même :

$[\downarrow(\mathbb{H}, Q>0)\downarrow$ et $\downarrow(\mathbb{H}, Q=0)\downarrow] \; \vdash_{\overline{\text{cons}}} \downarrow(\mathbb{H}, Q\geq 0)\downarrow$ (b)

$[\downarrow(\mathbb{H}, Q\neq 0)\downarrow$ et $\downarrow(\mathbb{H}, Q=0)\downarrow] \; \vdash_{\overline{\text{cons}}} \downarrow\mathbb{H}\downarrow$ (c)

$[\downarrow(\mathbb{H}, Q>0)\downarrow$ et $\downarrow(\mathbb{H}, Q\leq 0)\downarrow] \; \vdash_{\overline{\text{cons}}} \downarrow\mathbb{H}\downarrow$ (d)

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

$\mu_{4,a}(d_1,d_2) = \mu_{4,a'}(d_1,d_2) = d_1 + d_2$

$\mu_{4,b}(d_1,d_2) = d_1.d_2$

$\mu_{4,c}(d_1,d_2) = d_1.d_2$

$\mu_{4,d}(d_1,d_2) = d_1.d_2 + d_2$

Ces 4 fonctions sont majorées par $\mu_4(d_1,d_2) = d_1.d_2 + d_1 + d_2$

Enfin, 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. Ce qui renvient à affirmer :

$[\downarrow(\mathbb{H}, Q>0)\downarrow$ et $\downarrow(\mathbb{H}, Q<0)$ et $\downarrow(\mathbb{H}, Q=0)\downarrow] \; \vdash_{\overline{\text{cons}}} \downarrow\mathbb{H}\downarrow$ (e)

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

$\mu_{4,e}(d_1,d_2,d_3) = d_1.d_2 + d_1.d_3 + d_2.d_3$

3) Versions algébriques dynamiques de l'implication et de la disjonction

La version algébrique dynamique de l'implication

Définition et notation 5 :

Soient $\mathbb{H}_1$ et $\mathbb{H}_2$ deux systèmes de csg portant sur des polynomes de $\mathbf{K}[\mathbf{X}]$. Nous dirons que *le système* $\mathbb{H}_1$ *implique dynamiquement* $\mathbb{H}_2$ lorsque, pour tout système de csg $\mathbb{H}$ portant sur des polynomes de $\mathbf{K}[\mathbf{X},\mathbf{Y}]$, on a la construction d'incompatibilité forte :

$\downarrow[\mathbb{H}_2(\mathbf{X}), \mathbb{H}(\mathbf{X},\mathbf{Y})]\downarrow \; \vdash_{\overline{\text{cons}}} \downarrow[\mathbb{H}_1(\mathbf{X}), \mathbb{H}(\mathbf{X},\mathbf{Y})]\downarrow$

Nous noterons cette implication dynamique par :

$$\bullet(\ \mathbb{H}_1(\mathbf{X}) \Rightarrow \mathbb{H}_2(\mathbf{X}) \ )^\bullet.$$

Lorsque le système $\mathbb{H}_1$ est vide, nous utilisons la notation $\bullet(\ \mathbb{H}_2(\mathbf{X}) \ )^\bullet$.

Remarques :

1) On a trivialement l'équivalence des affirmations :

$$\downarrow \mathbb{H}_1 \downarrow \quad \text{et} \quad \bullet(\ \mathbb{H}_1 \Rightarrow (1 = 0) \ )^\bullet$$

2) La vision dynamique de l'implication correspond, dans les références [**Lom x**] à l'«implication forte vue comme existence potentielle». En tant qu'implication forte «statique», c'était une liste d'identités algébriques. En tant qu'implication dynamique, cela devient un algorithme de manipulations d'identités algébriques. Dans la mise en oeuvre concrète d'algorithmes de construction du théorème des zéros réel, la vision dynamique est en fait beaucoup plus fructueuse que la vision statique. Certaines subtilités s'introduisent, comme le fait que deux implications qui ont la même signification peuvent avoir des dynamiques distinctes (c.-à-d. qu'elles se traduisent pas des algorithmes de manipulations d'identités algébriques distincts), et ont alors des coûts (en termes de temps de calcul) différents. (pour plus de détails voir le paragraphe “Variations sur le thème des implications dynamiques”).

Il apparaît en fin de compte que les “bonnes notions” sont celles d'incompatibilité forte et d'implication dynamique, tandis que la notion d'implication forte serait plutôt un incident de parcours. Nous verrons un peu plus loin que les raisonnements cas par cas peuvent être interprétés par une autre “bonne notion”, la version dynamique du «ou» .

La notation que nous utilisons ici est légèrement distincte de celle utilisée dans les précédentes références [**Lom**] pour noter les existences potentielles. Ceci nous permet de mieux insister sur la différence de signification entre une implication forte «statique» et une implication dynamique.

Fonction-degré d'une implication dynamique

Une implication dynamique $\bullet(\ \mathbb{H}_1 \Rightarrow \mathbb{H}_2)^\bullet$ signifie par définition un algorithme fournissant la construction :

$$\downarrow [\, \mathbb{H}_2 \,,\, \mathbb{H} \,] \downarrow \ \vdash_{\overline{\text{cons}}} \downarrow [\, \mathbb{H}_1 \,,\, \mathbb{H} \,] \downarrow$$

Chaque fois que nous établissons une implication dynamique particulière, nous devons établir des ‘majorations primitives récursives de degré’ pour cette construction d'incompatibilités fortes : le degré de l'incompatibilité forte construite est majoré par une fonction $\Delta(d,..;k,...)$ où d est le degré de l'incompatibilité forte initiale, k le nombre de csg dans $\mathbb{H}_2$ etc.... (le point-virgule isole les ‘variables’, qui dépendent de l'incompatibilité 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-degré acceptable pour l'implication dynamique considérée, ou encore, (par abus) nous parlons de *la* fonction-degré attachée à l'implication dynamique.

