Reprint de la première partie de

Mémoire présenté en vue de l'Habilitation à diriger des Recherches

présenté en Novembre 1990
à l'Université de Nice

Henri LOMBARDI

Laboratoire de Mathématiques
UFR des Sciences et Techniques
Université de Franche-Comté
25030 BESANCON
FRANCE
Tel 81 66 63 40

Email : TDNBESAC@FRGREN81

ALGEBRE REELLE DISCRETE

Une étude historique sur les problèmes d'effectivité en algèbre réelle.
(1990. Mémoire d'habilitation.)

En collaboration avec : Gonzalez L., Recio T., Roy M.F.:
Spécialisation de la suite de Sturm et sous-résultants. I et II .
(1989 . A paraître au RAIRO : Journal d'Informatique Théorique)

En collaboration avec Roy M.-F. :
Théorie constructive élémentaire des corps ordonnés.
(A paraître aux Publications Mathématiques de Besançon. 1990)

Théorème effectif des zéros réel et variantes (avec une majoration explicite des degrés).
(1990. Mémoire d'habilitation)

Une étude historique sur les problèmes d'effectivité en algèbre réelle

UNE ETUDE HISTORIQUE SUR LES PROBLEMES D'EFFECTIVITE EN ALGEBRE REELLE

Henri LOMBARDI

Introduction

L'effectivité en algèbre réelle a une longue histoire, qui s'est considérablement accélérée dans les quinze dernières années. Nous nous proposons dans cet article d'en retracer quelques étapes essentielles. Nous discuterons cependant peu les questions de complexité, qui sont l'enjeu de nombreux travaux actuels. Nous préférons en effet discuter plus en détail des problèmes d'effectivité du point de vue des mathématiques constructives, dans l'espoir de convaincre le lecteur de l'utilité de cette démarche générale. Nous supposons le lecteur familier avec la théorie d'Artin-Schreier, le 17ème problème de Hilbert et le théorème des zéros réel, ainsi qu'avec quelques définitions et résultats de base de la logique mathématique.

Nous citons maintenant les étapes marquantes, selon nous, de cette histoire.

Le premier succès marquant en algèbre réelle effective a été le théorème de Sturm ([Stu]), qui donne un algorithme explicite pour calculer le nombre de racines réelles d'un polynôme sur un intervalle, ceci uniquement par des calculs dans le corps des coefficients du problème. Sylvester a ensuite amélioré la méthode de Sturm ([Syl]). Bien qu'il ne formule pas le résultat de manière explicite, sa méthode permet de calculer dans la clôture réelle du corps des coefficients d'une famille de polynômes donnée (polynômes en une variable).
Mais après ces premiers succès, un grand vide.

En 1900, Hilbert formule une séries de problèmes illustres, dont le 17ème : un polynôme réel en plusieurs variables qui est partout positif ou nul, peut-il toujours s'écrire comme somme de carrés de fractions rationnelles ?
Une solution hautement non constructive, avec intervention lourde de l'axiome du choix, est fournie par Artin-Schreier, à travers la théorie des corps formellement réels (on dit aujourd'hui : corps réel). Leur théorie est un énorme marteau pour enfoncer un clou de taille moyenne. Néanmoins, la puissance de la méthode impressionne, et elle dominera longtemps : les grands théorèmes d'existence en algèbre seront systématiquement prouvés par le théorème de Zorn, et on s'intéressera bien peu, pendant longtemps, aux méthodes plus explicites, parce que trop laborieuses. Un théorème essentiel qui fait tenir debout la théorie d'Artin-Schreier est qu'un corps réel peut être ordonné. Ce théorème, connu comme hautement non constructif, et semblant incontournable, a longtemps découragé les tentatives de fournir une version effective de la théorie.

En 1941, la thèse de Hollkott ([Hol]), passée inaperçue, donne une preuve constructive de l'existence de la clôture réelle pour un corps ordonné discret (c.-à-d. où les lois de composition et le signe d'un élément sont donnés de manière explicite).

En 1951, A. Tarski ([Tar]) publie le résultat (annoncé en 31) fondamental de complétude et décidabilité de la théorie formelle des corps réels clos, en généralisant la méthode de Sturm.
En 1954, A. Seidenberg ([Sei]) propose une preuve "géométrique" du même résultat.

En 1955, A. Robinson ([Rob]) donne une solution récursive (mais pas entièrement constructive) du 17ème problème de Hilbert, basée sur le théorème de Tarski.
En 1957, G. Kreisel ([Kre1]) publie une idée de preuve du même résultat, qui cette fois-ci fournit un algorithme primitif récursif, et qui est constructive (pour autant qu'il n'y ait pas de trou dans la preuve). Ce résultat, combiné avec celui de Hollkott, donne donc la version constructive de la théorie d'Artin-Schreier, pour le cas des corps ordonnés discrets.

Les problèmes de complexité des calculs concernant les ensembles semi-algébriques définis sur $\mathbb{Q}$ sont abordés systématiquement par Collins en 1975 ([Col]) et ont fait l'objet de nombreux travaux depuis.

En 1964, Krivine donne un premier théorème des zéros réels ([Kri]).

En 1974, G. Stengle publie le théorème des zéros réel dans sa forme la plus générale ([Ste]), mais sans preuve constructive.

En 1981, C. Delzell, s'appuyant sur le théorème de Stengle construit une solution continue pour le 17ème problème de Hilbert. C'est, à peu de chose près, la solution constructive du problème dans le cas de polynômes à coefficients réels. Il est remarquable qu'après la solution constructive du théorème fondamental de l'algèbre par Brouwer dans les années 20, il ait fallu attendre jusqu'en 1981 la solution constructive d'un problème non trivial d'algèbre réelle lorsque les coefficients sont des nombres réels généraux et non des réels algébriques. Il est également significatif que ce travail ait eu lieu sous l'impulsion de Kreisel.

En 1989 enfin, après avoir reconstruit le résultat de Hollkott, avec M-F Roy ([LR]), nous donnons une solution constructive du théorème de Stengle ([Lom]), pour le cas des corps ordonnés discrets. Ce résultat permet notamment de rendre le travail de Delzell entièrement constructif.

pour autant qu'il n'y a pas de trou dans la preuve!

1) Algèbre réelle discrète (théorie des corps ordonnés discrets)

Précisions concernant la terminologie, et quelques résultats classiques

Lorsqu'on discute de problèmes d'effectivité, il faut d'abord bien s'entendre sur la nature des objets qu'on manipule. L'algèbre réelle concerne les problèmes liés aux polynômes à coefficients réels. Plus généralement, nous parlons de corps ordonnés et de polynômes à coefficients dans ces corps. Mais du point de vue des calculs effectifs, la situation n'est pas du tout la même si on considère tous les nombres réels "classiques", ou si on considère seulement les nombres réels "effectivement construits" (c.-à-d. limites de suites de Cauchy explicitement calculables et explicitement convergentes), ou encore si on se limite aux nombres réels algébriques (racines de polynômes à coefficients entiers).
Pour y voir clair le mieux est de préciser d'une part les théories formelles considérées, d'une part, la sémantique utilisée d'autre part.

Théories formelles

Préliminaire
Toutes les théories formelles que nous considérons sont basées sur le calcul des prédicats du premier ordre, classique ou intuitionniste.
On rappelle que le calcul des prédicats classiques peut être identifié à un fragment du calcul des prédicats intuitionniste : chaque prédicat n'est utilisé que précédé d'une double négation, les seuls connecteurs logiques utilisés sont $\neg$ et $\wedge$ et le seul quantificateur utilisé est $\forall$. Une formule de ce fragment est démontrable intuitionnistiquement si et seulement si elle l'est classiquement. Et toute formule classique est classiquement équivalente à une formule du fragment. L'inconvénient majeur est le très faible contenu sémantique constructif des formules du fragment.
En outre au moment de la formalisation d'une théorie mathématique, il y a en général des divergences d'opinion (notamment entre mathématiciens classiques et constructifs, mais pas seulement) sur les axiomes, prédicats et symboles fonctionnels à choisir pour traduire la pratique concrète.
Ici, nous précisons diverses théories formelles rendant compte des diverses notions de corps ordonnés, (et non à des théories formelles à prétentions "totalisantes" telle que ZFC (théorie des ensembles avec axiome du choix)), ceci dans le but de rendre clair quelles structures nous étudions et de quel point de vue.

Théories intuitionnistes
Théorie intuitionniste des corps ordonnés discrets : notée $\mathbf{COD_I}$. On peut prendre pour axiomes ceux des corps ordonnés, en rajoutant un axiome précisant que l'ordre est discret :

$x > 0$ ou $x = 0$ ou $x < 0$

Théorie intuitionniste des corps réels discrets. Les axiomes sont, outre ceux des corps, les axiomes de réalité :

1 + une somme de carrés = 0 est absurde

(il faut un axiome pour chaque "longueur" de somme)
et l'axiome correspondant au caractère discret du corps :

$x \neq 0$ ou $x = 0$

On note cette théorie $\mathbf{CRD}$

Théorie intuitionniste des corps ordonnés réels clos discrets. Obtenue à partir de $\mathbf{COD_i}$ en rajoutant les axiomes correspondant à :

un polynôme qui change de signe sur un intervalle possède une racine sur l'intervalle

(il faut un axiome pour chaque degré). Nous notons la théorie $\mathbf{CORCD_i}$.

Cette théorie possède un algorithme d'élimination des quantificateurs. La théorie est complète, en particulier, pour toute formule F , on a le théorème " F ∨ ¬F ". (cf. par exemple [LR]).

Théorie intuitionniste des corps réels clos discrets. Elle est obtenue à partir de $\mathbf{CRD_i}$ en rajoutant les axiomes correspondant à :

tout carré est une puissance 4

un polynôme de degré impair possède une racine

Le premier des axiomes cités ci-dessus équivaut à : pour tout x, x ou –x est un carré.

Nous notons la théorie $\mathbf{CRCD_i}$. Cette théorie est "équivalente" à la théorie $\mathbf{CORCD_i}$. (cf. par exemple [LR] pour une preuve constructive).

En outre, chaque fois que nous avons un modèle constructif (cf. le paragraphe "sémantiques") **K** pour l'une de ces théories formelles **T** , nous pouvons considérer les théories **T'(K)** , (avec **T'** contenant le symbole < si **K** est ordonné) où chaque élément de **K** est rajouté comme constante de la théorie formelle, et où sont rajoutés les axiomes (concernant ces constantes) qui explicitent la structure de **K** .

Les théories formelles classiques correspondantes : $\mathbf{CO_c}$, $\mathbf{CR_c}$, $\mathbf{CORC_c}$, $\mathbf{CRC_c}$ (pour lesquelles le caractère discret relève du tiers exclu).

Sémantiques

La sémantique concerne d'une part l'interprétation des symboles logiques (connecteurs et quantificateurs), d'autre part l'interprétation des symboles non logiques (variables, constantes, prédicats, symboles de fonction). Nous nous étendrons peu sur la première partie. Les régles de la logique intuitionniste vérifient ce qu'il faut pour que tout théorème ait une interprétation sous forme d'une construction, le plus immédiatement sensible étant que tout objet "démontré exister" peut être construit selon une procédure directement reliée à la preuve d'existence. Les règles de la logique classique, a contrario, répondent à une notion de vérité purement abstraite dans un univers "à la Zermelo-Frankel" supposé exister au moins de manière idéale, conformément à la philosophie du "réalisme platonicien"[1].

Voyons maintenant la question de l'interprétation des symboles non logiques, ou "théorie des modèles".

Du point de vue classique, un modèle d'une théorie formelle est fournie par : un ensemble (domaine du modèle) qui est le domaine des variables (les quantifications sont relatives à ce domaine), et une interprétation pour chaque constante, chaque symbole de fonction, chaque prédicat. Un symbole de fonction est interprété par une fonction au sens de la théorie des ensembles (un graphe fonctionnel, arbitraire) n'impliquant aucune procédure de calcul explicite. Si le modèle considéré par le mathématicien classique est trop sophistiqué, il est possible qu'aucune sémantique constructive ne puisse y faire face (pour le moment du moins) : voir à ce sujet la difficulté à fonder constructivement l'analyse non standard, malgré une heuristique constructive de cette théorie (cf. [HR]).

Du point de vue constructif, le domaine de définition doit être "construit", et les symboles de fonctions sont toujours interprétés comme représentant des fonctions calculables.

Cependant les notions de construction, d'effectivité ou de calculabilité sont des notions

---

[1] Quant à ceux qui se réfugient derrière une position formaliste "voici des jeux particulièrement amusants, ne cherchons surtout pas à les interpréter dans une réalité

premières non définies.
On peut donner une interprétation constructive pour le point de vue classique concernant les fonctions en considérant simplement que le résultat du calcul peut être fourni par un oracle.
Ainsi, à tout théorème de mathématiques constructives correspond "sa signification concrète" qui est un algorithme récursif à oracles[2]. Ceci permet de comprendre comment les théorèmes de mathématiques constructives peuvent s'appliquer même dans des contextes non constructifs. Le plus souvent (en fait dans toutes les mathématiques couramment pratiquées) l'algorithme est uniformément primitif récursif, c.-à-d. a une structure globale indépendante des réponses des oracles et n'utilise comme boucles que des boucles **Répéter** (éventuellement emboîtées) où le nombre d'itérations est calculé avant l'exécution de la boucle. Le mot uniformément fait allusion à la structure de l'algorithme, qui ne dépend pas des réponses des oracles questionnés en cours de route, et qui est donc "uniforme".

La courte discussion précédente aura peut-être convaincu (à tort selon nous) le lecteur classique, que la calculabilité des mathématiciens constructifs est au fond identique à la notion classique de récursivité.
Mais,

- d'une part, le mathématicien constructif n'exclut pas en principe l'existence d'algorithmes effectifs quoique non récursifs (la récursivité est l'effectivité "mécanique"),
- d'autre part, le fait qu'un algorithme est récursif (et pas seulement partiellement récursif) sous entend qu'il aboutit toujours à un résultat, or le $\forall\ \exists$ sous-jacent à cette phrase demande déjà pour être interprété une notion d'effectivité a priori lorsqu'on n'adhère pas au réalisme platonicien (actuellement très majoritaire) selon lequel un Univers idéal à la Zermelo-Frankel existe bel et bien,
- enfin, contrairement à la sémantique classique, où un algorithme récursif à oracles peut être prouvé exister par des moyens purement idéaux, les méthodes constructives excluent par avance une telle preuve, et tout algorithme prouvé constructivement est implicitement écrit (avec la preuve de sa convergence) dans la preuve, donc arrive avec une complexité limitée a priori[3].

Analyse de la théorie d'Artin-Schreier telle qu'exposée dans Van der Waerden (2ème édition anglaise de Modern Algebra)

Dans la seconde édition de 'Modern Algebra' ([VdW]), Van der Waerden n'utilise pratiquement pas l'axiome du choix, et se limite à l'utilisation de choix dénombrables en cascade (l'analogue formel est l'axiome du choix dépendant, accepté par à peu près tout le monde). Dans la préface, il justifie cette approche en estimant que l'axiome du choix est un élément étranger à l'algèbre,

---

2 Nous nous situons dans la lignée de Bishop. C'est le point de vue constructif minimal, qui a l'avantage de ne jamais entrer en contradiction flagrante, ni avec les mathématiques classiques, ni avec les différentes autres variantes de mathématiques constructives. Une discussion impliquant les principaux courants des mathématiques constructives alourdirait beaucoup trop notre exposé. On consultera [BR] pour un exposé "fulgurant" des principaux points de vue constructifs, ou [Bee] pour un exposé très détaillé.

3 Par exemple le théorème des zéros réel général de Stengle implique classiquement l'existence d'un algorithme récursif explicitant l'identité algébrique cherchée et qui aboutit toujours : essayer toutes les écritures possibles dans le corps des coefficients jusqu'à tomber sur une identité algébrique du type voulu. Cette preuve non constructive fournit un algorithme, mais de complexité inconnaissable.
Un autre exemple, plus dramatique, est lorsqu'on démontre classiquement l'existence d'un algorithme récursif, mais qu'il n'y aura jamais de méthode constructive pour trouver l'algorithme : c'est par exemple le cas du 'théorème' « tout réel présenté récursivement à la Cauchy peut être présenté récursivement à la Dedekind », mais l'algorithme dans la conclusion dépend du fait de savoir si le réel est rationnel ou irrationnel, fait qui ne

et en remarquant que l'algèbre 'dénombrable' est en général suffisante pour les besoins mathématiques.