La transitivité des implications dynamiques

La proposition suivante est immédiate : il suffit d'enchainer les deux algorithmes de constructions d'incompatibilités fortes.

Proposition 6 : Soient $\mathbb{H}_1$, $\mathbb{H}_2$, $\mathbb{H}_3$ trois systèmes de csg portant sur des polynomes de **K**[**X**] . Alors:

$[\ {}^\bullet(\ \mathbb{H}_1 \Rightarrow \mathbb{H}_2\ )^\bullet$ et ${}^\bullet(\ [\ \mathbb{H}_1\ ,\ \mathbb{H}_2\ ] \Rightarrow \mathbb{H}_3\ )^\bullet\ ]$ impliquent ${}^\bullet(\ \mathbb{H}_1 \Rightarrow \mathbb{H}_3\ )^\bullet$

Supposons que la première implication dynamique admette comme fonction-degré acceptable $\Delta^1(d;\mathbf{p})$ où d est le degré de $\downarrow [\ \mathbb{H}_2,\ \mathbb{H}\ ] \downarrow$ et **p** représente certains paramètres dépendant de $\mathbb{H}_1$ et $\mathbb{H}_2$, supposons de même une fonction-degré acceptable $\Delta^2(d;\mathbf{q})$ pour la deuxième implication dynamique, alors une fonction-degré pour l'implication dynamique construite est obtenue en composant les deux fonctions-degré précédentes :

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

La proposition qui suit est un corollaire immédiat de la précédente.

Proposition 7 : Soient $\mathbb{H}_1$, $\mathbb{K}_1$, $\mathbb{K}_2$, ..., $\mathbb{K}_n$ des systèmes de csg portant sur des polynomes de **K**[**X**] . Alors :

$$[\ {}^\bullet(\ \mathbb{H}_1 \Rightarrow \mathbb{K}_1\ )^\bullet, {}^\bullet(\ \mathbb{H}_1 \Rightarrow \mathbb{K}_2\ )^\bullet\ , ..., {}^\bullet(\ \mathbb{H}_1 \Rightarrow \mathbb{K}_n\ )^\bullet\ ]$$
$$\vdash_{\overline{\text{cons}}} \quad {}^\bullet(\ \mathbb{H}_1 \Rightarrow [\ \mathbb{K}_1\ ,\ \mathbb{K}_2\ , ..., \mathbb{K}_n\ ]\ )^\bullet$$

En outre, une fonction-degré pour l'implication dynamique construite est obtenue en composant (dans un ordre arbitraire) les fonctions-degré des implications dynamiques de l'hypothèse

Cas des implications dynamiques avec une seule condition de signe dans la conclusion

Combinée avec le corollaire précédent, la proposition qui suit permet de montrer l'équivalence d'une implication dynamique avec la donnée d'une liste d'incompatibilités fortes. Cette donnée était appelée une implication forte dans les articles précédents.

Proposition 8 :

Soient $\mathbb{H}_1$ un système de csg portant sur des polynomes de **K**[**X**] , Q un élément de **K**[**X**] , σ un élément de $\{ > , < , = , \geq , \leq , \neq \}$ et σ' l'élément opposé, alors :

$$\downarrow (\ \mathbb{H}_1\ ,\ Q\ \sigma\ 0\ ) \downarrow \quad \text{si et seulement si} \quad {}^\bullet(\ \mathbb{H}_1 \Rightarrow Q\ \sigma'\ 0\ )^\bullet$$

Si d_1 est le degré d'une incompatibilité forte $\downarrow (\ \mathbb{H}_1\ ,\ Q\ \sigma\ 0\ ) \downarrow$, alors une fonction-degré acceptable pour l'implication dynamique est

$$\Delta(d) = \mu_4(d,d_1) = d.d_1 + d + d_1 .$$

Inversement si d_Q est le degré du polynome Q et si Δ est une fonction-degré acceptable pour l'implication dynamique, le degré de l'incompatibilité forte peut être majoré par $\Delta(2.d_Q)$.

preuve> Dans le sens direct : soit $\mathbb{H}$ un système de csg et une incompatibilité forte $\downarrow \mathbb{H}, Q\sigma' 0\downarrow$ de degré d, on peut construire l'incompatibilité forte $\downarrow(\mathbb{H}_1, \mathbb{H})\downarrow$ en raisonnant cas par cas. Dans le cas $Q\sigma 0$ on utilise l'incompatibilité forte $\downarrow(\mathbb{H}_1, Q\sigma 0)\downarrow$ de degré d_1 et dans le cas $Q\sigma' 0$ on utilise l'incompatibilité forte $\downarrow \mathbb{H}, Q\sigma' 0\downarrow$, on conclut en utilisant la proposition 4.
Réciproque : on a une incompatibilité forte sous forme paire de degré $2.d_Q$:

$$\downarrow(Q\sigma 0, Q\sigma' 0)\downarrow,$$

obtenue en lisant convenablement l'identité

$$Q^2 + Q.(-Q) = 0,$$

on applique alors la définition de l'implication dynamique en prenant pour $\mathbb{H}$ la seule condition $Q\sigma 0$. ❑

La version algébrique dynamique de la disjonction

Définition et notation 9 :

Soient $\mathbb{H}_1, \mathbb{H}_2, \ldots, \mathbb{H}_k$ et $\mathbb{K}_1, \mathbb{K}_2, \ldots, \mathbb{K}_m$ des systèmes de csg portant sur des polynomes de $\mathbf{K}[\mathbf{X}]$.

Nous disons que *le système* $\mathbb{H}_1$ *implique dynamiquement la disjonction* $\mathbb{K}_1 \vee \mathbb{K}_2 \vee \ldots \vee \mathbb{K}_m$ lorsque, pour tout système de csg $\mathbb{H}$ portant sur des polynomes de $\mathbf{K}[\mathbf{X},\mathbf{Y}]$, on a la construction d'incompatibilité forte :

$\{\downarrow[\mathbb{K}_1(\mathbf{X}), \mathbb{H}(\mathbf{X},\mathbf{Y})]\downarrow$ et ... et $[\mathbb{K}_m(\mathbf{X}), \mathbb{H}(\mathbf{X},\mathbf{Y})]\}$ $\vdash_{\overline{cons}}$ $\downarrow[\mathbb{H}_1(\mathbf{X}), \mathbb{H}(\mathbf{X},\mathbf{Y})]\downarrow$

Nous noterons cette implication-disjonction dynamique par :

$$^\bullet(\ \mathbb{H}_1(\mathbf{X}) \Rightarrow [\mathbb{K}_1(\mathbf{X}) \vee \mathbb{K}_2(\mathbf{X}) \vee \ldots \vee \mathbb{K}_m(\mathbf{X})]\ )^\bullet.$$

Lorsque le système $\mathbb{H}_1$ est vide, nous utilisons la notation

$$^\bullet(\ \mathbb{K}_1(\mathbf{X}) \vee \mathbb{K}_2(\mathbf{X}) \vee \ldots \vee \mathbb{K}_m(\mathbf{X})\ )^\bullet.$$

Enfin, la notation :

$$^\bullet(\ [\mathbb{H}_1 \vee \mathbb{H}_2 \vee \ldots \vee \mathbb{H}_k] \Rightarrow [\mathbb{K}_1 \vee \mathbb{K}_2 \vee \ldots \vee \mathbb{K}_m]\ )^\bullet$$

signifie que chacune des implications-disjonctions dynamiques

$$^\bullet(\ \mathbb{H}_i(\mathbf{X}) \Rightarrow [\mathbb{K}_1(\mathbf{X}) \vee \mathbb{K}_2(\mathbf{X}) \vee \ldots \vee \mathbb{K}_m(\mathbf{X})]\ )^\bullet \quad (i = 1, \ldots, k)$$

est vérifiée

Exemples : La proposition 4 peut être relue comme affirmant les implications-disjonctions dynamiques suivantes :

$$^\bullet(\ Q \neq 0 \Rightarrow [Q > 0 \vee Q < 0]\ )^\bullet \quad (a)$$

$$^\bullet(\ Q \leq 0 \vee Q \geq 0\ )^\bullet \quad (a')$$

$$^\bullet(\ Q \geq 0 \Rightarrow [Q > 0 \vee Q = 0]\ )^\bullet \quad (b)$$

$$^\bullet(\ Q \neq 0 \vee Q = 0\ )^\bullet \quad (c)$$

$$^\bullet(\ Q > 0 \vee Q \leq 0)^\bullet \quad (d)$$

$$^\bullet(\ Q = 0 \vee Q > 0 \vee Q < 0\ )^\bullet \quad (e)$$

Remarque : Toute formule sans quantificateur de la théorie du premier ordre des anneaux totalement ordonnés dicrets à paramètres dans $\mathbf{K}$ est équivalente à une

formule en forme normale disjonctive et donc à une formule du type

$$\mathbb{K}_1(\mathbf{X}) \vee \mathbb{K}_2(\mathbf{X}) \vee \ldots \vee \mathbb{K}_m(\mathbf{X})$$

où les $\mathbb{K}_i(\mathbf{X})$ sont des systèmes de csg portant sur des polynomes de $\mathbf{K}[\mathbf{X}]$.
Les implications-disjonctions dynamiques consituent une forme de raisonnement purement «identité algébrique» concernant les formules sans quantificateur, où la logique a été évacuée au profit d'algorithmes de constructions d'identités algébriques.

Fonction-degré d'une implication-disjonction dynamique

Une implication-disjonction dynamique

$$^\bullet(\ \mathbb{H}_1(\mathbf{X}) \Rightarrow [\ \mathbb{K}_1(\mathbf{X}) \vee \mathbb{K}_2(\mathbf{X}) \vee \ldots \vee \mathbb{K}_m(\mathbf{X})\ ]\ )^\bullet$$

signifie par définition un algorithme fournissant la construction :

$$\{ \downarrow [\ \mathbb{K}_1(\mathbf{X}) \ ,\ \mathbb{H}(\mathbf{X},\mathbf{Y})\ ] \downarrow \text{et} \ldots \text{et} [\ \mathbb{K}_m(\mathbf{X})\ ,\ \mathbb{H}(\mathbf{X},\mathbf{Y})\ ]\ \} \quad \vdash_{\text{cons}} \quad \downarrow [\ \mathbb{H}_1(\mathbf{X})\ ,\ \mathbb{H}(\mathbf{X},\mathbf{Y})\ ] \downarrow$$

Chaque fois que nous établissons une implication dynamique particulière, nous devons établir des ‘majorations primitives récursives de degré’ pour cette construction d'incompatibilités fortes : le degré de l'incompatibilité forte construite est majoré par une fonction $\Delta(d_1,..,d_m)$ où d_i est le degré de l'incompatibilité forte initiale n°i.
Nous disons qu'il s'agit d'une fonction-degré acceptable pour l'implication-disjonction dynamique considérée.

En relisant les majorations de degré données à la proposition 4, on obtient des fonctions-degré acceptable pour les implications-disjonctions dynamiques données à l'exemple précédent.

La transitivité des implications-disjonctions dynamiques

L'énoncé le plus général est le suivant :
les implications-disjonctions dynamiques

$$^\bullet(\ [\ \mathbb{H}_1 \vee \mathbb{H}_2 \vee \ldots \vee \mathbb{H}_k\ ] \Rightarrow [\ \mathbb{K}_1 \vee \mathbb{K}_2 \vee \ldots \vee \mathbb{K}_m\ ]\ )^\bullet$$

et

$$^\bullet(\ [\ \mathbb{K}_1 \vee \mathbb{K}_2 \vee \ldots \vee \mathbb{K}_m\ ] \Rightarrow [\ \mathbb{L}_1 \vee \mathbb{L}_2 \vee \ldots \vee \mathbb{L}_n\ ]\ )^\bullet$$

impliquent :

$$^\bullet(\ [\ \mathbb{H}_1 \vee \mathbb{H}_2 \vee \ldots \vee \mathbb{H}_k\ ] \Rightarrow [\ \mathbb{L}_1 \vee \mathbb{L}_2 \vee \ldots \vee \mathbb{L}_n\ ]\ )^\bullet$$

Cette transitivité s'obtient en enchainant les algorithmes de constructions d'incompatibilités fortes. Les fonctions-degré résultantes s'obtiennent donc par composition convenable des fonctions-degré initiales.