Van der Waerden démontre l'existence de la *clôture algébrique* seulement pour les corps dénombrables. La clôture algébrique est obtenue en énumérant les polynômes à coefficients dans le corps et en rajoutant leurs racines au fur et à mesure (p. 194-195). Néanmoins cette solution n'est pas entièrement constructive dans la mesure où les choix en cascade exigent, à chaque fois, de factoriser le polynôme considéré dans l'extension précédemment construite. Ce qui n'est pas toujours faisable par un algorithme. Cette construction peut cependant fonctionner de manière entièrement satisfaisante dans un corps dénombrable de caractéristique nulle où les polynômes sont décomposables en facteurs premiers. Ce travail est réalisé dans la section 42, p. 134-137 (the field-theoretical operations in a finite number of steps).

On sait aujourd'hui qu'il est possible de donner une construction d'une clôture algébrique dans le cas général d'un corps dénombrable discret. Il faut cependant beaucoup plus se fatiguer, et il n'est en outre pas toujours possible de construire un isomorphisme entre deux clôtures algébriques obtenues à partir de deux énumérations distinctes du corps (cf. [MRR])[4].

Pour obtenir une *clôture réelle* d'un corps réel dans le cas dénombrable, Van der Waerden énumère la clôture algébrique, et rajoute au corps de départ des éléments de la clôture algébrique, en les testant les uns après les autres, en imposant à chaque étape que l'extension reste réelle. Il semble impossible de rendre cette 'construction' vraiment effective parce qu'on ne voit absolument pas comment le critère de réalité (savoir décider si un élément est ou non une somme de carrés) pourrait passer d'une extension à la suivante (alors que pour la factorisabilité des polynômes, ça marche au moins en caractéristique zéro).
Curieusement (pour nous), Van der Waerden, p 232., estime que cette 'construction', quand elle est utilisée pour obtenir une clôture réelle de $\mathbb{Q}$, est plus satisfaisante que la prise en considération directe des nombres réels algébriques, qui, dit-il, réclame «a transcendantal detour» (un détour transcendant par $\mathbb{R}$). Ainsi, il situe le hiatus entre construction satisfaisante ou insatisfaisante d'une clôture réelle à l'endroit «dénombrable / non dénombrable»[5], alors qu'il faut le situer à l'endroit «corps réel / corps ordonné».
Remarquons pour terminer que Van der Waerden ne mentionne pas que l'existence et unicité de la clôture réelle d'un corps *ordonné* dans le cas dénombrable implique, sans recours à l'axiome du choix, l'existence et unicité dans le cas général[6] puisqu'il n'y a aucun choix à opérer pour recoller entre elles les clôtures réelles des sous-corps de type fini du corps considéré. Cet "oubli" est bien entendu cohérent avec le fait signalé ci-dessus : son extrême réticence à l'égard du non dénombrable.

Une étude détaillée sur le problème de la clôture réelle dans la théorie des ensembles classique sans axiome du choix est faite par T. Sander ([Sa]). Notre travail ([LR]) est dans un cadre différent : nos méthodes sont entièrement constructives, (et en outre sans recours à aucun

---

4 Une contrepartie formelle classique de ce phénomène est l'impossibilité de prouver l'existence de la clôture algébrique d'un corps dénombrable dans la théorie des ensembles classiques sans aucun axiome de choix dénombrable (cf. [Sa]).

5 D'un point de vue constructif, l'infini est une notion purement négative. La comparaison entre $\mathbb{N}$ et $\mathbb{R}$ est alors une comparaison, non de la grandeur de deux objets insaisissables, mais de la complexité logique des constructions qu'ils impliquent. Ainsi un détour par $\mathbb{R}$ pour démontrer un théorème concernant un infini dénombrable n'est en fait bien souvent rien d'autre qu'un détour par des énoncés du type $\forall\,\exists$ portant sur des entiers naturels. Ce serait le cas ici. De toute manière, quoique plus compliqué que $\mathbb{N}$, l'infini $\mathbb{R}$ peut être traité de manière constructive comme l'a montré Bishop (cf. [BB]).

choix, même dénombrable), mais nous ne discutons pas la question de ce qui pourrait être cohérent avec ZF à condition de nier l'axiome du choix dénombrable.

Sturm et Sylvester : comment calculer dans la clôture réelle du corps des coefficients

Dans la théorie d'Artin-Schreier, le théorème de Sturm joue un rôle marginal (cf [VdW]) et sert seulement à démontrer l'unicité, à **K**-isomorphisme unique près, de la clôture réelle d'un corps ordonné **K** . Néanmoins, la preuve d'unicité donnée dans [VdW] utilise la factorisation d'un polynôme dans **K**[X] et n'est donc pas entièrement constructive.
En fait les théorèmes de Sturm et Sturm-Sylvester permettent de calculer dans la clôture réelle de **K** sans jamais avoir à calculer de factorisation de polynômes. Nous expliquons maintenant rapidement comment. (cf. [BKR], [CR], [GLRR] pour plus de détails) .
Le théorème de Sturm-Sylvester permet en effet de calculer le nombre de racines d'un polynôme P rendant un polynôme $Q > 0$ sur un intervalle donné.
A partir de là, et vu le lemme de Thom, on arrive à calculer le signe de $Q(\xi)$ si ξ est une racine de P spécifiée à la Thom :
Soient $P, Q_1, Q_2, \ldots, Q_n$ des polynômes de **K**[X] , $[\sigma_1, \sigma_2, \ldots, \sigma_n]$ une liste de signes stricts. Supposons que **K** possède une clôture réelle **R** . On peut déterminer le nombre de racines de P (dans **R**) qui attribuent les signes $\sigma_1, \sigma_2, \ldots, \sigma_n$ aux polynômes $Q_1, Q_2, \ldots, Q_n$ de la manière suivante : on considère la famille des polynômes R_i formée des 3^n produits de Q_j pris à la puissance 0, 1 ou 2 . Puis on calcule pour chaque R_i le nombre de racines de P rendant R_i positif, le nombre de racines de P rendant R_i négatif et le nombre de racines de P rendant R_i nul. Enfin, on en déduit $\sigma_1, \sigma_2, \ldots, \sigma_n$ en résolvant un système linéaire (en fait on peut se ramener à un calcul nettement plus court). Ceci donne en particulier un test dans **K** pour savoir s'il existe une racine de P dans **R** vérifiant un codage à la Thom particulier, puis pour calculer le signe de $Q(\xi)$ si ξ est une racine de P dans **R** codée à la Thom dans **K** . Donc on sait calculer dans l'extension ordonnée **K**[ξ] de **K** . En itérant le processus, on peut calculer dans la clôture réelle de **K** . Signalons que l'utilisation du lemme de Thom simplifie l'exposé et abaisse la complexité du calcul, mais n'est pas indispensable, puisqu'une racine de P peut aussi être spécifiée comme unique racine sur un intervalle construit avec les racines de P'.

Tarski, Seidenberg, Cohen : comment décider tous les problèmes du premier ordre en algèbre réelle discrète

Le travail de Tarski et ses retombées. Tarski ([Tar] 1951, annoncé en 1931) se base sur les idées de Sturm et Sylvester. Il donne un algorithme qui transforme toute formule du premier ordre (pour la théorie $\mathbf{CORC_c}$) en une formule sans quantificateur équivalente. Les termes du langage des corps ordonnés sont tous égaux à des polynômes en plusieurs variables. Les formules sans quantificateur de cette théorie, ramenées sous forme normale sont donc équivalentes à des disjonctions de «systèmes de conditions de signes portant sur des polynômes en plusieurs variables». Le problème de l'élimination des quantificateurs se ramène alors au problème de l'élimination d'un quantificateur existentiel devant un système de conditions de signes portant sur des polynômes en plusieurs variables.
La méthode de Tarski est en fait très naturelle : le théorème de Sturm permet d'éliminer un quantificateur existentiel devant une égalité à 0 , une généralisation du théorème de Sturm permet d'éliminer un quantificateur existentiel devant un système de conditions de signes

un nombre de variations de signes calculé à partir de la suite des restes "à la Sturm" initialisée avec deux polynômes P et S arbitraires (au lieu des polynômes P et P' dans l'algorithme classique de Sturm).
La portée de la méthode de Tarski, le principe de transfert qu'elle implique, son applicabilité à des corps réels clos non archimédiens, n'ont cependant pas été rapidement assimilés par les algébristes (à l'exception de Seidenberg).
Du point de vue algorithmique, Hörmander ([Hör], 1983) propose une méthode au fond analogue à celle de Tarski, mais d'une simplicité conceptuelle remarquable (cf. la preuve du principe de Tarski-Seidenberg dans [BCR] chap. 1). Le prix à payer est une plus grande complexité en temps et en espace. Le théorème de Sturm extrait en effet quelques informations pertinentes d'un énorme tableau de Hörmander : bénéfice, élégance et rapidité, contrepartie, moins grande lisibilité de "ce qui se passe en fait".
Du point de vue de la complexité, on a mis beaucoup de temps à s'apercevoir que la méthode de Tarski pouvait être la base d'algorithmes au fond pas si mauvais que cela (cf. [BKR] et [CR]) qui ont en outre l'avantage de fonctionner dans le cas non archimédien.

La méthode "géométrique" de Seidenberg .
Dans [Sei] (1954), Seidenberg propose une nouvelle approche, beaucoup plus géométrique, du problème de la décision des questions "d'algèbre élémentaire" (c.-à-d. des questions d'algèbre réelle lorsqu'elles sont formalisables dans la théorie des corps ordonnés). Il insiste en outre sur le principe de transfert. Sa méthode est une méthode pour décider si une variété algébrique réelle est vide ou non, et fournit comme sous produit une méthode d'élimination des quantificateurs (ceci quel que soit le corps réel clos considéré). Nous donnons une traduction des quelques lignes où il explique le principe de sa méthode :

> « Au départ, nous avons eu une idée pour une preuve pratiquement immédiate dans le cas du corps des nombres réels, et qui de toute manière rend tout à fait claire la méthode de décision. ... Nous nous demandons s'il y a un point réel sur une variété V :
>
> $f_1(x_1, x_2, ..., x_n) = 0$, $f_2(x_1, x_2, ..., x_n) = 0$, ..., $f_s(x_1, x_2, ..., x_n) = 0$
>
> Dans le cas du corps $\mathbb{R}$, cela est vrai si et seulement si il y a sur V un point réel plus près de l'origine que tous les autres (au sens large). En arrangeant les choses de manière que l'origine ne soit le centre d'aucune sphère contenant une composante de V de dimension ≥ 1, la condition de minimalité détermine une sous variété W de V , de dimension plus petite que V (si V est de dimension ≥ 1) et contenant un point réel si et seulement si V en contient un. On est ainsi ramené à décider si une variété de dimension 0 contient un point réel : par des projections appropriées, on se ramène au cas d'un espace ambiant de dimension 1 , cas qui est traité par le théorème de Sturm».

On voit que l'utilisation du théorème de Sturm est ramenée à la toute dernière étape.
Comme le remarque Seidenberg, cette méthode (celle qu'il a découverte au départ) s'applique a posteriori pour tout corps réel clos, mais il a été obligé de la raffiner (et de la compliquer) dans la mesure où il se plaçait dans la situation où il ne savait pas encore que, pour n'importe quel corps réel clos, toute variété possédant un point réel en possède également un à distance minimale de l'origine.
Seidenberg remarque aussi que sa méthode est a priori moins coûteuse que celle de Tarski, et pourrait avoir des applications en algorithmique concrète. Ce qui est assez pertinent, puisque des idées géométriques de même nature sont à l'oeuvre dans les travaux de complexité donnant les meilleurs résultats actuels ([Gri], [HRS]).

Cohen : une méthode semi-algébrique (cf. [Coh] 1969)
D'après Hörmander ([Hör] p. 371), son algorithme est basé sur un manuscrit de Cohen datant de 1967. En 1969, Cohen publie une preuve[7] à la fois très élégante et très proche de l'algorithme de Hörmander[8]. La preuve est si courte que nous pouvons la reproduire presque en entier (nous introduisons une ou deux modifications de terminologie mineures par rapport à son article). Soit $\mathbf{R}$ un corps réel clos. Cohen appelle *relation polynomiale* une relation dans $\mathbf{R}^n$ définie comme combinaison booléenne de conditions de signes portant sur les polynômes à coefficients entiers en les n variables considérées[9]. Il appelle *fonction semi-algébrique effective*, une fonction $f : \mathbf{R}^n \longrightarrow \mathbf{R}$, définie de telle manière qu'on ait un algorithme primitif récursif qui calcule, à partir d'une relation polynomiale arbitraire $A(y,t_1,t_2,...,t_k)$ une autre relation polynomiale $B(x_1,x_2,...,x_n,t_1,t_2,...,t_k)$ telle qu'on ait l'équivalence dans $\mathbf{R}$:

$$A(f(x_1,x_2,...,x_n),t_1,t_2,...,t_k) \iff B(x_1,x_2,...,x_n,t_1,t_2,...,t_k)$$

en abrégé : $$A(f(\mathbf{x}),\mathbf{t}) \iff B(\mathbf{x},\mathbf{t})$$

En considérant la relation $y = t$ on voit que, entre autres choses, le graphe de f doit être semi-algébrique défini sur $\mathbb{Q}$, et le but est en quelque sorte de montrer que toute fonction semi-algébrique définie sur $\mathbb{Q}$ est semi-algébrique effective. Cohen remarque que les fonctions semi-algébriques effectives sont stables par composition, et qu'elles contiennent les fonctions : $+$, $-$, $\times$, signe.
Il considère ensuite le polynôme générique de degré $\leq d$, en une seule variable x, $P_d(c_0,c_1,...,c_d,x) = P_d(\mathbf{c},x)$ (les c_i sont les coefficients).
Le lemme suivant est presque immédiat :

> Une fonction f est semi-algébrique effective si et seulement si on connaît une procédure primitive récursive qui calcule à partir de d une relation polynomiale $B(\mathbf{c},\mathbf{x},s)$ avec l'équivalence dans $\mathbf{R}$: $$\text{signe}(P_d(\mathbf{c},f(\mathbf{x}))) = s \iff B(\mathbf{c},\mathbf{x},s)$$

Il démontre ensuite, par récurrence sur d, le Théorème n°d suivant :

> Le tableau complet des signes du polynôme générique P_d est donné par $2d+2$ fonctions semi algébriques effectives (la première donne le nombre de racines, les d suivantes donnent les racines en ordre croissant[10], les $d+1$ suivantes donnent les signes sur les intervalles successifs[11])

La preuve récurrente de Cohen est facile (cela fonctionne comme la construction du tableau de Hörmander). On pourrait en donner une autre basée sur les théorèmes de Sturm et Sturm-Sylvester. Enfin il en déduit le théorème de Tarski sous la forme suivante :

> On a une procédure primitive récursive qui calcule, à partir d'une relation polynomiale $A(x_1,x_2,...,x_n)$ une autre relation polynomiale $B(x_2,...,x_n)$ avec l'équivalence dans $\mathbf{R}$: $$\exists\, x_1\ A(x_1,x_2,...,x_n) \iff B(x_2,...,x_n)$$

Il suffit en effet de considérer les tableaux complets de signes pour les polynômes intervenant dans A considérés comme des polynômes en la variable x_1. Ces tableaux vont dépendre des paramètres $x_2,...,x_n$, mais via des fonctions semi-algébriques effectives, ce qui permettra de les gluer en un seul grand tableau sur lequel, chaque fois que sa "forme générale" est fixée, l'existence d'un x_1 vérifiant $A(x_1,x_2,...,x_n)$ sera immédiate à tester. La "forme générale" de

---

7 Elle sert en fait de mise en jambe pour une preuve de décidabilité dans la théorie des corps p-adiques, qui lui permet d'établir un algorithme primitif récursif là où Ax et Kochen avaient, dans une série d'articles célèbres, établi des résultats de décidabilité avec une preuve à base d'ultrafiltres.