On démontrerait pour les implications-disjonctions dynamiques le principe de substitution analogue à celui démontré pour les implications dynamiques, par la même méthode.

Cas avec une seule condition de signe

Proposition 10 : Supposons que dans une implication-disjonction dynamique

$$^\bullet(\ \ \mathbb{H}_1 \ \Rightarrow [\ \mathbb{K}_1 \vee \mathbb{K}_2 \vee \ldots \vee \mathbb{K}_m\ ]\ )^\bullet$$

chaque système $\mathbb{K}_i$ du second membre soit une seule condition de signe $Q_i\ \sigma_i\ 0$, et notons $Q_i\ \tau_i\ 0$ la condition de signe opposée.

Alors on a l'implication-disjonction dynamique :

$$\bullet(\quad \mathbb{H}_1(\mathbf{X}) \Rightarrow [\, Q_1\, \sigma_1\, 0 \vee Q_2\, \sigma_2\, 0 \vee \ldots \vee Q_m\, \sigma_m\, 0\,] \,)^\bullet \quad \text{(a)}$$

si et seulement si on a une incompatibilité forte :

$$\downarrow \mathbb{H}_1(\mathbf{X}) , Q_1\, \tau_1\, 0 , Q_2\, \tau_2\, 0 , \ldots, Q_m\, \tau_m\, 0 \downarrow \qquad \text{(b)}$$

On obtient sans difficulté les précisions suivantes concernant les degrés.
Si (a) est vérifié avec une fonction-degré acceptable $\Delta^1(d_1 , \ldots, d_m)$ et si chaque Q_i a pour degré δ_i alors on a une incompatibilité forte (b) de degré $\Delta^1(2.\delta_1 , \ldots, 2.\delta_m)$.
Si on a une incompatibilité forte (b) de degré δ, alors l'implication dynamique (a) admet pour fonction-degré acceptable :

$$(d_1 , \ldots, d_m) \mapsto \mu_4(d_1 , \mu_4(d_2 , \ldots, \mu_4(d_m , \delta)\ldots)$$

Variations sur le thème des implications dynamiques

Pour de nombreuses implications de base, on a des algorithmes plus rapides, et moins coûteux en degré, que celui donné en appliquant les propositions 7 et 8, lorsqu'on veut les traiter en implications dynamiques.

Implications triviales et implications simples

Définition 11 : (**implications triviales**)

Une implication $\mathbb{H}_1(\mathbf{X}) \Rightarrow \mathbb{H}_2(\mathbf{X})$ est dite triviale lorsque toute incompatibilité forte $\downarrow [\, \mathbb{H}_2(\mathbf{X}) , \mathbb{H}(\mathbf{X},\mathbf{Y}) \,] \downarrow$ fournit par simple relecture l'incompatibilité forte $\downarrow [\, \mathbb{H}_1(\mathbf{X}) , \mathbb{H}(\mathbf{X},\mathbf{Y}) \,] \downarrow$.
L'implication dynamique $\bullet(\mathbb{H}_1(\mathbf{X}) \Rightarrow \mathbb{H}_2(\mathbf{X}))^\bullet$ accepte alors pour fonction-degré : $\Delta_0(d) = d$.

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.
De même, l'implication $B = 0 \Rightarrow A.B = 0$ est triviale,
tandis que la contrapposée ne l'est pas.
On a aussi 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 12 : (**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 polynomes 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 polynomes 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 polynomes supposés > 0 (resp ≠ 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'implication dynamique correspondant à une implication simple donnée du type :

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

Dans l'incompatibilité forte :

$$\downarrow [\, \mathbb{H}(\mathbf{X},\mathbf{Y}) , T(\mathbf{X}) = 0 \,] \downarrow$$

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 :

$$\downarrow [\, \mathbb{H}(\mathbf{X},\mathbf{Y}) , \mathbb{H}_1(\mathbf{X}) \,] \downarrow \ .$$

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 13 : (implications simples en tant qu'implications dynamiques)

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-degré : $(d;\delta) \mapsto d + \delta$, où δ est le degré absolu de l'implication simple.

b) Une implication simple : $\mathbb{H}_1(\mathbf{X}) \Rightarrow T(\mathbf{X})\ \sigma\ 0$ accepte pour fonction-degré : $(d;\delta') \mapsto d.\delta'$, 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’. 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 :

Substitution 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-degré : $d \mapsto d.\delta'$.

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-degré $\Delta : d \mapsto d + \delta$.

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

Soit Q un polynome, 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 coutent rien :

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

Signalons enfin quelques implications, qui sans être des implications simples, sont d'un traitement “rapide” en tant qu'implications dynamiques :

Proposition 14 : (fonctions-degré de quelques implications particulières)

a) L'implication $[A > 0 , A.B \geq 0] \Rightarrow B \geq 0$ accepte pour fonction-degré : $(d;\delta) \mapsto d + 2.\delta$ 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-degré : $(d;\delta,\delta') \mapsto \sup(d.\delta', d + 2.\delta)$ 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-degré : $(d;\delta) \mapsto d + 2.\delta$ où $\delta = d(A.B)$.

d) L'implication $[A \geq 0 , A.B > 0] \Rightarrow B > 0$ accepte pour fonction-degré : $(d;\delta,\delta') \mapsto \sup(d.\delta', d + 2.\delta)$ 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-degré : $(d;\delta,\delta') \mapsto d.\delta' + 2\delta$ 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-degré : $(d;k) \mapsto 2k.d$

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

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

Par exemple 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.

Le principe de substitution

Proposition 15 :

On considère des variables $X_1,X_2,...,X_n$, $U_1,U_2,...,U_h$, $Z_1,Z_2,...,Z_k$, et des polynomes $P_1,P_2,...,P_n$ de $\mathbf{K}[\mathbf{Z}]$. Notons $\mathbf{P}(\mathbf{Z})$ pour $P_1(\mathbf{Z}), ..., P_n(\mathbf{Z})$.

Si on a $\quad {}^{\bullet}(\mathbb{H}_1(\mathbf{X},\mathbf{U}) \Rightarrow \mathbb{H}_2(\mathbf{X},\mathbf{U}))^{\bullet}$ (a)

alors on a aussi $\quad {}^{\bullet}(\mathbb{H}_1(\mathbf{P}(\mathbf{Z}),\mathbf{U}) \Rightarrow \mathbb{H}_2(\mathbf{P}(\mathbf{Z}),\mathbf{U}))^{\bullet}$ (b)

preuve>

Notons $\mathbf{X} = \mathbf{P}(\mathbf{Z})$ pour : $X_1 = P_1(\mathbf{Z}), ..., X_n = P_n(\mathbf{Z})$. Soient $Y_1,Y_2,...,Y_n$ des nouvelles variables.

Pour tout R figurant dans $\mathbb{H}_2(\mathbf{X},\mathbf{U})$ considérons l'égalité qui peut être obtenue par divisions successisves (les degrés des R_i sont tous inférieurs ou égaux au degré de R) :

$$R(\mathbf{X},\mathbf{U}) = R(\mathbf{Y},\mathbf{U}) + (X_1 - Y_1)\, R_1(\mathbf{X},\mathbf{Y},\mathbf{U}) + ... + (X_n - Y_n)\, R_n(\mathbf{X},\mathbf{Y},\mathbf{U}) \quad (1)$$

En substituant $P_i(\mathbf{Z})$ à Y_i on obtient une égalité :

$$R(\mathbf{P}(\mathbf{Z}),\mathbf{U}) = R(\mathbf{X},\mathbf{U}) + (X_1 - P_1(\mathbf{Z}))\, R_1(\mathbf{X},\mathbf{P}(\mathbf{Z}),\mathbf{U}) + ... + (X_n - P_n(\mathbf{Z}))\, R_n(\mathbf{X},\mathbf{P}(\mathbf{Z}),\mathbf{U}) \quad (2)$$

Ces égalités fournissent une implication simple :

$${}^{\bullet}([\, \mathbb{H}_2(\mathbf{X},\mathbf{U}) , \mathbf{X} = \mathbf{P}(\mathbf{Z}) \,] \Rightarrow \mathbb{H}_2(\mathbf{P}(\mathbf{Z}),\mathbf{U}))^{\bullet} \quad (3)$$

dont le degré ralatif est majoré par

$$\mu = \sup (1 , \sup\{\deg((X_i - P_i(\mathbf{Z}))\, R_i(\mathbf{X},\mathbf{P}(\mathbf{Z}),\mathbf{U}) / \deg(R(\mathbf{P}(\mathbf{Z}),\mathbf{U}))) ; \\ R \text{ figure dans } \mathbb{H}_2 \ , R(\mathbf{P}(\mathbf{Z}),\mathbf{U}) \neq \text{cte} \}$$

De la même manière, pour les R figurant dans $\mathbb{H}_1$ on a des égalités :

$$R(\mathbf{X},\mathbf{U}) = R(\mathbf{P}(\mathbf{Z}),\mathbf{U}) - (X_1 - P_1(\mathbf{Z}))\, R_1(\mathbf{X},\mathbf{P}(\mathbf{Z}),\mathbf{U}) - ... - (X_n - P_n(\mathbf{Z}))\, R_n(\mathbf{X},\mathbf{P}(\mathbf{Z}),\mathbf{U}) \quad (4)$$

qui fournissent une implication simple

$${}^{\bullet}([\, \mathbb{H}_1(\mathbf{P}(\mathbf{Z}),\mathbf{U}) , \mathbf{X} = \mathbf{P}(\mathbf{Z}) \,] \Rightarrow [\, \mathbb{H}_1(\mathbf{X},\mathbf{U}) , \mathbf{X} = \mathbf{P}(\mathbf{Z}) \,])^{\bullet} \quad (5)$$

dont le degré ralatif est majoré par

$$\lambda = \sup (1 , \sup\{\deg((X_i - P_i(\mathbf{Z}))\, R_i(\mathbf{X},\mathbf{P}(\mathbf{Z}),\mathbf{U})) / \deg((R\mathbf{X},\mathbf{U})) ;\ R \text{ figure dans } \mathbb{H}_1 \ \}$$

Par ailleurs l'implication dynamique :

$${}^{\bullet}([\, \mathbb{H}_1(\mathbf{X},\mathbf{U}) , \mathbf{X} = \mathbf{P}(\mathbf{Z}) \,] \Rightarrow [\, \mathbb{H}_2(\mathbf{X},\mathbf{U}) , \mathbf{X} = \mathbf{P}(\mathbf{Z}) \,])^{\bullet} \quad (6)$$

accepte la même fonction-degré que l'implication dynamique (a).

En composant (5), (6) et (3) on obtient :

$${}^{\bullet}([\, \mathbb{H}_1(\mathbf{P}(\mathbf{Z}),\mathbf{U}) , \mathbf{X} = \mathbf{P}(\mathbf{Z}) \,] \Rightarrow \mathbb{H}_2(\mathbf{P}(\mathbf{Z}),\mathbf{U}))^{\bullet} \quad (7)$$

Comme les variables $\mathbf{X}$ ne figurent pas dans $\mathbb{H}_1(\mathbf{P}(\mathbf{Z}),\mathbf{U})$, on a l'implication dynamique :

$${}^{\bullet}(\mathbb{H}_1(\mathbf{P}(\mathbf{Z}),\mathbf{U}) \Rightarrow [\, \mathbb{H}_1(\mathbf{P}(\mathbf{Z}),\mathbf{U}) , \mathbf{X} = \mathbf{P}(\mathbf{Z}) \,]))^{\bullet} \quad (8)$$

obtenue en remplaçant les X_i par les P_i dans l'incompatibilité forte initiale, et elle accepte pour fonction-degré : $d \mapsto d.\delta$ avec $\delta = \sup(\deg(P_i))$.