8 qu'il faudrait peut-être rebaptiser algorithme de Cohen-Hörmander.

9 Il s'agit donc d'une relation semi-algébrique définie sur $\mathbb{Q}$.

10 en prenant n'importe quoi pour remplacer les racines en surnombre.

11 même remarque. Signalons aussi que la preuve "rigoureuse" demanderait "un seul théorème" qui inclut

ce grand tableau dépendra de $x_2,...,x_n$ via des fonctions semi-algébriques effectives, ce qui permet de conclure.
Nous terminerons en remarquant que le saucissonnage des ensembles semi-algébriques "à la Collins" (cf. [Col]) peut être vu comme une traduction de l'algorithme de Cohen dans un langage plus ensembliste, dans le contexte où un ensemble semi-algébrique est fixé au départ et où on l'analyse par projections successives sur des espaces de coordonnées de dimensions décroissantes.

Notons pour terminer ce paragraphe «Tarski-Seidenberg-Cohen» que les trois méthodes s'appliquent pour décider des problèmes d'algèbre réelle élémentaire dans un corps **K** donné mais en supposant implicitement que l'on sait décider le signe de tout élément du corps des coefficients du problème à résoudre.

Hollkott : Preuve constructive de l'existence de la clôture réelle d'un corps ordonné discret

Le problème de la preuve constructive de l'existence d'une clôture réelle pour un corps ordonné arbitraire n'est pas résolu par la décidabilité de la théorie des corps réels clos. Une théorie formelle peut fort bien être prouvée constructivement complète et décidable sans pour autant qu'on puisse en construire un modèle : le cas de la théorie formelle intuitionniste des corps algébriquement clos discrets avec constantes dans un corps discret donné constructivement, mais non constructivement énumérable, fournit un "contre-exemple" au théorème de complétude de Gödel. (cf. [MRR] sur l'impossibilité construire "en général" une clôture algébrique pour un corps discret).
Dans le cas de la théorie des corps réels clos, ce qui fait marcher la construction, c'est l'unicité. Une fois qu'on a un algorithme pour calculer dans la clôture réelle "censée exister", il suffit d'arriver à démontrer, sans utiliser l'existence de la clôture réelle, que l'algorithme fonctionne toujours, c.-à-d. n'aboutit jamais à un blocage ni à une contradiction. Les objets que manipule alors l'algorithme ne sont rien d'autre que les éléments d'une clôture réelle. En fait, ce plan de preuve est difficile à mettre en oeuvre[12], même avec l'algorithme de Hörmander (le plus simple de tous).

La thèse de Hollkott ([Hol], Hambourg, 1941) est restée longtemps ignorée. La date et le lieu de sa production en sont sans doute la cause principale. En 1967, Zassenhaus ([Za]) rend partiellement compte des résultats de Hollkott, sans signaler le fait, essentiel pour nous et pour Hollkott lui-même, qu'il ne s'agit pas seulement de calculer dans la clôture réelle, mais surtout de donner une preuve constructive de son existence. La preuve, extrêmement algorithmique, est difficile à suivre. Il y a une récurrence sur le degré du polynôme dont on veut introduire la racine, portant sur plusieurs théorèmes simultanément.
L'idée de base est simple : si on a construit une extension ordonnée de **K** contenant toutes les racines de P' alors on sait "où sont" les racines de P et on peut construire une extension ordonnée contenant une racine de P . Néanmoins, pour faire fonctionner correctement cette idée de base, il faut beaucoup se fatiguer. Il faut savoir que le théorème des accroissements finis est valable pour P et P' (sous forme : P' positif implique P croissant), alors que la preuve ordinaire utilise déjà l'existence de la clôture réelle. D'où l'introduction du théorème des accroissements finis "jusqu'au degré d" dans la liste des théorèmes à démontrer par récurrence.

---

12 Le lecteur pourra se convaincre de la difficulté de la tâche en essayant de démontrer "directement" que dans un corps ordonné, l'algorithme de Sturm n'attribue jamais un nombre de racines strictement négatif à un

Par ailleurs, pour construire $\mathbf{K}[\xi]$ où ξ est une racine réelle de P, on se rend compte qu'on a besoin non seulement de l'extension $\mathbf{L}$ contenant les racines réelles de P' mais également d'autres extensions obtenues en rajoutant des racines de polynômes à coefficients dans $\mathbf{L}$ et, fort heureusement, de degrés strictement inférieurs à celui de P.
Dans [LR] nous avons utilisé les mêmes idées que Hollkott, sans connaître son travail. Notre preuve est plus abstraite et beaucoup plus lisible. Une simplification notable est obtenue par une preuve du théorème des accroissements finis dans tout corps ordonné : une identité algébrique explicite le taux d'accroissement de P sur un intervalle comme barycentre à coefficients rationnels positifs de valeurs de la dérivée en des points "rationnels" de l'intervalle. Mais surtout, l'introduction de la notion de corps ordonné d-clos (corps ordonné où tout polynôme de degré inférieur ou égal à d vérifie le théorème des valeurs intermédiaires) permet de bien maîtriser conceptuellement les récurrences à tiroir de la thèse de Hollkott. Récurrences à tiroir en fait inévitables et qui expliquent pourquoi la preuve constructive a "tellement" tardé. Dans la version française détaillée de [LR], nous explicitons sur quel bon ordre se passe cette récurrence lorsqu'on la "dévisse" complètement.

G. Kreisel : Sommes de carrés effectives

En 1955, à la demande d'Artin, Kreisel fournit un algorithme (uniformément) primitif récursif qui résout le 17ème problème de Hilbert. Nous rendons compte ici de l'article "Sums of squares" ([Kre1] 1957), simples notes données à un colloque[13]. On pourra aussi consulter [Kre2] pour quelques commentaires sur [Kre1].
Le 17ème problème de Hilbert peut être vu comme un cas particulier du théorème des zéros réel de Stengle ([Ste]). Il dit que si une question concernant des signes de polynômes est toujours vraie (lorsque les variables parcourent la clôture réelle du corps des coefficients) alors cela doit se manifester par une identité algébrique (de la même manière le théorème des zéros de Hilbert dit : si une famille de polynômes ne s'annule jamais simultanément dans la clôture algébrique du corps des coefficients, cela se manifeste par une identité algébrique qui explicite 1 comme élément de l'idéal engendré par les polynômes).
L'idée de base, qu'on ne retrouvera que 32 ans plus tard dans [Whi] et [Lom], est de partir d'une preuve formelle du résultat (ici : un polynôme donné est toujours ≥ 0) et de transformer cette preuve formelle en un algorithme de calcul de l'identité algébrique.
Kreisel considère le polynôme générique de degré d à n variables $g_{n,d}(\mathbf{c},\mathbf{x})$ ($\mathbf{c}$ représente les coefficients et $\mathbf{x}$ les variables), et il commence par remarquer que, d'après Tarski-Seidenberg[14], la formule exprimant :

"$g_{n,d}(\mathbf{c},\mathbf{x})$ est positif ou nul pour tout $\mathbf{x}$" [15]

est équivalente à une formule sans quantificateur qui peut être mise sous forme normale disjonctive :

---

13 Notes que je n'ai commencé à pouvoir décrypter qu'après avoir résolu la question du théorème des zéros effectif par une méthode somme toute apparentée. Il me semble aujourd'hui que la preuve de Kreisel doit pouvoir être adaptée au théorème des zéros.

14 A. Robinson ([Rob]) a déjà utilisé le principe de Tarski-Seidenberg pour donner une solution récursive (mais sans borne de complexité) pour le 17ème problème de Hilbert, sans avoir recours au théorème d'homomorphisme d'Artin-Lang. Dans [Kre2], Kreisel donne un argument en faveur du fait que les preuves "à la Robinson" via la théorie des modèles (non constructive) donnent néanmoins lieu à des algorithmes dont la complexité peut être bornée en termes de l'ordinal ε_0 de Gentzen. Il resterait à préciser dans quelle mesure l'argument de Kreisel est constructif ou non. Dans [Sco2] (p. 70-71), Scowcroft développe une discussion analogue, et semble-t-il plus convaincante, au sujet du théorème des zéros de Stengle.

15

" tel système de conditions de signes[16] est vrai"
ou " tel système de conditions de signes est vrai"
ou etc...

Les coefficients d'un polynôme f particulier[17] partout positif ou nul vérifient donc un de ces systèmes de conditions de signes, système que nous notons $\mathbb{H}(\mathbf{c})$ ou plus simplement $\mathbb{H}$. L'implication

$$(\mathbb{H}(\mathbf{c}) \Rightarrow \forall \mathbf{x}\ g_{n,d}(\mathbf{c},\mathbf{x}) \geq 0)$$

est donc démontrable dans la théorie classique des corps ordonnés réels clos. Si, à partir de la preuve formelle de cette implication, nous pouvons construire une preuve formelle de l'implication :

($\mathbb{H}(\mathbf{c}) \Rightarrow$ $g_{n,d}(\mathbf{c},\mathbf{x})$ est égale à telle somme de carrés de fractions rationnelles)

nous aurons gagné.

Pour cela, nous devons tout d'abord nous débarrasser de la relation d'ordre, et passer dans la théorie des corps réels clos "tout court". Dans $\mathbb{H}$ nous pouvons supposer que les conditions de signes sont toutes de la forme $Q_i(\mathbf{c}) \geq 0$, ou $R_j(\mathbf{c}) = 0$, ou $S_k(\mathbf{c}) \neq 0$. Nous remplaçons toute condition de signe $Q_i(\mathbf{c}) \geq 0$ par $Q_i(\mathbf{c}) = y_i^2$ où y_i est une nouvelle variable. Nous notons $\mathbb{H}' = \mathbb{H}'(\mathbf{c},\mathbf{y})$ le système ainsi obtenu. Par ailleurs le second membre de l'implication est maintenant : $\mathbb{C}'$: $\forall \mathbf{x}\ \exists z\ g_{n,d}(\mathbf{c},\mathbf{x}) = z^2$.

Si nous examinons maintenant la preuve de ($\mathbb{H}' \Rightarrow \mathbb{C}'$) dans la théorie des corps réels clos (sans relation d'ordre), nous pouvons regrouper les axiomes non logiques utilisés, en nombre fini, en trois sous groupes :

- les axiomes purement universels de la théorie des anneaux commutatifs : $\mathbb{A}_1$ (il sont en nombre fini)
- un axiome de réalité : $\mathbb{A}_2$:
  $\forall u_1\ \forall u_2 \ldots \forall u_s\ 1 + u_1^2 + u_2^2 \ldots + u_s^2 \neq 0$ (un seul suffit)
- des axiomes existentiels : $\mathbb{A}_3$:
  a) $\forall u \neq 0\ \exists z\ u.z = 1$,
  b) $\forall u\ \exists z\ (u = z^2$ ou $u = -z^2)$, et des axiomes
  c,r) $\forall u_1\ \forall u_2 \ldots \forall u_{2r+1}\ \exists z\ z^{2r+1} + u_1.z^{2r} + u_2.z^{2r-1} + \ldots + u_{2r+1} = 0$
  (pour un nombre fini de valeurs de r, mais le r maximum utilisé suffirait)

On a donc une preuve dans le calcul des prédicats classique pour le théorème :

($\mathbb{H}'$ et $\mathbb{A}_1$ et $\mathbb{A}_2$ et $\mathbb{A}_3$) $\Rightarrow$ $\mathbb{C}'$

Par ailleurs on a aussi une preuve pour :

($\mathbb{A}_1$ et $\neg\, \mathbb{A}_2$ et $\mathbb{A}_3$) $\Rightarrow$ $\forall \mathbf{x}\ \exists u_1\ \exists u_2 \ldots \exists u_s\ g_{n,d}(\mathbf{x}) = u_1^2 + u_2^2 \ldots + u_s^2$

(si $g_{n,d}(\mathbf{x})$ est un carré, c'est clair, sinon, $-g_{n,d}(\mathbf{x})$ est un carré non nul et on utilise $\neg\, \mathbb{A}_2$ et l'existence d'un inverse d'un non nul).

Donc cela fournit une preuve dans le calcul des prédicats classique pour :

($\mathbb{H}'$ et $\mathbb{A}_1$ et $\mathbb{A}_3$) $\Rightarrow$ $\forall \mathbf{x}\ \exists u_1\ \exists u_2 \ldots \exists u_s\ g_{n,d}(\mathbf{x}) = u_1^2 + u_2^2 \ldots + u_s^2$

Il faut maintenant arriver à faire façon des quantificateurs existentiels dans l'hypothèse. Pour cela on rajoute des symboles fonctionnels, le symbole ι ($\iota(u)$ est abrégé en u^{-1}) pour l'inverse d'un non nul (par convention l'inverse de 0 est pris égal à 0), un symbole ρ où $\rho(u)$ note une racine carrée de u ou de $-u$, et un symbole ρ_r où $\rho_r(u_1,u_2,\ldots,u_{2r+1})$ note une racine d'un polynôme de degré impair (il y a besoin d'un symbole par degré considéré). Chaque axiome utilisé dans $\mathbb{A}_3$ peut alors être remplacé par un axiome purement universel (par exemple le a) devient : $\forall u \neq 0\ \ u.u^{-1} = 1$). On appelle $\mathbb{A}_3'$ le nouveau système

---

16 portant sur des polynômes en les coefficients de f.

17 Les coefficients sont maintenant des éléments d'un

d'axiomes obtenu. D'où une preuve dans le calcul des prédicats classique pour :

$$(\mathbb{H}'(\mathbf{c},\mathbf{y}) \text{ et } A_1 \text{ et } A_3') \Rightarrow \forall \mathbf{x}\ \exists u_1\ \exists u_2 \ldots \exists u_s\ g_{n,d}(\mathbf{x}) = u_1^2 + u_2^2 \ldots + u_s^2$$

avec le langage étendu par les symboles fonctionnels cités.

En appliquant le premier ε-théorème de Hilbert on peut alors décrypter la preuve en une construction de termes $t_{i,1}(\mathbf{c},\mathbf{y},\mathbf{x})$, $t_{i,2}(\mathbf{c},\mathbf{y},\mathbf{x})$,... , $t_{i,s}(\mathbf{c},\mathbf{y},\mathbf{x})$ (i = 1, 2, ... N) du nouveau langage, avec une preuve de

$$(\mathbb{H}'(\mathbf{c},\mathbf{y}) \text{ et } A_1 \text{ et } A_3') \Rightarrow \bigvee_{i=1\ldots N} g_{n,d}(\mathbf{x}) = t_{i,1}^2 + t_{i,2}^2 \ldots + t_{i,s}^2$$

On remarque que puisque l'axiome de réalité n'est plus dans les hypothèses, le symbole ρ peut être interprété aussi bien comme donnant une racine carrée de u qu'un racine carrée de $-u$.

Il s'agit maintenant de voir comment transformer ces expressions obtenues en une seule somme de carrés de fractions rationnelles.

Pour ce qui concerne le connecteur **ou** on remarque que si on a $f = \Sigma\, a_i^2$ ou $f = \Sigma\, b_j^2$, alors $(f - \Sigma\, a_i^2).(f - \Sigma\, b_j^2) = 0$ qui se réécrit $f.(\Sigma\, a_i^2 + \Sigma\, b_j^2) = f^2 + \Sigma\, a_i^2 b_j^2$. Ce qui donne : $f = (f^2 + \Sigma\, a_i^2 b_j^2).(\Sigma\, a_i^2 + \Sigma\, b_j^2)^{-1}$ ou $-1 = (\Sigma\, a_i^2).(\Sigma\, b_j^2)^{-1}$.

Par ailleurs $-1 = (\Sigma\, a_i^2)$ ou $-1 = (\Sigma\, b_j^2)$ implique $-1 = \Sigma\, a_i^2 + \Sigma\, b_j^2 + \Sigma\, a_i^2\, b_j^2$.

Au fur et à mesure qu'on va décrypter l'écriture de $g_{n,d}(\mathbf{x})$ comme somme de carrés utilisant les symboles ι , ρ et ρ_r en une somme de carrés utilisant des symboles ι , ρ et ρ_r de moins en moins imbriqués, on obtient parallèlement l'alternative selon laquelle -1 s'écrit comme une somme de carrés, qu'on désimbrique parallèlement à f . A la fin du processus, on obtiendra que $g_{n,d}(\mathbf{x})$ ou -1 est égal à une somme de carrés de fractions rationnelles, ce qui permettra de conclure.