En résumé, si Δ^1 est une fonction-degré acceptable pour (a), une fonction-degré acceptable pour (b) est donc : $d \mapsto \lambda.\Delta^1(\mu.\delta.d)$ ❑

Formules de Taylor mixtes

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

Si $\deg(P) \leq 4$, on a les 8 formules de Taylor mixtes suivantes:

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

Comme toutes les combinaisons de signes possibles se présentent, on obtient : si u et v n'attribuent pas la même suite de signes pour un polynome P de degré $\leq$ 4 et ses dérivées successives, alors on a une identité algébrique 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 plus grand indice pour lequel les deux signes ne sont pas identiques

Plus généralement on a :

Proposition 16 : (formules 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.

Formules de Taylor généralisées (le lemme de Thom sous forme d'identités algébriques)

Le lemme de Thom affirme (entre autres) que l'ensemble des points où un polynome et ses dérivées successives ont chacun un signe fixé, est un intervalle. Une preuve facile, par récurrence sur le degré du polynome, est basée sur le théorème des accroissements finis. Nous pouvons, grâce aux formules de Taylor mixtes, traduire ce fait géométrique sous forme d'identités algébriques, que nous appellerons des **formules de Taylor généralisées**. Plutôt que de risquer un énoncé, nous donnons un exemple.

Un exemple : Considérons le polynome générique de degré 4

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

Considérons le système de conditions de signe portant sur le polynome P et ses dérivées successives par rapport à la variable X :

$\mathbb{H}(U)$: $P(U) > 0$, $P'(U) < 0$, $P^{(2)}(U) < 0$, $P^{(3)}(U) < 0$, $P^{(4)}(U) > 0$.

Considérons également le système de conditions de signe généralisées obtenues en relachant toutes les inégalités, sauf la dernière :

$\mathbb{H}'(U)$: $P(U) \geq 0$, $P'(U) \leq 0$, $P^{(2)}(U) \leq 0$, $P^{(3)}(U) \leq 0$, $P^{(4)}(U) > 0$.

Le lemme de Thom affirme (entre autres) :

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

Nous allons voir que ce fait géométrique est rendu évident par des identités algébriques.

On écrit les formules de Taylor mixtes suivantes :

$\alpha)$ $P^{(3)}(Z) = P^{(3)}(V) + P^{(4)}.(Z - V)$

$\beta)$ $P^{(2)}(Z) = P^{(2)}(U) + P^{(3)}(Z).(Z - U) - 1/2\ P^{(4)}.(Z - U)^2$

$\gamma)$ $P'(Z) = P'(U) + P^{(2)}(U).(Z - U) + 1/2\ P^{(3)}(Z).(Z - U)^2 - 1/3\ P^{(4)}.(Z - U)^3$

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

Posons $\boxed{\Delta_1 = Z - U\ ,\ \Delta_2 = V - Z}$

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

$$\beta') \qquad P^{(2)}(Z) = P^{(2)}(U) + P^{(3)}(V).\Delta_1 - P^{(4)}\ [\Delta_1.\Delta_2 + 1/2\ \Delta_1^2]$$

On obtient de la même manière, par substitutions :

$$\gamma') \qquad P'(Z) = P'(U) + P^{(2)}(U).\Delta_1 + 1/2\ P^{(3)}(V).\Delta_1^2 - P^{(4)}.[\Delta_1^2.\Delta_2/2 + \Delta_1^3/3]$$

et enfin

$$\begin{aligned}\delta')\ P(Z) \ = \ & P(V) - P'(U).\Delta_2 - P^{(2)}(U).[\Delta_1.\Delta_2 + 1/2\Delta_2^2] \\ & - P^{(3)}(V).[\ \Delta_1^2.\Delta_2/2 + \Delta_1.\Delta_2^2/2 + \Delta_2^3/6] \\ & + P^{(4)}.[\Delta_1^3.\Delta_2/3 + \Delta_1^2.\Delta_2^2/2 + \Delta_1.\Delta_2^3/2 + \Delta_2^4/8]\end{aligned}$$

Les égalités $\alpha)$, $\beta')$, $\gamma')$, $\delta')$ donnent l'implication cherchée sous forme d'une identité algébrique. La première est une formule de Taylor ordinaire portant sur le polynome $P^{(3)}$. Les trois dernières peuvent être vues comme des formules de Taylor généralisées portant sur les polynomes $P^{(2)}$, P' et P .

Plus généralement, on obtient:

Théorème 17 : (évidence forte du lemme de Thom)

Soit T une variable distincte des C_i . Soient $P \in \mathbf{K}[\mathbf{C}][T]$, de degré s en T , $\sigma_1, \sigma_2, ..., \sigma_s$ une liste formée de $<$ ou $>$. On note $\mathbb{H}(\mathbf{C},T)$ ou $\mathbb{H}(T)$ le système de csg : $P'(\mathbf{C},T)\ \sigma_1\ 0, ..., P^{(i)}(\mathbf{C},T)\ \sigma_i\ 0, ..., P^{(s)}(\mathbf{C},T)\ \sigma_s\ 0$ (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 : $P^{(s)}(\mathbf{C},T) > 0$, $P^{(i)}(\mathbf{C},T) \geq 0$, $i = 1, ..., s-1$.