Voyons comment on élimine un symbole de racine carrée ρ non enfoui dans d'autres ρ ou ρ_r . On a donc une expression "somme de carrés de fractions rationnelles en ρ(s)". On se ramène au cas "somme de carrés de polynômes en ρ(s)" en utilisant "la quantité conjuguée". Par ailleurs, on se souvient que ρ(s) peut être interprété comme $\sqrt{s}$ ou $\sqrt{-s}$, et cela donne en fait deux égalités : l'une $f = \Sigma\, (a_i + \Sigma\, b_i\sqrt{s}\,)^2$ et l'autre $f = \Sigma\, (c_j + \Sigma\, d_j\sqrt{-s}\,)^2$.

On utilise maintenant un raisonnement cas par cas, ce qui est légitime puisqu'on sait traiter les **ou** . Si $\Sigma\, a_i b_i \neq 0$ on a $2\sqrt{s} = (\Sigma\, a_i b_i)^{-1}.(f - \Sigma\, a_i^2 - s\, \Sigma\, b_i^2)$ ce qui permet de faire disparaître $\sqrt{s}$ de la première expression. Si $\Sigma\, a_i b_i = 0$, on essaie avec la deuxième. Si $\Sigma\, a_i b_j = \Sigma\, c_j d_j = 0$, on obtient $f = \Sigma\, a_i^2 + s\, \Sigma\, b_i^2 = \Sigma\, c_j^2 - s\, \Sigma\, d_j^2$, d'où :

$$-s^2.(\Sigma\, b_i^2)(\Sigma\, d_j^2) = f^2 - f.(\Sigma\, a_i^2 + \Sigma\, c_j^2) + (\Sigma\, a_i^2)(\Sigma\, c_j^2)$$

et on peut conclure, en séparant encore quelques cas, que f ou -1 s'écrit comme une somme de carrés d'expressions "moins imbriquées" que celles du départ.

Il faut traiter de manière analogue le cas des symboles ρ_r . Cette fois-ci, un raisonnement par récurrence sur r est nécessaire.

Il faut enfin vérifier que les variables y_i qui avaient été introduites pour remplacer les ≥ 0 par des $= y_i^2$ peuvent n'apparaître que sous forme de carrés dans l'expression finale, où on les remplace alors par $Q_i(\mathbf{c})$, ce qui donnera une expression comme sommes de carrés de fractions rationnelles pondérés par des éléments positifs du corps des coefficients une fois qu'on aura spécialisé les c_i .

Même ainsi explicitée, la preuve de Kreisel nous semble encore un peu obscure. Notamment, il n'est pas tout à fait clair de savoir comment on se débrouille avec le symbole ι (qui représente l'inverse d'un élément, avec ι(0) = 0 par convention) : la réduction d'une écriture comportant comme seuls symboles fonctionnels ...

en effet problème du fait que u.ι(v) n'est égal à uw.ι(vw) que lorsque w est non nul ou u.v nul.

Whiteley : Une approche constructive du théorème des zéros réel via le calcul des séquents

Walter Whiteley démontre avec une facilité déconcertante une version faible du théorème des zéros réel :

Soient $f_1(\mathbf{x})$, ..., $f_r(\mathbf{x})$, $g(\mathbf{x})$ des polynômes à coefficients entiers. Si on a une preuve de l'implication $[\ f_1(\mathbf{x}) = 0$ et .... et $f_r(\mathbf{x}) = 0\ ] \Rightarrow g(\mathbf{x}) = 0$ dans la théorie formelle des anneaux intègres réels alors on peut construire un nullstellensatz, c.-à-d. une identité algébrique du type :

$\Sigma\ a_i(\mathbf{x}).f_i(\mathbf{x}) = m.g(\mathbf{x})^p + \Sigma\ b_j(\mathbf{x})^2$ (m et p sont des entiers ≥ 1)

Plus précisément, Whiteley utilise un calcul des séquents à la Gentzen[18], et il donne un algorithme qui transforme une dérivation du séquent :

$$f_1(\mathbf{x}) = 0\ ,\ \ldots\ ,\ f_r(\mathbf{x}) = 0 \ \vdash\ g(\mathbf{x}) = 0$$

en une construction de l'identité algébrique de type voulu.

La partie la plus difficile consiste à réduire la dérivation à une "forme normale" ou les coupures sont limitées à des formules atomiques. Il s'agit là d'une extension du Hauptsatz de Gentzen, pour le cas d'une théorie avec égalité et axiomes "atomiques".

Les identités algébriques sont ensuite faciles à construire "le long d'une dérivation normale" (comme dit Whiteley, les Nullstellensatz sont des feuilles qui poussent naturellement sur l'arbre d'une dérivation normale). L'algorithme de Whiteley (en entier) est primitif récursif.

Il semble que le calcul naturel serait particulièrement bien adapté à ce genre de démonstration (cf. [Pra] corollaire 3.2.2.5 p. 256).

La principale faiblesse du théorème de Whiteley est qu'il ne fait que la moitié du travail. Il manque en effet un algorithme pour passer de manière automatique d'une preuve de :

$$[\ f_1(\mathbf{x}) = 0 \text{ et } \ldots \text{ et } f_r(\mathbf{x}) = 0\ ] \Rightarrow g(\mathbf{x}) = 0$$

dans $\mathbf{CRC_c}$ à une preuve de cette même implication dans la théorie des anneaux réels intègres. (voir cependant la note de bas de page n°14).

Or c'est précisément le traitement des quantificateurs existentiels qui est le point le plus délicat dans une preuve de nullstellensatz (aussi bien dans [Kre1] que dans [Lom]).

Il nous semble assez plausible qu'on puisse développer dans le cadre du calcul naturel une théorie de l'existence potentielle analogue à celle donnée dans [Lom], ce qui donnerait une preuve du théorème des zéros réels entièrement basée sur la logique.

La solution constructive complète du théorème des zéros réels et de ses variantes

Dans la solution que nous avons donnée du problème ([Lom]), nous avons une heuristique analogue à celle de Kreisel. Cependant, nous ne nous basons pas sur une preuve dans une théorie formelle, mais sur l'algorithme de Hörmander, de conception particulièrement simple.

Le théorème général sur lequel sont basés le théorème des zéros réel et ses variantes est le suivant : on considère un système d'égalités et inégalités portant sur des polynômes de $\mathbf{K}[\mathbf{X}] = \mathbf{K}[X_1,X_2,\ldots,X_n]$, où $\mathbf{K}$ est un corps ordonné de clôture réelle $\mathbf{R}$; ce système définit une partie semi-algébrique S de $\mathbf{R}^n$; le théorème affirme que S est vide si et

---

18 tous les axiomes de la théorie des anneaux intègres réels sont mis sous forme: dérivation d'une formule

seulement si il y a une identité algébrique d'un certain type construite à partir des polynômes donnés, et qui rend évident le fait que S est vide.
L'idée générale de notre preuve constructive est la suivante. On peut tester si S est vide par l'algorithme de Hörmander , appliqué de manière itérative pour diminuer par étapes le nombre de variables sur lesquelles portent les conditions de signes. 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]).
Nous introduisons la notion d'*implication forte* : une implication forte est une forme forte (donnée par des identités algébriques explicites) pour l'implication *universelle* correspondante : $\forall\, \mathbf{x} \in \mathbf{R}^n \ (\ \mathbb{H}(\mathbf{x}) \Rightarrow \mathbb{H}'(\mathbf{x}) \ )$.
On vérifie alors que les axiomes purement universels s'expriment sous forme d'implications fortes (c.-à-d. encore sous forme "stellensatzisée").
Un autre pas consiste à traduire sous forme de *constructions d'implications fortes* certains raisonnements élémentaires (du genre : « si $A \Rightarrow B$ et $B \Rightarrow C$ alors $A \Rightarrow C$ », ou les preuves par cas).
Il faut 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* :
L'algorithme de Hörmander introduit des racines de polynômes par application du théorème des valeurs intermédiaires, aussi nous avons besoin d'une forme "stellensatzisée" pour les énoncés du genre :

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

Une traduction "mot à mot" de cette alternance de quantificateurs en termes d'implications fortes semblerait devoir être : pour toute spécification à la Thom des x_i non fortement incompatible avec $\mathbb{H}_1(\mathbf{x})$, le système $\mathbb{H}_2(\mathbf{x},\mathbf{t})$ est lui-même non fortement incompatible. Mais, dans l'algorithme, les valeurs prises par les x_i peuvent dépendre de valeurs prises par des paramètres y_j , et ceci nécessite une reformulation (où les x_i , au lieu d'être spécifiés à la Thom, sont soumis à des conditions arbitraires). En outre, il nous faut donner une forme constructive à l'implication « $\mathbb{H}$ non fortement incompatible » implique « $\mathbb{H}'$ non fortement incompatible ». Ceci nous a conduit à considérer la contrapposée sous la forme suivante : on sait construire une identité algébrique signifiant l'incompatibilité de $\mathbb{H}$ à partir d'une identité algébrique signifiant l'incompatibilité de $\mathbb{H}'$.

Signalons également qu'une simplification importante dans la construction du nullstellensatz réel est obtenue à travers une version "identité algébrique" du lemme de Thom, donnée par ce que nous appelons les *formules de Taylor mixtes*, qui sont démontrées au moyen du théorème algébrique des accroissements finis.

Notons enfin deux sous-produits importants de la construction effective des nullstellensatz réels. (cf. [Lom] version française détaillée).
Le premier est une nouvelle preuve constructive de l'existence la clôture réelle d'un corps ordonné discret. La preuve du théorème des zéros n'utilise pas en tant que telles des extensions ordonnées de $\mathbf{K}$. Elle permet alors d'affirmer que l'algorithme de Hörmander, qui, par sa construction, ne bloque jamais, aboutit nécessairement à des résultats cohérents lorsqu'il est

Le deuxième est une preuve constructive du résultat suivant : si $\mathbf{K}$ est un corps réel, la théorie $\mathbf{CRCD_i(K)}$ est cohérente. Ceci explicite exactement la signification constructive du théorème classique (non prouvable constructivement) selon lequel tout corps réel possède une clôture réelle. Cela autorise à travailler constructivement dans un corps réel comme s'il était sous-corps d'un corps réel clos, tant qu'on ne se préoccupe que d'énoncés du premier ordre.

Problèmes en suspens

Prenez un livre de géométrie algébrique réelle tel que [BCR], et essayez de donner une preuve constructive de tout théorème qui y est démontré (ou, si ça coince, essayez de trouver les substituts constructifs intéressants), ceci en supposant les corps tous discrets.
Note pessimiste : pour le moment, seuls les résultats de base ont subi ce traitement.
Note optimiste : beaucoup d'énoncés dépendent de la décidabilité de la théorie du premier ordre et leur preuve est dores et déjà constructive (cf. [Cos2]).

2) Algèbre réelle générale

Présentation des problèmes

Nous appelons algèbre réelle générale l'algèbre des nombres réels pour les 4 opérations élémentaires. Nous considérons les nombres réels présentés à la Cauchy (les seuls avec lesquels on puisse développer une théorie constructive des opérations algébriques élémentaires). Alors on n'a pas de test pour le signe d'un x (imaginez x donné par un oracle qui répond à la question : donnez moi s'il vous plaît une approximation rationnelle à $1/2^n$ du nombre réel x). Par contre nous avons constructivement :

$$\forall\, x<y \quad \forall\, z \quad (\, x<z \text{ ou } z<y\,) \qquad (1)$$

Pour ces réels constructifs, les relations d'inégalités strictes $>$, $<$, $\neq$ sont des relations de caractère positif, c.-à-d. dont on peut être assuré par un simple test, tandis que les relations $\leq$, $\geq$, $=$ ont un caractère négatif. Elles sont définies comme signifiant l'absurdité de la relation "positive" correspondante. Du point de vue constructif minimal (celui de Bishop) on ne peut pas déduire $x \neq y$ à partir de $\neg\,(x = y)$ [19] (c.-à-d. à partir de sa double négation).
Nous disons x est **écarté** de y pour signifier que nous considérons $x \neq y$ dans sa signification positive.
Des axiomes pour la théorie constructive des corps ordonnés, $\mathbf{CO_i}$, ont été proposés par Heyting. Nous pouvons décrire cette théorie formelle comme suit, sans souci de minimalité aucun :

- on utilise le langage des anneaux commutatifs, avec les prédicats $>$, $\geq$, $=$, $\neq$. La logique est la logique intuitionniste pour le premier ordre. Les axiomes peuvent être regroupés de la manière suivante.
- axiomes usuels pour l'égalité
- axiomes des anneaux commutatifs
- axiomes pour $\neq$: $\quad \neg\,(x \neq y) \iff x = y$
  $\quad x \neq 0 \iff \exists\, y\ x.y = 1 \iff x < 0 \text{ ou } x > 0$
- axiomes pour $>$: $\quad \neg\,(x > y) \iff x \leq y$
  $\quad x > y \implies x + z > y + z$

19 L'école constructiviste russe de Markov accepte cette déduction (bien qu'elle rejette le tiers exclu $x = 0$

$$x>0 \text{ et } y>0 \Rightarrow x.y>0 \text{ et } x+y>0$$
$$x+y>0 \Rightarrow x>0 \text{ ou } y>0$$

Comme nous nous intéressons aux propriétés purement algébriques (c.-à-d. grosso modo celles qui concernent les polynômes), nous n'avons pas vraiment besoin que toutes les suites de Cauchy convergent. Autrement dit, tout sous-corps de $\mathbb{R}$ qui sera réel clos (notion qui reste à définir dans ce nouveau cadre) fera pour nous aussi bien l'affaire que $\mathbb{R}$. Pour préciser la notion de corps réel clos dans le cadre non discret, nous avons besoin de bien connaître les propriétés purement algébriques fondamentales de $\mathbb{R}$.
Par ailleurs, comme nous nous intéressons particulièrement au cas "non discret", nous n'avons de fait pas droit aux infiniment petits : en prenant $x=0$, y infiniment petit positif et z un réel ordinaire dans (1) on obtient $0<z$ ou $z\leq 0$ qui n'est pas constructivement valide[20]. Autrement dit, notre sémantique implicite sera toujours celle d'un sous-corps de $\mathbb{R}$.

Certains théorèmes classiques indémontrables constructivement pour des fonctions continues arbitraires sont néanmoins prouvables lorsque l'on se restreint aux fonctions polynômes, ou semi-algébriques continues (ils sont en règle générale prouvables pour les fonctions semi algébriques définies sur $\mathbb{Q}$ parce qu'on est ramené au cas discret).
Nous en citerons deux, tout à fait significatifs.
Tout d'abord nous établissons un lemme :

Si un polynôme P est de degré $\leq d$ et si $x_0, x_1, ..., x_d$ sont $d+1$ points distincts, il est équivalent d'affirmer : «un des coefficients de P au moins est écarté de 0 » ou «un des $P(x_i)$ au moins est écarté de 0 ». On dira alors que P est écarté de 0 .

Preuve via la formule d'interpolation de Lagrange.
Le premier théorème que nous voulons citer est le théorème des valeurs intermédiaires sous la forme suivante :

Si $a<b$, si P est un polynôme écarté de 0 , et si $P(a)\leq 0$, $P(b)\geq 0$ alors il existe un c sur $[a,b]$ tel que $P(c)=0$.

preuve : Comme P est écarté de 0 on peut considérer un x sur $[a,b]$ avec $P(x)\neq 0$. Si $P(x)>0$ on démarre une dichotomie avec a et x , si $P(x)<0$ avec x et b . A chaque étape, on considère un point x du tiers central de l'intervalle avec $P(x)\neq 0$), ce qui permet de continuer la dichotomie. ❑

On peut par exemple définir la racine carrée de x^2 (c.-à-d. la valeur absolue de x) sans avoir besoin de savoir si x est ≤ 0 ou ≥ 0 , en appliquant ce théorème.