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

On a alors les implications dynamiques suivantes :

$$\bullet\big(\ [\ \mathbb{H}'(U),\ \mathbb{H}'(V)\ ,\ U\ \sigma_1\ V\ ] \quad \Rightarrow \quad P(U) > P(V)\ \big)\bullet \qquad (a)$$

$$\bullet\big(\ [\ \mathbb{H}_1(U),\ V > U\ ] \quad \Rightarrow \quad P(V) > P(U)\ \big)\bullet \qquad (b)$$

$\bullet([\, \mathbb{H}'(U) , \mathbb{H}'(V) , \; U < Z < V \,] \;\Rightarrow\; \mathbb{H}(Z))\bullet$ (c)

Ce sont des implications simples qui ne coûtent rien.

preuve> L'implication dynamique (a) résulte de formules de Taylor mixtes. L'implication dynamique (b) résulte de la formule de Taylor ordinaire au point U. Les formules de Taylor généralisées établies pour l'implication dynamique (c) résultent des formules de Taylor mixtes. On constate qu'il s'agit d'implications simples qui ne coûtent rien (ceci parce que U, V, Z sont des variables et non des polynomes. ❑

4) Existences potentielles

Notations et définitions

Elles sont tout à fait analogues à celles données pour les implications dynamiques.

Définition et notation 18 :

Soient $\mathbb{H}_1$ un système de csg portant sur des polynomes de $\mathbf{K}[\mathbf{X}]$, $\mathbb{H}_2$ un système de csg portant sur des polynomes 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 polynomes de $\mathbf{K}[\mathbf{X},\mathbf{Y}]$, les variables Y_i et T_j étant deux à deux distinctes, on a la construction d'implication forte :

$\downarrow [\, \mathbb{H}_2(\mathbf{X},\mathbf{T}) , \mathbb{H}(\mathbf{X},\mathbf{Y})]\downarrow \;\; |\!\!-\!\!\!-_{\overline{cons}} \downarrow [\, \mathbb{H}_1(\mathbf{X}) , \mathbb{H}(\mathbf{X},\mathbf{Y})]\downarrow$.

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

Nous noterons cette existence potentielle par :

$\bullet(\;\; \mathbb{H}_1(\mathbf{X}) \Rightarrow \exists \;\; \mathbf{T} \;\; \mathbb{H}_2(\mathbf{X},\mathbf{T}) \;\;)\bullet$.

Lorsque le système $\mathbb{H}_1$ est vide, nous utilisons la notation $\bullet(\exists \;\; \mathbf{T} \;\; \mathbb{H}_2(\mathbf{X},\mathbf{T}))\bullet$.

La notion de fonction-degré acceptable pour une existence potentielle peut être elle aussi directement recopiée du cas des implications dynamiques.

Remarques :

1) La notion d'existence potentielle est une notion d'existence faible. L'existence potentielle signifie qu'il n'est pas grave de faire comme si les T_i existaient vraiment, parce que cela n'introduit pas de contradiction: on peut paraphraser la définition en disant :

pour construire l'incompatibilité forte $\downarrow [\, \mathbb{H}_1(\mathbf{X}) , \mathbb{H}(\mathbf{X},\mathbf{Y})]\downarrow$

il suffit d'avoir construit $\downarrow [\, \mathbb{H}_2(\mathbf{X},\mathbf{T}) , \mathbb{H}(\mathbf{X},\mathbf{Y})]\downarrow$

2) On pourrait étendre la définition de l'existence potentielle en remplaçant le système de csg $\mathbb{H}_2(\mathbf{X},\mathbf{T})$ par une disjonction de systèmes de csg, comme on a fait avec la notion d'implication-disjonction dynamique.

Quelques règles de manipulation des énoncés d'existence potentielle

La transitivité des existences potentielles est immédiate. Voici l'énoncé précisé en termes de fonctions-degré acceptables.

Théorème 19 : (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 $\mathbb{H}_3(\mathbf{X},\mathbf{T},\mathbf{U})$.

Les existences potentielles

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

impliquent l'existence potentielle :

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

Supposons que la première existence potentielle admette comme fonction-degré acceptable $\Delta^1(d;\mathbf{p})$ où d est le degré de l'incompatibilité forte $\downarrow [\ \mathbb{H}_2(\mathbf{X},\mathbf{T})\ ,\ \mathbb{H}(\mathbf{X},\mathbf{Y})\ ]\downarrow$ 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 fonction-degré acceptable $\Delta^2(d;\mathbf{q})$ pour la deuxième existence potentielle, alors une fonction-degré pour l'existence potentielle construite est donnée par :

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

Voici maintenant un énoncé précis correspondant aux preuves cas par cas d'une existence potentielle.

Proposition 20 : (raisonnement cas par cas)

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

i) Si Δ^i (i = 1,2,3) sont les trois fonctions-degré des existences potentielles supposées, une fonction-degré pour l'existence potentielle déduite est donnée par : $\Delta = \mu_{4,e}\ o\ (\Delta^1,\Delta^2,\Delta^3)$

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

$$\Delta = \mu_{4,c}\ o\ (\Delta^1,\Delta^2) = \Delta^1.\Delta^2$$

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

$$\Delta = \mu_{4,d}\ o\ (\Delta^1,\Delta^2) = \Delta^1.\Delta^2 + \Delta^2$$

iv) Enfin, dans le cas où on démontre une existence potentielle cas par cas

avec deux signes généralisés $\geq$ et $\leq$ on obtient :

$$\Delta = \mu_{4,a} \circ (\Delta^1,\Delta^2) = \Delta^1 + \Delta^2$$

Le principe de substitution pour les existences potentielles se démontre comme pour les implications dynamiques.

Un autre principe utile est le fait que l'existence implique l'existence potentielle. Il s'obtient facilement : on remplace les variables T_i «existentielles» par les polynomes concrets P_i qui réalisent l'existence. On reconnait là une analogie formelle avec la règle d'introduction du quantificateur existentiel en calcul naturel par exemple.

Proposition 21 : (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 : $\dot{(}\ \mathbb{H}_2(\mathbf{X},\mathbf{P}(\mathbf{X})) \Rightarrow \exists\ \mathbf{T}\ \mathbb{H}_2(\mathbf{X},\mathbf{T})\ \dot{)}$.