Le deuxième théorème est le théorème des accroissements finis (presque) classique :

Si P'' est écarté de 0 alors pour $a<b$ arbitraires, on peut trouver c sur $]a,b[$ tel que :
$$P(b)-P(a)=(b-a).P'(c)$$

preuve> Comme P'' est écarté de 0 on peut construire u, v avec $P'(u)\neq P'(v)$. Soit d majorant le degré de P . On utilise une formule du théorème algébrique des accroissements finis à $d+1$ points (celle par exemple pour les polynômes de degré $\leq d+1$). Le taux d'accroissements de P est donc barycentre à coefficients positifs de $d+1$ valeurs de P' sur l'intervalle. Deux de ces valeurs sont écartées (calculer $P'(u)$ et $P'(v)$ par interpolation de Lagrange). Donc l'une est distincte du taux d'accroissement, par exemple strictement inférieure. Une autre est alors forcément strictement supérieure. Et on conclut par le théorème des valeurs intermédiaires. ❑
On voit que le deuxième théorème est démontrable à partir du premier dans la théorie $\mathbf{CO}_1$.

---

[20] Il est sans doute possible de considérer l'analyse classique comme intermédiaire entre l'analyse constructive

Remarque : la preuve ne donne pas c comme fonction continue de a et b .
De manière générale, les preuves constructives n'assurent la continuité[21] que sous les deux conditions suivantes : 1) l'espace de définition de la fonction est un espace métrique complet séparable, et 2) f(x) est l'unique y vérifiant la propriété A(x,y).
La condition 2) n'est par exemple pas assurée pour "y est un entier plus grand que x". Quoique l'existence de y ne fasse pas problème, y résulte de x par un calcul "non extensionnel" : deux représentations à la Cauchy distinctes du même réel x conduisent à deux valeurs de y distinctes.

Le théorème suivant est constructif.

Si P est un polynôme partout > 0 sur [a,b] alors il existe $\chi > 0$ tel que $P(x) > \chi$ sur [a,b].

preuve> Soient $x_1, x_2, ..., x_d$ les parties réelles des zéros de P' rangées en ordre croissant. Posons $y_0 = a$, $y_{d+1} = b$, et pour $i = 1, ..., d$: $y_i = f(x_i)$ où

$$f(x) = a \text{ si } x \leq a \text{ , } x \text{ si } a \leq x \leq b \text{ , } b \text{ si } b \leq x.$$

On a : $\inf \{P(x); a \leq x \leq b\} = \inf \{P(y_i); i = 0, 1, ..., d+1\}$
En effet : ce résultat est facile pour P à coefficients rationnels et se prolonge par continuité pour le cas de coefficients réels arbitraires. ❑

NB : On peut espérer a priori étendre le résultat au cas d'un polynôme à plusieurs variables et d'un compact semi-algébrique défini sur $\mathbb{Q}$, il est par contre tout à fait exclu qu'on prouve constructivement que P atteint son minimum sur [a,b].

En tout état de cause, l'algèbre constructive des nombres réels semble trop mal connue pour qu'on puisse proposer valablement une axiomatique pour la théorie $\mathbf{CORC_i}$.
L'élucidation constructive du théorème des zéros dans le cas des coefficients dans $\mathbb{R}$ nous semble une condition préalable. Le but est en quelque sorte le suivant : trouver la théorie formelle la plus simple possible qui rende compte de tous les résultats constructifs de l'algèbre réelle, dès qu'ils sont formulables dans le langage de $\mathbf{CO_i}$.
Un autre problème clé peut être celui de la construction de la clôture réelle d'un corps ordonné à la Heyting, mais l'enjeu mathématique n'est pas celui annoncé dans la mesure où implicitement nous travaillons avec un sous-corps de $\mathbb{R}$.

Nous rendons compte maintenant de travaux qui cernent en partie la question du théorème des zéros réels dans $\mathbb{R}$.

Delzell : une solution continue et constructive du 17ème problème de Hilbert

Comme nous le signalions dans l'introduction le résultat de Delzell est apparemment le premier résultat constructif non élémentaire en algèbre réelle générale, (excepté le théorème fondamental de l'algèbre, qui peut être interprété comme un résultat d'algèbre réelle).

Les ingrédients de la preuve de Delzell semblent tous constructifs, ce sont essentiellement :
– le théorème des zéros réel (discret) qui a aujourd'hui une solution constructive satisfaisante.
– le théorème de finitude (discret) : tout fermé **K**-semi-algébrique (c.-à-d. semi-algébrique défini par des équations et inéquations à coefficients dans **K** supposé discret) est réunion d'un nombre fini de fermés **K**-semi-algébriques élémentaires (un fermé semi-algébrique est

[21] continuité

élémentaire s'il est défini par des inéquations du type $P(\mathbf{x}) \geq 0$). On trouve dans [Cos1] une preuve constructive du résultat.

- le théorème de triangulation semi-algébrique d'un semi-algébrique (discret).

Présentons maintenant le résultat essentiel de Delzell.

On considère le polynôme générique homogène de degré d (pair) en n variables, qu'on note $f_{n,d}(\mathbf{c},\mathbf{x})$. Soit m le nombre de coefficients c_i . On note $P_{n,d}$ le fermé $\mathbb{Q}$ -semi-algébrique tel que dans tout corps réel clos discret $\mathbf{R}$ on ait l'équivalence :

$$\forall\, \mathbf{c} \in \mathbf{R}^m \quad (\mathbf{c} \in P_{n,d}(\mathbf{R}) \text{ [22]} \iff \forall\, \mathbf{x} \in \mathbf{R}^n \; f_{n,d}(\mathbf{c},\mathbf{x}) \geq 0) \qquad (1)$$

Delzell construit un entier s et des fonctions $\mathbb{Q}$ -semi-algébriques[23] continues $r_i(\mathbf{c},\mathbf{x})$ et $s_j(\mathbf{c},\mathbf{x})$ de $P_{n,d}(\mathbf{R}) \times \mathbf{R}^n$ vers $\mathbf{R}$, qui en tant que fonctions de $\mathbf{x}$ sont des polynômes homogènes de degrés respectivement $ds + d/2$ et ds , telles qu'on ait :

$$\forall\, \mathbf{c} \in P_{n,d}(\mathbf{R}) \;\; \forall\, \mathbf{x} \in \mathbf{R}^n \quad f_{n,d}(\mathbf{c},\mathbf{x}) = \frac{\sum r_i(\mathbf{c},\mathbf{x})^2}{f_{n,d}(\mathbf{c},\mathbf{x})^{2s} + \sum s_j(\mathbf{c},\mathbf{x})^2} \qquad (2)$$

En multipliant au second membre le haut et le bas par le dénominateur et en développant le produit au numérateur on obtient une écriture de $f_{n,d}(\mathbf{c},\mathbf{x})$ comme somme de carrés de fractions rationnelles homogènes en $\mathbf{x}$:

$$\forall\, \mathbf{c} \in P_{n,d}(\mathbf{R}) \;\; \forall\, \mathbf{x} \in \mathbf{R}^n \quad f_{n,d}(\mathbf{c},\mathbf{x}) = \sum t_h(\mathbf{c},\mathbf{x})^2 \qquad (3)$$

Les coefficients de chaque $t_h(\mathbf{c},\mathbf{x})$ (vue comme fraction rationnelle en $\mathbf{x}$) sont des fonctions $\mathbb{Q}$ -semi-algébriques continues de $\mathbf{c}$. Comme le dénominateur de $t_h(\mathbf{x})$ ne s'annule qu'en des zéros de $f_{n,d}(\mathbf{x})$ on peut montrer que chaque $t_h(\mathbf{c},\mathbf{x})$ est une fonction semi-algébrique continue sur $P_{n,d}(\mathbf{R}) \times \mathbf{R}^n$.

Nous donnons une idée très rapide de la construction de Delzell. On décompose $P_{n,d}$ en un nombre fini de fermés semi-algébriques élémentaires W_k . Sur W_k on a une écriture telle que (2) avec les r_i et les s_j qui sont des polynômes d'après le théorème de Stengle (dont il faut donner une version "homogène": Delzell déduit la version homogène de la version non homogène par une construction assez simple). Il faut ensuite arriver à recoller ensemble les écritures distinctes obtenues pour chaque W_k . C'est assez fatigant, mais néanmoins faisable, au moyen d'une partition de l'unité. La preuve comporte quelques détours assez subtils et apparemment inévitables.

Nous discutons ensuite la question : en quoi cette construction entièrement basée sur le cas des corps réels clos discrets donne la solution constructive dans le cas réel "général" ?

Tout d'abord, puisque nous travaillons en polynômes homogènes, nous pouvons considérer que nous sommes sur des sphères (de $\mathbb{R}^m$ et $\mathbb{R}^n$), donc sur un compact. Dans le cas discret une fonction semi-algébrique continue sur un compact semi-algébrique est, constructivement, uniformément continue, donc les écritures (2) et (3) s'étendent à $P_{n,d}(\mathbb{R}) \times \mathbb{R}^n$ par continuité.

Il nous reste à voir comment l'équivalence (1) est constructivement prouvable lorsqu'on remplace le corps réel clos discret $\mathbf{R}$ par $\mathbb{R}$, c.-à-d. à donner une preuve constructive de l'implication :

$$\forall\, \mathbf{c} \in \mathbb{R}^m \quad [\,(\forall\, \mathbf{x} \in \mathbb{R}^n \; f_{n,d}(\mathbf{c},\mathbf{x}) \geq 0) \Rightarrow \mathbf{c} \in P_{n,d}(\mathbb{R})\,]$$

Notons $Q_{n,d}(\mathbb{R})$ la partie de $\mathbb{R}^m$ définie par le premier membre de l'implication.

---

[22] Plus précisément $P_{n,d}$ est une fermé semi-algébrique générique: c'est une combinaison booléenne d'équations et inéquations portant sur des polynômes à coefficients entiers en les variables $\mathbf{c}$ et pour tout corps réel clos $\mathbf{K}$, $P_{n,d}(\mathbf{K})$ est la partie de $\mathbf{K}^m$ correspondante.

[23]

Il est clair que $Q_{n,d}(\mathbb{R})$ est un cône convexe fermé et que le point $\mathbf{c}$ correspondant à la forme $(\Sigma\, x_i^2)^{d/2}$ est intérieur à $Q_{n,d}(\mathbb{R})$. Donc $Q_{n,d}(\mathbb{R})$ est l'adhérence de son intérieur.
Enfin $Q_{n,d}(\mathbb{R})$ et $P_{n,d}(\mathbb{R})$ ont les mêmes points rationnels puisque l'équivalence (1) est valable pour les réels algébriques. Etant donné un point de $Q_{n,d}(\mathbb{R})$ on peut donc l'expliciter comme limite d'une suite de points rationnels de $P_{n,d}(\mathbb{R})$, et on conclut en remarquant que $P_{n,d}(\mathbb{R})$ est fermé puisque réunion finie de fermés élémentaires.

Terminons par une interrogation quant à la validité constructive de la forme forte (1') de l'équivalence (1), (nous explicitons (1') ci-dessous).
La fonction "distance à $P_{n,d}$", $\mathbf{c} \longmapsto d(\mathbf{c},P_{n,d}(\mathbf{R}))$ (avec $\mathbf{R}$ corps des nombres réels algébriques) est une fonction semi-algébrique contractante qui se prolonge par continuité à $\mathbb{R}^m$ et cela montre que $P_{n,d}(\mathbb{R})$, adhérence de $P_{n,d}(\mathbf{R})$, est un fermé situé (la fonction distance est calculable).

Problème : Peut-on démontrer constructivement l'équivalence :

$$\forall\, \mathbf{c} \in \mathbb{R}^m \quad (d(\mathbf{c},P_{n,d}(\mathbb{R})) > 0 \quad \Longleftrightarrow \quad \exists\, \mathbf{x} \in \mathbb{R}^n \; f_{n,d}(\mathbf{c},\mathbf{x}) < 0) \qquad (1') \quad ?$$

Signalons enfin que Scowcroft ([Sco3]) étend le résultat de Delzell, par les mêmes méthodes, à des formes de Nullstellensatz réel plus générales (bien qu'analogues à celle utilisée par Delzell) : celles où l'implication $\forall\, \mathbf{x} \in \mathbf{R}^n \; (\mathbb{H}(\mathbf{c},\mathbf{x}) \Rightarrow \mathbb{H}'(\mathbf{c},\mathbf{x}))$ à traduire en identité algébrique, est, par définition, vraie pour $\mathbf{c}$ dans une partie fermée.

Scowcroft : les problèmes du type $\forall\, \exists$ en algèbre réelle intuitionniste et/ou constructive

Le travail de Scowcroft ([Sco1], [Sco2]) démarre comme un travail concernant la validité de certaines formules du type $\forall\, \exists$ de $\mathbf{CO}_i$ dans le modèle de Scott de l'analyse intuitionniste[24]. Nous en rendons compte assez brièvement, à la mesure de ce que nous avons pu comprendre vu le caractère assez sophistiqué des méthodes employées.

Il démontre tout d'abord, par des arguments non constructifs, que pour certaines classes de formules sans quantificateurs $M(\mathbf{x})$ et $N(\mathbf{x},\mathbf{y})$, la formule :

$$\forall\, \mathbf{x} \; [\; M(\mathbf{x}) \Rightarrow \exists\, \mathbf{y}\; N(\mathbf{x},\mathbf{y}) \;] \qquad (1)$$

est "valide" dans le modèle de Scott si et seulement si une certaine formule

$$\forall\, \mathbf{x} \; [\; M(\mathbf{x}) \Rightarrow \exists\, \mathbf{y}\; G(\mathbf{x},\mathbf{y}) \;] \qquad (2)$$

est "vraie". Où G est algorithmiquement construite à partir de M et N. A priori, G est plus fort que N (aussi bien classiquement que constructivement) et signifie grosso modo :

«N avec des conditions de continuité concernant la dépendance de $\mathbf{y}$ par rapport à $\mathbf{x}$».

Nous avons mis des guillemets à "valide" et à "vrai" pour insister sur le fait que la preuve fonctionne dans le cadre des mathématiques classiques, avec une sémantique du type réalisme platonicien.
Toute formule prouvable constructivement est valide dans le modèle de Scott. Ceci donne donc une méthode pour prouver (non constructivement) que certaines formules "vraies classiquement" ne sont pas prouvables constructivement (par exemple "$x \geq 0$ ou $x \leq 0$", mais il y a des exemples plus sophistiqués).

Il démontre ensuite deux résultats qui concernent beaucoup plus directement le point de vue constructif minimal. Ces résultats sont démontrés pour une classe plus restreinte de formules M et N : ce sont les formules qualifiées de simples, c.-à-d. les conjonctions :

$$\wedge\; (\wedge\, p_{i,j}(\mathbf{x}) > 0 \quad \Rightarrow \quad \vee\; q_{i,k}(\mathbf{x}) > 0)$$

---

24 Nous ne présentons ici que l'aspect [illegible] de Scott de l'analyse intuitionniste.

où les $p_{i,j}$ et $q_{i,k}$ sont des polynômes à coefficients dans $\mathbf{R}$ (nombres réels algébriques). Notons que les formules considérées dans la suite sont, lorsque les variables sont prises dans $\mathbf{R}$, toutes testables d'après la complétude et décidabilité de la théorie $\mathbf{CORCD_i}$. Et qu'il n'y a donc aucune "querelle sémantique" concernant ce que signifie leur "vérité".
Le premier résultat, le plus intéressant pour nous, est l'implication suivante (cf. [Sco2], Théorème 1 p. 50) :

(2) est vraie dans $\mathbf{R}$ implique (1) est constructivement vraie dans $\mathbb{R}$

qui est démontrée (croyons nous) dans le style "minimal" de Bishop. Cette preuve doit donc fournir un théorème ou schéma de théorème démontrable dans une théorie formelle $\mathbf{CORC_i}$ (rappelons que cette théorie reste à définir, mais justement c'est ici un critère important qui est mis en évidence).
Le deuxième résultat est par contre obtenu en utilisant des principes intuitionnistes à la Brouwer[25], une équivalence qui concerne la même classe de formules M et N :

(1) est intuitionnistiquement vraie dans $\mathbb{R}$ implique (2) est vraie dans $\mathbf{R}$

Ici la "vérité" pour (1) est celle du point de vue intuitionniste de Brouwer.
Ce deuxième résultat laisse augurer une règle de déduction qui serait prouvable dans une théorie $\mathbf{CORC_i}$ et qui dirait : à partir d'une preuve de (1) dans $\mathbf{CORC_i}$ on peut construire une preuve de (2) dans $\mathbf{CORCD_i}$. En effet, même si les principes intuitionnistes à la Brouwer ne sont pas admissibles d'un point de vue constructif minimal, ils donnent en général lieu à des règles de déduction correctes dans les théories formelles constructives (cf. par exemple dans [Bee] l'étude des principes de continuité dans les théories formelles constructives).

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

Bibliographie

[BB] Bishop E., Bridges D. : Constructive Analysis. (Springer-Verlag; 1985)

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

[Bee] Beeson M. : Foundations of Constructive Mathematics (Springer-Verlag; 1985)

[BKR] Ben-Or M., Kozen D., Reif J. : The complexity of elementary algebra and geometry. J. of Computation and Systems Sciences 32. 251-264 (1986).

[BR] Bridges D., Richman F. : Varieties of Constructive Mathematics. London Math. Soc. LNS 97. Cambridge University Press (1987)

[Coh] Cohen P. J. : Decision procedures for real and p-adic fields. Comm. in Pure and Applied Math. 22, p. 131-151 (1969)

[Col] Collins G.E. : Quantifier Elimination for real closed fields by cylindric algebraic decomposition. Second GI Conference on Automata Theory and Formal Languages. LNCS vol 33, 134-183, Springer-Verlag, Berlin (1975).

---

[25] Principes qui entrent en contradiction directe avec les mathématiques classiques, et ne sont pas admissibles

[Cos1] Coste M. : Ensembles semi-algébriques. in Géométrie algébrique réelle et formes quadratiques. Lect. Notes in Math. 959 (Springer 1975) p. 109-138.

[Cos2] Coste M. : Effective Semi-Algebraic Geometry, in Geometry and Robotics. Lect. Notes in Computer Science 391 (Springer 1989) p. 1-27.

[CR] Coste M., Roy M.-F. : Thom's lemma, the coding of real algebraic numbers and the computation of the topology of semi-algebraic sets. J. Symbolic Computation 5 , 121-129 (1988).

[Del] Delzell C. N. : A continuous, constructive solution to Hilbert's 17th problem. Inventiones mathematicae. 76, p. 365-384 (1984)

[GLRR] Gonzalez L., Lombardi H., Recio T., Roy M.-F. : Spécialisation de la suite de Sturm et sous-résultants. Version détaillée, dans CALSYF journées du GRECO de Calcul Formel 1989.

[Gri] Grigor'ev D. : Complexity of deciding Tarski algebra. J. Symbolic Computation 5 (1988) 65-108.

[Hol] Hollkott A. : Finite Konstruktion geordneter algebraischer Erweiterungen von geordneten Grundkörpen. Dissertation.Hamburg, 1941, p.1-65.

[Hör] Hörmander, L. : The analysis of linear partial differential operators, vol 2, Berlin, Heidelberg, New-York, Springer (1983). 364-367.

[HR] Harthong J., Reeb G. : Intuitionnisme 84. in : La Mathématique non standard (Fondements des Sciences) Editions du CNRS, Paris, 1989, p.213-252.

[HRS] Heintz J., Roy M.-F., Solerno P. : Sur la complexité du principe de Tarski-Seidenberg. A paraître au Bulletin de la S.M.F..

[Kre1] Kreisel, G. : Sums of squares. Summer Institute in Symbolic Logic. Cornell University. 313-320. (1957).

[Kre2] Kreisel, G. : Mathematical significance of consistency proofs. J. of Symbolic Logic. Vol 23, n°2, 155-182 (1958).

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

[Lom] Lombardi H. : Théorème des zéros réel effectif et variantes. Publications Mathématiques de Besançon 88-89. Fascicule n°1. Version anglaise moins détaillée : «Effective real Nullstellensatz and variants» à paraître dans les comptes rendus de MEGA 90, chez Birkhaüser.

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

[MN] Metakides G., Nerode A. : Effective content of field theory. Annals of Math. Logic 17, p 289-320, 1979.

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

[Pra] Prawitz D. : Ideas and results of proof theory. Proceedings of the second scandinavian logic symposium (juin 70). Studies in Logic and Foundations of Mathmatics n°63, 235-307. North Holland.

[Rob] Robinson, A. : On ordered fields and definite functions. Math. Ann. 130, p. 257-271 (1955).

[Tar] Tarski A. : A decision method for elementary algebra and geometry. Prepared for publication by J.C.C. Mac Kinsey, Berkeley (1951).
Le résultat était annoncé en 1931 dans : Sur les ensembles définissables de nombres réels I. Fundamenta mathematicae, vol 17, 210-239, 1931.

[San] Sander T. : Existence and uniqueness of the real closure of an ordered field. A paraître dans le Journal of Pure and Applied Algebra.

[Sco1] Scowcroft P. : The real-algebraic structure of Scott's model of intuitionistic analysis. Annals of Pure and Applied Logic, 27, (1984), 275-308.

[Sco2] Scowcroft P. : A transfer theorem in constructive real algebra. Annals of Pure and Applied Logic, 40, (1988), 29-87.

[Sco3] Scowcroft P. : Some continuous Positivstellensätze. Journal of Algebra, 124, (1989), 521-532.

[Sei] Seidenberg A. : A new decision method for elementary algebra. Ann. of Math. 60, p. 365-374 (1954)

[Ste] Stengle, G. : A Nullstellensatz and a Positivestellensatz in semialgebraic geometry. Math. Ann. 207, 87-97 (1974)

[Stu] Sturm C. : Mémoire sur la résolution des équations numériques. Inst. France Sc. Math. Phys. 6 (1835)

[Syl] Sylvester J. J. : On a theory of syzygetic relations of two rational integral functions, comprising an application to the theory of Sturm's function. Trans. Roy. Soc. London (1853).
reprint dans : Sylvester : Collected Math Papers. Chelsea Pub. Comp. NY 1983 vol 1 429-586

[VdW] Van der Waerden : Modern Algebra. Ungar, New-York. 1953. 2ème édition anglaise.

[Whi] Whiteley W. : Invariant computations for analytic projective geometry. 1989

[Zas] Zassenhaus H. : A real root calculus. pp. 383-392 in: Computational aspects in abstract algebra. Proceedings of a conference held at Oxford: 29th. August - 2nd September 1967. Ed. John Leech. Pergamon Press.

SPECIALISATION DE LA SUITE DE STURM ET SOUS-RESULTANTS

SPECIALISATION DE LA SUITE DE STURM ET SOUS-RESULTANTS (I) et (II)

Laureano GONZALEZ
Tomas RECIO
Mathématiques
Université de Santander
Espagne

Henri LOMBARDI
Laboratoire de Mathématiques
Université de Franche-Comté
25 030 Besançon cédex
France

Marie-Françoise ROY
I R M A R
Université de Rennes
35 042 Rennes cédex
France

Résumé

Le but de cet article composé de deux parties est de présenter et de comparer les différents algorithmes pour compter le nombre de racines réelles d'un polynôme et leurs généralisations. La clé pour comprendre les relations entre les diverses méthodes est l'étude de la suite de Sturm-Habicht, qui repose sur la théorie des polynômes sous-résultants.

Dans I.1. nous donnons le théorème de Sturm et sa généralisation.

Dans I.2. nous donnons une légère généralisation de la notion de polynôme sous-résultant de deux polynômes; ceci permet de simplifier les démonstrations concernant les polynômes sous-résultants, de préciser les algorithmes pour les calculer, et de traiter de manière agréable les problèmes de spécialisation, même lorsqu'il y a chute du degré (d'un ou même parfois des deux polynômes).

Dans le II.1. nous définissons et étudions la suite de Sturm-Habicht.

Dans le II.2. nous décrivons et comparons différentes méthodes pour compter le nombre de racines réelles d'un polynôme.

Mots clé

Sous-résultants, algorithme des sous-résultants, suite de Sturm, suite de Sturm-Habicht, spécialisation, nombre de racines réelles

Introduction

Nous présentons dans le I.1. une notion générale de suite de Sturm de deux polynômes P et Q et donnons ses propriétés. Si $Q = 1$, on retrouve le théorème de Sturm qui permet de déterminer le nombre de racines réelles d'un polynôme P . Dans le cas général on détermine la différence entre le nombre de racines réelles de P rendant Q (strictement) positif et le nombre de racines réelles de P rendant Q (strictement) négatif. Ces résultats, quoique peu connus, ont des sources classiques (cf. [Syl]). Nous indiquons ensuite les difficultés rencontrées lorsque on cherche à spécialiser ce calcul.

Dans le I.2. , nous étudions les polynômes sous-résultants. Nous donnons les résultats classiques de cette théorie, et nous précisons les relations entre la suite des sous-résultants et la suite des restes pour la division euclidienne. Nous introduisons une légère généralisation de la notion de polynôme sous-résultant. L'utilité de cette généralisation s'avère lorsque nous étudions les problèmes liés à la spécialisation dans le I.2.c ; en outre, les preuves de plusieurs résultats sont simplifiées.

Dans le I.2.c , nous indiquons comment se spécialisent ces polynômes sous-résultants.

Dans le I.2.d , nous donnons différentes variantes de l'algorithme des sous-résultants de Habicht-Loos.

Dans le II.1. , nous définissons la suite de Sturm-Habicht de deux polynômes qui est une sorte de suite de Sturm formelle. Nous démontrons par une méthode directe les résultats de Habicht et les améliorons, obtenant ainsi que la suite de Sturm-Habicht fait aussi bien l'affaire que la suite de Sturm pour compter le nombre de racines réelles d'un polynôme P (ou pour déterminer la différence entre le nombres de racines réelles de P rendant Q (strictement) positif et le nombre de racines réelles de P rendant Q (strictement) négatif). Nous indiquons comment se spécialise la suite de Sturm-Habicht et donnons un algorithme de calcul.

Dans le II.2. , nous présentons la méthode d'Hermite pour déterminer le nombres de racines réelles de P . Nous établissons un lien direct, purement algébrique, entre les résultats obtenus par cette méthode et ceux obtenus par la méthode de Sturm. La suite de Sturm-Habicht est la clé pour comprendre la situation. C'est aussi elle qui donne les calculs les plus généraux et les plus simples.

Quelques détails supplémentaires (dans les preuves, ou sur quelques points historiques) peuvent être trouvés dans [GLRR2].

I.1.) Suite de Sturm de deux polynômes

a) Définitions et notations

Suite des restes

Soient un anneau intègre **A** et son corps de fractions **K**. Nous noterons:

d(P): le degré d'un polynôme P,
cd(P): son coefficient dominant,
$\mathbf{cf}_j(P)$: son coefficient de degré j (égal à 0 si j est > d(P)).

Soient P et S deux polynômes à coefficients dans **A** . Nous noterons **Rst**(P,S) le reste de la division euclidienne de P par S dans **K**[X] . On a la relation :

$$\mathbf{Rst}(a.P,b.S) = a.\mathbf{Rst}(P,S)$$

Nous considérons maintenant la **suite des restes de l'algorithme d'Euclide**, démarrant avec le numéro 0 , et définie de manière récurrente par :

$$\mathbf{Rst}^0(P,S) := P, \qquad \mathbf{Rst}^1(P,S) := S,$$
$$\mathbf{Rst}^{m+1}(P,S) := \mathbf{Rst}(\mathbf{Rst}^{m-1}(P,S), \mathbf{Rst}^m(P,S))$$

On arrête la suite au plus petit entier n tel que $\mathbf{Rst}^{n+1}(P,S) = 0$.
Le polynôme $\mathbf{Rst}^m(P,S)$ est le **m-ième reste** de P et S .
Nous noterons par ailleurs $\mathbf{Rst}_j(P,S)$ le reste de degré j (avec $j < \inf(d(P),d(S))$, s'il existe, dans la suite des restes de l'algorithme d'Euclide. Nous prolongeons cette notation comme suit pour toutes les valeurs de $j \leq \sup(d(P),d(S)+1)$. Nous posons $t = \sup(d(P),d(S)+1)$, et nous définissons :

$$\mathbf{Rst}_t(P,S) := P \qquad \mathbf{Rst}_{t-1}(P,S) := S$$

et , pour $0 < j < t-1$:

$$\mathbf{Rst}_j(P,S) := \begin{cases} \mathbf{Rst}^m(P,S) & \text{si } j = d(\mathbf{Rst}^m(P,S)) \quad (m \geq 1) \\ \mathbf{Rst}^{m+1}(P,S) & \text{si } j+1 = d(\mathbf{Rst}^m(P,S)) \quad (m \geq 1) \\ 0 & \text{si ni j ni j+1 n'est le degré d'un reste } \mathbf{Rst}^m(P,S) \ (m \geq 1) \end{cases}$$

On remarquera que si j+1 et j sont les degrés de deux restes consécutifs, la définition reste cohérente. L'intérêt de cette définition-convention apparaîtra en I.2.b et I.2.c .

Remarque 1 :
Si un point a d'une extension de **K** n'est pas racine de P , il ne peut être racine de deux restes successifs. En effet le PGCD de deux restes successifs coincide avec le PGCD de P et S .

Suite des restes signés de P et S

Etant donnés deux polynômes P et S nous appelerons:

suite des restes signés de P et S

la suite des restes de l'algorithme d'Euclide (démarrant avec P et S) avec des modifications de signes convenables comme suit :

$$\boxed{\mathbf{Rss}^m(P,S) := (-1)^{\frac{m(m-1)}{2}} \mathbf{Rst}^m(P,S)}$$

de sorte qu'on ait la relation de récurrence :

$$\mathbf{Rss}^{m+1}(P,S) = -\,\mathbf{Rst}(\,\mathbf{Rss}^{m-1}(P,S)\,,\,\mathbf{Rss}^{m}(P,S)\,).$$

avec l'initialisation: $\mathbf{Rss}^{0}(P,S) := P, \qquad \mathbf{Rss}^{1}(P,S) := S,$

En posant $t = \sup(d(P),d(S)+1)$, nous notons également

$$\mathbf{Rss}_{t}(P,S) := P \qquad\qquad \mathbf{Rss}_{t-1}(P,S) := S$$

et, pour $0 < j < t-1$:

$$\mathbf{Rss}_j(P,S) := \begin{cases} \mathbf{Rss}^{m}(P,S) & \text{si } j = d(\mathbf{Rss}^{m}(P,S)) \quad (m \geq 1) \\ \mathbf{Rss}^{m+1}(P,S) & \text{si } j+1 = d(\mathbf{Rss}^{m}(P,S)) \quad (m \geq 1) \\ 0 & \text{si ni } j \text{ ni } j+1 \text{ n'est le degré d'un reste } \mathbf{Rss}^{m}(P,S) \quad (m \geq 1) \end{cases}$$

Suite de Sturm

Etant donnés deux polynômes P et Q nous appelerons:

suite de Sturm de P et Q

la suite des restes signés de P et $R := \mathbf{Rst}(P'Q,P)$:

$$\boxed{\mathbf{Stu}^{m}(P,Q) := \mathbf{Rss}^{m}(P,R)}$$

de sorte qu'on ait la relation de récurrence :

$$\mathbf{Stu}^{m+1}(P,Q) = -\mathbf{Rst}(\,\mathbf{Stu}^{m-1}(P,Q)\,,\,\mathbf{Stu}^{m}(P,Q)\,).$$

avec l'initialisation $\mathbf{Stu}^{0}(P,Q) = P, \quad \mathbf{Stu}^{1}(P,Q) = \mathbf{Rst}(P'Q,P).$

Nous notons de même

$$\boxed{\mathbf{Stu}_j(P,Q) := \mathbf{Rss}_j(P,R)} \quad \text{pour } j \leq d(P)$$

Si $Q = 1$ on note $\mathbf{Stu}^{m}(P,Q)$ et $\mathbf{Stu}_j(P,Q)$ respectivement $\mathbf{Stu}^{m}(P)$ et $\mathbf{Stu}_j(P)$ et on retrouve la notion classique de **suite de Sturm de P** .