Si δ majore les degrés des P_i , l'existence potentielle accepte pour fonction-degré : $(d;\delta) \mapsto d.\sup(1,\delta)$

Corollaire : (mêmes hypothèses)

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

Si Δ^1 est une fonction-degré acceptable pour l'implication forte de l'hypothèse, une fonction-degré acceptable pour la conclusion est donnée par : $\Delta = \Delta^1(d.\sup(1,\delta))$ où δ majore les degrés des P_i .

Existences potentielles fondamentales

On sait démontrer les existences potentielles correspondant aux deux axiomes existentiels de la théorie des corps réels clos.

Théorème 22 : (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:

$$\dot{(}\ U \neq 0 \Rightarrow \exists\, T \quad 1 = U.T\ \dot{)}$$

Soit δ le degré de U, une fonction-degré acceptable pour l'existence potentielle est $\Delta_{22}(d;\delta) = d + d.\delta + \delta$

Remarque: La preuve de cette existence potentielle recopie ce qu'on fait, dans la preuve du théorème des zéros de Hilbert, pour passer du théorème des zéros faible au théorème des zéros général (par exemple dans l'exposé classique de Van der Warden). La notion d'existence potentielle de l'inverse d'un non nul est donc en filigrane dans les classiques.

Théorème 23 : (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 polynome change de signe. Ce qui s'écrit, en notant P(U) pour P(X,U) :

$$\dot{(}\ [\, P(U).P(V) < 0\,,\ U < V\ ] \Rightarrow \exists\, Z\ [\, P(Z) = 0\,,\ U < Z < V\ ]\ \dot{)}$$

Et une fonction-degré acceptable est donnée par :

$$\Delta_{23}(d;\delta,s) = \left((2d+7)\,(\delta+1) \right)^{\gamma'(s)} \quad \text{où} \quad \gamma'(s) = 2^{(s+2)^2/2}$$

Remarque : La preuve du théorème précédent "recopie" la preuve classique, par récurrence sur le degré du polynome P, du théorème «si un corps est ordonné et si $P(u).P(v) < 0$ avec P irréductible, alors le corps $\mathbf{K}[W]/P(W)$ est réel». Ceci donne l'existence potentielle d'une racine. Pour avoir la racine sur l'intervalle, il y a de nouveau une récurrence à faire. Tout ceci conduit à une relativement mauvaise fonction-degré. Le problème semble difficile à contourner. Dans le cas complexe (théorème des zéros de Hilbert), l'existence potentielle d'une racine d'un polynome non constant est au contraire extrêmement simple (si le polynome P est unitaire, il suffit de tout réduire modulo P) et conduit à une fonction-degré tout à fait raisonnable.

5) Majorations finales

Tableaux de Hörmander

Nous donnons ici quelques majorations directement liées à l'algorithme de Hörmander lui-même.

Proposition 24 : (Tableau de Hörmander pour des polynomes en une variable)

Soit $\mathbf{K}$ un corps ordonné, sous-corps d'un corps réel clos $\mathbf{R}$.

Soit $L = [P_1, P_2, ..., P_k]$ une liste de polynomes de $\mathbf{K}[Y]$.

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

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

Si s majore les degrés des P_i, le nombre de coefficients d'éléments de $\mathcal{P}$, et donc aussi le nombre de points du tableau de Hörmander est majoré par :

$\Lambda_{24}(s,k) = (k+1)^{2^s}$

L'algorithme de Hörmander traite des polynomes en n variables, en éliminant chaque variable l'une après l'autre. A chaque élimination d'une variable, le nombre de polynomes à considérer et leurs degrés croissent de manière impressionnante. Ceci est précisé dans la proposition suivante :

Proposition 25 : (Tableau de Hörmander paramétré)

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 polynomes de $\mathbf{K}[X_1, X_2, ..., X_n][Y]$.

On peut construire une famille finie $\mathcal{F}$ de polynomes 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 polynomes 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 polynome de G et de chaque pseudo-division est majoré par : $\mu_{25}(\delta,s) = \delta.(s+1)!$, sauf si $n = 0$ (donc $\delta = 0$) et alors $\mu_{25}(0,s) = s$.
le nombre d'éléments de la famille G est majoré par : $\Lambda_{25}(s,k) = (k+1)^{2^s}$

Mené jusqu'au bout, cet algorithme produit donc une explosion de degrés obtenue en itérant n–1 fois (n étant le nombre de variables) la fonction $s \mapsto s!$. Ceci conduit à la majoration finale.

Nullstellensatz, positivestellensatz et nichtnegativestellensatz réels effectifs

Théorème 26 : 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 polynomes 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 $\downarrow \mathbb{H}(X_1,X_2,...,X_n) \downarrow$ (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 : $\downarrow \mathbb{H}(X_1,X_2,...,X_n) \downarrow$ (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 $\downarrow \mathbb{H}(X_1,X_2,...,X_n) \downarrow$ (dans **K**) de degré majoré par $\mu_{26}(d,k,n)$ qui est donné par la tour d'exponentielle à n+4 étages

$$2^{2^{\cdot^{\cdot^{\cdot^{\cdot^{d.\lg(d)+\lg\lg(k)+cte}}}}}}$$

Remarque : La principale cause d'explosion des degrés dans la majoration finale actuelle réside dans l'utilisation de l'algorithme de Hörmander.
On peut donc espérer améliorer sensiblement ces majorations en se basant sur d'autres preuves, élémentaires mais moins longues, d'incompatibilité.

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

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

[Lom b] Lombardi H. : Effective real nullstellensatz and variants, in «MEGA 90», mai 1991, chez Birkhaüser. (Version anglaise plus courte)

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

[Lom d] Lombardi H.: Théorème effectif des zéros réel et variantes, avec une majoration explicite des degrés. 1990. Mémoire d'habilitation.

[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» in «MEGA 90», mai 1991, chez Birkhaüser.

[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 semi-algebraic geometry. Math. Ann. 207, 87-97 (1974)