Nombre de changements de signes

Toutes les définitions précédentes ont été faites en utilisant seulement la structure de corps de **K**. Nous allons maintenant introduire des notions qui nécessitent que le corps **K** soit muni d'un ordre. Supposons donc qu'on a fixé un ordre, noté $\leq$, sur le corps **K** et notons **R** la clôture réelle de **K** . Si **K** est réel clos, **R** coïncide avec **K** .

On définit le **nombre de changements de signes** $V(a_0,\ldots,a_n)$ dans une suite $(a_0,\ldots,a_n)$ d'éléments de **K** par récurrence sur n :

$V(a_0) = 0$,

$V(a_0,\ldots,a_{n+1}) = V(a_0,\ldots,a_n)$ si $(a_0,\ldots,a_n) = (0,\ldots,0)$ ou si a_{n+1} a le même signe que le dernier élément non nul de $(a_0,\ldots,a_n)$

$V(a_0,\ldots,a_{n+1}) = V(a_0,\ldots,a_n) + 1$ sinon.

Si $\mathbf{f} = [f_0,f_1,\ldots,f_n]$ est une suite de polynômes et si a et b sont deux éléments de $\mathbf{K} \cup \{+\infty\} \cup \{-\infty\}$ on appelera **nombre de changements de signes de $f_0,f_1,\ldots,f_n$ en x** et on notera:

$$V(\,f_0,f_1,\ldots,f_n\,;\,x\,) = V(\,\mathbf{f}\,;\,x\,) := V(\,f_0(x),f_1(x),\ldots,f_n(x)\,).$$

On appelera **différence des changements de signe dans la suite $f_0,f_1,\ldots,f_n$ entre a et b** la quantité:

$$V(\,f_0,f_1,\ldots,f_n\,;\,a,b\,) := V(\,f_0,f_1,\ldots,f_n\,;\,a\,) - V(\,f_0,f_1,\ldots,f_n\,;\,b\,).$$

NB : si $x = +\infty$ ou $-\infty$, le signe d'un polynôme $g(x)$ est donné par le signe du coefficient dominant de g et la parité de l'exposant correspondant.

Soient $a < b$ deux éléments de $\mathbf{K} \cup \{+\infty\} \cup \{-\infty\}$, on note :

$\mathbf{V_{Rss}}(P,S ; a)$ le nombre de changements de signes dans la suite des restes signés de P et S en a,
$\mathbf{V_{Rss}}(P,S ; a,b) := \mathbf{V_{Rss}}(P,S ; a) - \mathbf{V_{Rss}}(P,S ; b)$
$\mathbf{V_{Rss}}(P,S) := \mathbf{V_{Rss}}(P,S ; -\infty) - \mathbf{V_{Rss}}(P,S ; +\infty)$
$\mathbf{V_{Stu}}(P,Q ; a) := \mathbf{V_{Rss}}(P,R ; a)$, où $R = \mathbf{Rst}(P'Q,P)$
$\mathbf{V_{Stu}}(P,Q ; a,b) := \mathbf{V_{Rss}}(P,R ; a,b)$
$\mathbf{V_{Stu}}(P,Q) := \mathbf{V_{Rss}}(P,R)$.
$\mathbf{V_{Stu}}(P ; a) := \mathbf{V_{Stu}}(P,1 ; a)$
$\mathbf{V_{Stu}}(P ; a,b) := \mathbf{V_{Stu}}(P)$

Soient $a < b$ comme ci-dessus et $\varepsilon \in \{+, 0, -\}$, on note :

$\mathbf{c}_\varepsilon(P,Q;a,b)$ le nombre d'éléments de :
$\{u \in]a, b[\,/\, P(u) = 0 , \text{signe}(Q(u)) = \varepsilon\}$
$\mathbf{c}_\varepsilon(P,Q) := \mathbf{c}_\varepsilon(P,Q;-\infty,+\infty)$
$\mathbf{c}(P;a,b) := \mathbf{c}_+(P,1;a,b)$
$\mathbf{c}(P) := \mathbf{c}_+(P,1)$

b) Propriétés de la suite de Sturm

Théorème 1 (voir Sylvester [Syl] pour un résultat analogue) :

Soit un corps $\mathbf{K}$, soit $\leq$ un ordre sur $\mathbf{K}$ et soit $\mathbf{R}$ la clôture réelle de $\mathbf{K}$ muni de l'ordre $\leq$. Soient P et Q deux polynômes quelconques à coefficients dans $\mathbf{K}$ et a et b (avec $a < b$) des points de $\mathbf{K}$ qui ne sont pas racines de P. Alors:

(i) $\mathbf{V_{Stu}}(P,Q;a,b) = \mathbf{c}_+(P,Q;a,b) - \mathbf{c}_-(P,Q;a,b)$.

(ii) $\mathbf{V_{Stu}}(P,Q) = \mathbf{c}_+(P,Q) - \mathbf{c}_-(P,Q)$.

démonstration:
Soit $n+1$ la longueur de la suite de Sturm de P et Q, $\mathbf{Stu}^n(P,Q)$ est donc le dernier élément de cette suite et le PGCD de P et $P'Q$. Soit $\mathbf{f}$ la suite définie par $f_m = \mathbf{Stu}^m(P,Q)/\mathbf{Stu}^n(P,Q)$. La démonstration du théorème 1 est une conséquence immédiate des lemmes suivants, qu'il est facile de démontrer avec la stratégie classique pour la preuve du théorème de Sturm. ❑

Lemme 1:

Soient P et S deux polynômes quelconques à coefficients dans un corps ordonné $\mathbf{K}$. Soit $n+1$ la longueur de la suite des restes signés de P et S ; $\mathbf{Rss}^n(P,S)$ est donc le dernier élément de cette suite et le PGCD de P et S.

Soit $\mathbf{g}$ la suite définie par $g_m = \mathbf{Rss}^m(P,S)/\mathbf{Rss}^n(P,S)$.

Si c est une racine dans $\mathbf{R}$ de g_i, $i \neq 0$, il y a exactement un changement de signe dans la suite $(g_{i-1}(x), g_i(x), g_{i+1}(x))$ pour tout x suffisamment proche de c.

Lemme 2 :

(i) f_0 a pour racines les racines de P non racines de Q.

(ii) $V(\mathbf{f};x) = V_{\mathbf{Stu}}(P,Q\ ;\ x)$ pour x non zéro de P ,

(iii) le nombre $V(\mathbf{f};x)$ diminue de 1 quand on passe à droite d'une racine de f_0 avec Q positif et augmente de 1 quand on passe à droite d'une racine de f_0 avec Q négatif,

(iv) le nombre $V(\mathbf{f};x)$ ne change pas quand on passe à droite d'une racine de f_i (i=1,..,n) non racine de f_0 .

Corollaire 1 (théorème de Sturm [Stu]) :

Si a et b ne sont pas racines de P , $V_{\mathbf{Stu}}(P;a,b)$ est le nombre de racines dans **R** de P entre a et b . En particulier $V_{\mathbf{Stu}}(P)$ est le nombre de racines dans **R** de P .

Corollaire 2:

Si a et b ne sont pas racines de P, $V_{\mathbf{Stu}}(P,Q^2;a,b)$ est le nombre de racines dans **R** de P non racines de Q entre a et b.

Corollaire 3 On a donc les égalités :

$$V_{\mathbf{Stu}}(P;a,b) = \mathbf{c}_0(P,Q;a,b) + \mathbf{c}_+(P,Q;a,b) + \mathbf{c}_-(P,Q;a,b),$$
$$V_{\mathbf{Stu}}(P,Q^2;a,b) = \mathbf{c}_+(P,Q;a,b) + \mathbf{c}_-(P,Q;a,b),$$
$$V_{\mathbf{Stu}}(P,Q;a,b) = \mathbf{c}_+(P,Q;a,b) - \mathbf{c}_-(P,Q;a,b)$$

qui permettent de calculer $\mathbf{c}_0(P,Q;a,b)$, $\mathbf{c}_+(P,Q;a,b)$ et $\mathbf{c}_-(P,Q;a,b)$ connaissant $V_{\mathbf{Stu}}(P;a,b)$, $V_{\mathbf{Stu}}(P,Q^2;a,b)$ et $V_{\mathbf{Stu}}(P,Q;a,b)$.

Remarque 2 :

Dans l'article [Syl] , Sylvester étudie le nombre $V_{\mathbf{Rss}}(P, S)$ de changements de signe dans la suite des restes signés de deux polunômes P et S , au moins dans le cas où P et S sont sans facteurs carrés et sans racine commune, en termes du nombre d'entrecroissements entre les racines de P et celles de S . Nous pouvons donner l'interprétation suivante pour le nombre $V_{\mathbf{Rss}}(P,S\ ;\ a,b)$ lorsque P n'a que des racines simples sur l'intervalle: on suppose que $P(a).P(b) \neq 0$, on compte les racines de P sur l'intervalle en affectant à chaque racine de P un coefficient égal au signe de P'S . Le nombre trouvé est égal à $V_{\mathbf{Rss}}(P,S\ ;\ a,b)$. La preuve est essentiellement la même que celle du théorème 1 .

Remarque 3 :

Le calcul de la suite de Sturm se fait uniquement avec les opérations de corps de **K** . Le calcul du nombre $V_{\mathbf{Stu}}(P,Q;a,b)$ pour a et b deux éléments de **K** (et même le fait que $a < b$) dépendent du choix de l'ordre sur **K** . Le résultat obtenu concerne le nombre de racines dans le corps réel clos **R** entre a et b .

D'un point de vue algorithmique, ceci signifie que la suite de Sturm est calculable dès que les opérations de **K** le sont . La détermination du nombre des racines dans **R** entre a et b (a et b deux éléments de **K** non racines de P avec $a < b$ pour l'ordre choisi) s'obtient ensuite par un nombre fini de tests de signes portant sur des éléments de **K** , il est calculable dès que l'ordre sur **K** l'est (c'est-à-dire qu'il y a un algorithme exact pour déterminer le signe d'un élément). Tous les calculs et tests se déroulent donc dans **K** .

On peut en outre également appliquer le théorème de Sylvester si a et b sont des éléments de $\mathbf{R} \cup \{+\infty\} \cup \{-\infty\}$ et il est encore possible de déterminer exactement les signes dans **R** des polynômes de la suite de Sturm par des calculs dans **K** si a et b sont convenablement codés dans **K** (cf. par exemple [CoR])

Le résultat du calcul dépend naturellement de l'ordre choisi sur **K** : considérons par

rend X positif et plus petit que tout rationnel strictement positif, P a deux racines dans la clôture réelle de $\mathbb{Q}(X)$ pour cet ordre, alors que si l'ordre choisi sur $\mathbb{Q}(X)$ est celui qui rend X négatif et plus grand que tout rationnel strictement négatif, P n'a aucune racine dans la clôture réelle de $\mathbb{Q}(X)$ pour cet ordre.

c) Problèmes de spécialisation

Soient **A** un anneau intègre, **K** son corps de fractions, P et Q des polynômes de **K**[X] . Supposons qu'on ait effectué le calcul de la suite de Sturm dans le corps **K** , et qu'on spécialise les coefficients de P et Q , c'est-à-dire qu'on considère un morphisme Sp de **A** dans un anneau intègre **A'** et les images Sp(P) et Sp(Q) de P et Q dans l'anneau **A'**[X] . Un exemple typique de cette situation est $\mathbf{A} = \mathbb{Z}[Y]$ et $\mathbf{A'} = \mathbb{Z}[\xi]$ où ξ est un nombre algébrique.

La suite de Sturm associée à Sp(P) et Sp(Q) ne peut pas s'obtenir facilement à partir de celle de P et Q parce que dans le processus de division euclidienne de P et Q , il apparait des éléments de **A** au dénominateur, et que ces éléments peuvent très bien se spécialiser à 0 . Dans ce cas, la suite de Sturm de Sp(P) et Sp(Q) ne s'obtient pas en spécialisant la suite de Sturm de P et Q , et les degrés des polynômes de la suite de Sturm de Sp(P) et Sp(Q) ne coincident pas avec ceux de la suite de Sturm de P et Q . Il faut en principe recommencer tout le calcul.

Nous allons voir dans le paragraphe suivant que grâce à la théorie des sous-résultants on peut obtenir la suite des restes par un algorithme qui se spécialise bien. On pourra ainsi définir en II.1. la suite de Sturm-Habicht, qui permettra aussi de compter les racines dans **R** d'un polynôme et se comportera bien par spécialisation.

Exemple 1:

Considérons l'exemple du polynôme général de degré 4 ,

$$P = X^4 + pX^2 + qX + r \ .$$

La suite de Sturm de P et P' , calculée dans $\mathbb{Q}(p,q,r)[X]$ est

$$\mathbf{Stu}^0(P) = X^4 + pX^2 + qX + r$$

$$\mathbf{Stu}^1(P) = 4\ X^3 + 2pX + q$$

$$\mathbf{Stu}^2(P) = -\ (1/4)\ (\ 2pX^2 + 3qX + 4r)$$

$$\mathbf{Stu}^3(P) = -\ \frac{4(\ (2.p^3 - 8.pr + 9.q^2).X + p^2q + 12.qr\ )}{p^2}$$

$$\mathbf{Stu}^4(P) = \frac{p^2.(16.p^4r - 4.p^3q^2 - 128.p^2r^2 + 144.pq^2r - 27.q^4 + 256.r^3)}{4.(2.p^3 - 8.pr + 9.q^2)^2}$$

Lorsqu'on choisit des valeurs particulières $p\ ,\ q\ ,\ r$ pour p , q , r la suite de Sturm de $P = X^4 + p.X^2 + q.X + r$ s'obtient en général en substituant dans la suite de Sturm de P la valeur de P . Toutefois lorsqu'un des dénominateurs s'annule en $p\ ,\ q\ ,\ r$ cette substitution n'a plus de sens et il faut faire un nouveau calcul pour obtenir la suite de Sturm de P .

C'est ainsi que si $p = 0$, la suite de Sturm de $P = X^4 + qX + r$ est

$$\mathbf{Stu}^0(P) = X^4 + qX + r \qquad \mathbf{Stu}^1(P) = 4X^3 + q$$

$$\mathbf{Stu}^2(P) = \frac{3qX + 4r}{4} \qquad \mathbf{Stu}^3(P) = \frac{-(27q^4 + 256r^3)}{27q^3}$$

I. 2.) Polynômes sous-résultants

Il est clair qu'on ne peut plus parler de sous-résultants sans s'inspirer de l'article de synthèse de [Loo]. Nous serons cependant en désaccord avec lui sur certains points de détail. Pour la théorie des sous-résultants voir également [Br], [BroT], [Col] et [Hab]. Pour l'expression des sous-résultants en fonction des racines (point que nous n'abordons pas) voir [Syl], [Bor], [Las], [Cha].

a) Définitions

Nous rappelons dans ce § la notion de polynôme sous-résultant et en donnons une légère généralisation . L'utilité de cette généralisation s'avérera lorsque nous étudierons les problèmes liés à la spécialisation.

Nous établissons en outre les relations liant polynômes sous-résultants "ordinaires" et "généralisés".

On considère toujours un anneau intègre **A** et son corps de fractions **K** .

Si P et S sont dans **A**[X], p , s , et j des entiers avec $d(P) \le p$, $d(S) \le s$ et $j < \inf(p,s)$, nous notons $\mathbf{Sylv}_j(P,p,S,s)$ la j-ème matrice extraite de la matrice de Sylvester de P et S (considérés comme étant de degrés p et s) : sur la base $X^{p+s-j-1}$,..., X^2, X, 1, les vecteurs lignes successifs de cette matrice sont : $P.X^{s-j-1}$,..., P.X, P, $S.X^{p-j-1}$,..., S.X, S . Cette matrice possède p+s-2j lignes et p+s-j colonnes.

Si $P = a_p X^p + a_{p-1} X^{p-1} + ... + a_0$, $S = b_s X^s + b_{s-1} X^{s-1} + ... + b_0$, $\mathbf{Sylv}_j(P,p,S,s)$ est donc la matrice:

$$\mathbf{Sylv}_j(P,p,S,s) = \left[\begin{array}{c} \left.\begin{array}{cccccccc} a_p & \cdots & a_0 & 0 & \cdots & 0 & & \\ 0 & a_p & \cdots & a_0 & 0 & \cdots & 0 & \\ \vdots & \ddots & & \ddots & & \vdots & & \\ 0 & \cdots & 0 & a_p & \cdots & a_0 & 0 & \\ 0 & \cdots & 0 & a_p & \cdots & a_0 & & \end{array}\right\} s-j \text{ filas de P} \\ \left.\begin{array}{cccccccc} b_s & \cdots & b_0 & 0 & \cdots & 0 & & \\ 0 & b_s & \cdots & b_0 & 0 & \cdots & 0 & \\ \vdots & \ddots & & \ddots & & \vdots & & \\ 0 & \cdots & 0 & b_s & \cdots & b_0 & 0 & \\ 0 & \cdots & 0 & b_s & \cdots & b_0 & & \end{array}\right\} p-j \text{ filas de S} \end{array}\right\} p+s-2j \text{ filas}$$

$$\underbrace{\qquad\qquad\qquad\qquad}_{p+s-j \text{ columnas}}$$

Par définition, le **déterminant polynomial d'une matrice** possédant N lignes et M colonnes, avec $M \geq N$ est un polynôme de degré inférieur ou égal à $j = M-N$: son coefficient de degré d est le déterminant extrait de cette matrice sur les colonnes 1,2,...,N-1,M-d .

Les **polynômes sous-résultants** de P et S (considérés comme étant de degrés p et s) sont les déterminants polynomiaux des matrices $\mathbf{Sylv}_j(P,p,S,s)$ et ils seront notés:

$$\mathbf{Sres}_j(P,p,S,s)$$

On a la relation: $\mathbf{Sres}_j(a.P,p,b.S,s) = a^{s-j}.b^{p-j}.\mathbf{Sres}_j(P,p,S,s)$.

Il est clair que les polynômes sous-résultants sont à coefficients dans **A** et que $\mathbf{Sres}_j(P,p,S,s)$ est de degré inférieur ou égal à j . Si $\mathbf{Sres}_j(P,p,S,s)$ est de degré $< j$ on dit qu'il est **défectueux**.

Les **coefficients sous-résultants** de P et S (considérés comme étant de degrés p et s) sont les: $\mathbf{sr}_j(P,p,S,s) := \mathbf{cf}_j(\mathbf{Sres}_j(P,p,S,s))$.

Le coefficient sous-résultant $\mathbf{sr}_j(P,p,S,s)$ est nul si et seulement si le degré de $\mathbf{Sres}_j(P,p,S,s)$ est $< j$ (c.-à-d. si le polynôme sous-résultant est défectueux).

Le sous-résultant $\mathbf{Sres}_0(P,p,S,s) = \mathbf{sr}_0(P,p,S,s)$ est le résultant de P et S si $p = d(P)$ et $s = d(S)$.

La **suite des sous-résultants** est la liste des $\mathbf{Sres}_j(P,p,S,s)$ pour j descendant de $\inf(p,s)-1$ à 0 . Nous donnerons en 2.c une extension "raisonnable" de la suite des sous-résultants en la faisant démarrer à $j = p$, du moins lorsque $p > s = d(S)$.

Nous appelerons **polynôme sous-résultant standard** un polynôme sous-résultant $\mathbf{Sres}_j(P,p,S,s)$ où $d(P) = p$ et $d(S) = s \leq p$. Ordinairement les sous-résultants calculés seront les sous-résultants standards[1] avec $p = d(P)$ et $s = d(S)$. Mais après spécialisation, il se peut que le degré de P ou celui de S se retrouve diminué, aussi est-il intéressant d'étudier le comportement des sous-résultants dans le cas où l'un des deux degrés est plus petit que le degré annoncé. Si les deux degrés sont trop petits, tous les polynômes sous-résultants sont nuls. Les autres polynômes sous-résultants peuvent tous être facilement calculés à partir des polynômes sous-résultants standards (ou vice-versa si l'autre polynôme sous-résultant n'est pas identiquement nul). Les relations entre polynômes sous-résultants standards et polynômes sous-résultants découlent de la proposition suivante.

Proposition 1 :

Nous supposons $d(P) \leq p$, $d(S) \leq s$, $j < \inf(p,s)$

a) Si $d(P) < p$ et $d(S) < s$, alors

$$\mathbf{Sres}_j(P,p,S,s) = 0$$

b)
$$\mathbf{Sres}_j(P,p,S,s) = (-1)^{(p-j)(s-j)}\ \mathbf{Sres}_j(S,s,P,p) \quad \text{et en particulier}$$
$$\mathbf{Sres}_j(P,p,S,p-1) = \mathbf{Sres}_j(S,p-1,P,p) \qquad (d(S) \leq p-1)$$

c) Si $s' \geq s$ et $d(P) = p$ alors

(i) $\mathbf{Sres}_j(P,p,S,s') = cd(P)^{s'-s}\ .\ \mathbf{Sres}_j(P,p,S,s)$

(ii) $\mathbf{Sres}_j(S,s',P,p) = ((-1)^{p-j}\, cd(P))^{s'-s}\ .\ \mathbf{Sres}_j(S,s,P,p)$

démonstration:

Utiliser la définition des polynômes sous-résultants avec des propriétés élémentaires des déterminants. ❑

NB : Lorsque P est unitaire de degré p , la proposition 1 c) (i) montre que le polynôme sous-résultant $\mathbf{Sres}_j(P,p,S,s)$ ne dépend pas du choix de $s \geq d(S)$.

---

[1] Les polynômes

Proposition 2 :

Soient P et S des polynômes de degrés p et $s < p-1$, alors :

a) $\mathbf{Sres}_j(P,p,\ S,p-1) = 0$ si $s < j < p-1$

b) $\mathbf{Sres}_s(P,p,\ S,p-1) = (cd(P)\ cd(S))^{p-s-1}\ S$

c) $\mathbf{Sres}_j(P,p,\ S,p-1) = cd(P)^{p-s-1}\ \mathbf{Sres}_j(P,p,\ S,s)$ pour $j < s$

démonstration:

Utiliser la définition de polynômes sous-résultants avec des propriétés élémentaires des déterminants ❑

b) Polynômes sous-résultants, suite des restes et PGCD

Nous établissons dans ce § les formules reliant explicitement la suite des restes à la suite des polynômes sous-résultants standards.

Rappelons que l'on note **Rst**(P,S) le reste de la division de P par S. Lorsque $p = d(P) \geq s = d(S)$, le polynôme $cd(S)^{p-s+1}$. **Rst**(P,S) est appelé le **pseudo-reste** de la division de P par S, et nous le noterons **Prst**(P,S) . Le pseudo-reste est donc proportionnel (par un élément de **A**) au reste, et il est à coefficients dans **A** (cela résulte par exemple de la proposition 4 infra). On a la relation:

$$\mathbf{Prst}(a.P,b.S) = a.b^{p-s+1}.\mathbf{Prst}\ (P,S).$$

Dans tout le § nous noterons (H) l'hypothèse suivante :

(H) $p = d(P) \geq s = d(S)$, $R = \mathbf{Rst}(P,S)$, et $r = d(R)$

Nous commençons par une proposition qui sert de base aux calculs qui suivent[2]:

Proposition 3 : Supposons (H) et $j < s$, alors:

(i) $\mathbf{Sres}_j(P,p,\ S,s) = \mathbf{Sres}_j(R,p,\ S,s)$

(ii) $\mathbf{Sres}_j(S,s,\ P,p) = \mathbf{Sres}_j(S,s,\ R,p)$

démonstration :

par exemple (i) Chaque ligne $P.X^k$ de la matrice $\mathbf{Sylv}_j(P,p,\ S,s)$ peut être remplacée par la ligne $R.X^k$ en lui rajoutant des lignes $-c_m.S.X^{k+m}$, en choisissant pour c_m les coefficients du polynôme B dans l'identité de la division euclidienne: $P = B.S + R$. Ces manipulations élémentaires ne modifient pas les déterminants extraits. Or, la nouvelle matrice obtenue n'est autre que $\mathbf{Sylv}_j(R,p,S,s)$. ❑

Proposition 4 : Lorsque $p = d(P) \geq s = d(S)$, on a les égalités

(i) $\mathbf{Sres}_{s-1}(S,s,\ P,p) = \mathbf{Prst}\ (P,S)$

(ii) $\mathbf{Sres}_{s-1}(P,p,\ S,p-1) = (-cd(P))^{p-s-1}\ \mathbf{Prst}\ (P,S)$

(iii) Si S est unitaire et $p' \geq p$ on a :

$\mathbf{Sres}_{s-1}(S,s,\ P,p') = \mathbf{Sres}_{s-1}(S,s,\ P,p) = \mathbf{Prst}\ (P,S) = \mathbf{Rst}(P,S)$

démonstration:

Utiliser les résultats des propositions 1,2 et 3. ❑

---

[2] En fait, tous les résultats des § b et c sont basés sur l'utilisation systématique des propositions 1 , 2 , 3

Le cas ordinaire

C'est le cas où les degrés dans la suite des restes baissent de un en un.

Proposition 5 : Supposons (H) et $p = s+1$. Alors nous avons:

a) $\mathbf{Sres}_{s-1}(P,p,\ S,s) = cd(S)^2\ R = \mathbf{Prst}\ (P,S)$

b) $\mathbf{Sres}_j(P,p,\ S,s) = cd(S)^2\ \mathbf{Sres}_j(S,s,\ R,s-1)$ pour $j < s-1$

Proposition 6 : Supposons (H), et que les degrés dans la suite des restes décroissent de un en un (en commençant au polynôme P). Posons $c(s) := cd(S)$ et, pour $j < s$, $c(j) := cd(\mathbf{Rst}_j)$. Alors :

$$\mathbf{Sres}_j(P,p,\ S,s) = (\ c(s).c(s-1)...c(j+1)\ )^2\ \mathbf{Rst}_j(P,S) \quad \text{pour } j < s\ .$$

En particulier, chaque polynôme sous-résultant est égal, à un carré dans **K** près, au reste correspondant.

démonstration des propositions 5 et 6:
La proposition 6 résulte de la proposition 5 , par induction sur j . La proposition 5a est un cas particulier de la proposition 4 (i) . La proposition 5b s'obtient en appliquant la proposition 3 puis les propositions 1b et 1c(i) . ❑

Le théorème de Habicht

Nous redémontrons maintenant le "théorème de Habicht" dans [Loo] par un calcul direct.

Théorème 2 (**théorème de Habicht** [Hab]) :

Nous supposons $d(P) \le p = s+1$, $d(S) \le s$.

Nous posons $S_p := P$, $S_s := S$, $S_j := \mathbf{Sres}_j(P,p,\ S,s)$ pour $j < s$,

$C(p) := 1$, $C(j) := \mathbf{cf}_j(S_j) =$ pour $j \le s$.

(i) Alors, pour $0 \le h < j \le s$, on a :

$$C(j+1)^{2(j-h)}\ S_h = \mathbf{Sres}_h(S_{j+1}\ j+1,\ S_j,j).$$

(ii) En particulier, lorsque $j < s$ on obtient

$$\mathbf{sr}_{j+1}(P,p,\ S,s)^{2(j-h)}\ S_h = \mathbf{Sres}_h(S_{j+1},j+1,\ S_j,j)$$

(iii) Si $d(S_{j+1}) = j+1$ et $d(S_j) = j \le s$, on obtient:

$$C(j+1)^2\ S_{j-1} = \mathbf{Prst}\ (S_{j+1},S_j)$$

démonstration:[3]

(ii) est la même chose que (i)

(iii) résulte de (i), avec $h = j-1$, et de la proposition 4 (i) .

(i) Les égalités à démontrer sont des identités algébriques. On peut donc supposer que les coefficients de P et S sont des *variables indépendantes*. On applique alors les résultats de la proposition 6 . Les deux membres de l'égalité à établir sont des multiples de $\mathbf{Rst}_h$. Les calculs sont simples. Nous les explicitons en reprenant les notations de la proposition 6 .

Nous posons $R_j := \mathbf{Rst}_j(P,S)$, $\gamma(j) := (\ c(s).c(s-1)...c(j+1)\ )^2 = C(j)/c(j)$.

On a donc $C(j+1)^2 = \gamma(j).\gamma(j+1)$, $S_j = \gamma(j).R_j$.

Par ailleurs $\mathbf{Sres}_h(S_{j+1},j+1,\ S_j,j) = \gamma(j+1)^{j-h}.\gamma(j)^{j-h+1}\mathbf{Sres}_h(R_{j+1},j+1,\ R_j,j)$

---

[3] Pour que le théorème affirme autre chose que des identités [illegible]

$$= \gamma(j+1)^{j-h}.\gamma(j)^{j-h+1}.(\,c(j).c(j-1)...c(h+1)\,)^2 R_h$$
$$= \gamma(j+1)^{j-h}.\gamma(j)^{j-h}.\gamma(h).R_h$$

et $S_h = \gamma(h).R_h$ ❑

Le cas défectueux

Proposition 7 : Supposons (H) . On a:

a) (i) $\mathbf{Sres}_{s-1}(P,p,\ S,s) = (-\,cd(S)\,)^{p-s+1}\ R\ = (-\,1)^{p-s+1}\ \mathbf{Prst}\ (P,S)$

(ii) $\mathbf{Sres}_j(P,p,\ S,s) = ((-\,1)^{s-j}\,cd(S))^{p-s+1}\ \mathbf{Sres}_j(S,s,\ R,s-1)$ pour $j < s-1$

b) On en déduit

(i) $\mathbf{Sres}_j(P,p,\ S,s) = 0$ si $r < j < s-1$

(ii) $\mathbf{Sres}_r(P,p,\ S,s) = (\,(-\,1)^{p-s-1}\ cd(S).cd(R)\,)^{s-r-1}\ \mathbf{Sres}_{s-1}(P,p,\ S,s)$

(iii) $\mathbf{Sres}_j(P,p,\ S,s) = (-\,1)^{(p-s-1)(s-j)}\,cd(S)^{p-r}\ \mathbf{Sres}_j(S,s,\ R,r)$ pour $j < r$

démonstration :
Les égalités de a) et b) sont conséquences des propositions 1,2 et 3. ❑

Proposition 8 :

Supposons (H) , et définissons $R_{-1} := P$, $R_0 := S$, $R_i := \mathbf{Rst}^{i+1}(P,S)$

$d_i = d(R_i)$, $e_i = d_{i-1} - d_i + 1$, $f_i = d_{i-1} - d_{i+1}$, $c_i = cd(R_i)$

alors, pour tout degré $d_i \leq s$, on a:

$$R_{i+1} = \mathbf{Sres}_{d_i - 1}\ (P,p,\ S,s)\ /\ (\varepsilon_i\ .\ c_0^{f_0}.\ c_1^{f_1}.....c_{i-1}^{f_{i-1}}.\ c_i^{e_i}\ )$$

où $\varepsilon_i = 1$ si $\Sigma_{0\leq k\leq i}\,(1+ d_k - d_i\,).e_k$ est pair , -1 sinon.

démonstration:
Se démontre par récurrence sur j en utilisant la proposition 7 . On amorce la pompe avec a) (i) et la récurrence fonctionne grâce à b) (iii). ❑

Sous-résultants et restes

Théorème 3 (sous-résultants et restes [Hab] [Loo]):

a) Supposons (H) . Soit $j < s$. Le polynôme $\mathbf{Sres}_j(P,p,S,s)$ est égal , à un facteur non nul près dans **K** , à $\mathbf{Rst}_j(P,S)$ [4].

b) Ce résultat reste vrai si $d(P) \leq p$, $d(S) \leq s$, l'une des deux inégalités étant une égalité, et $j < \inf(d(P),d(S))$, ou encore si $d(P) = p > s > j \geq d(S)$.

démonstration :

a) c'est vérifié pour $j = s - 1, \ldots , r$ d'après la proposition 7 , alinéas b (i) et b (ii) . Pour $j < r$ on utilise l'alinéa b (iii) qui nous ramène au cas de la suite des restes démarrant avec S et R . (preuve par induction sur le degré de P donc) .

b) la proposition 1 c) montre que $\mathbf{Sres}_j(P,p,\ S,s)$ et $\mathbf{Sres}_j(P,d(P),\ S,d(S))$ sont proportionnels avec un facteur non nul pour $j < \inf(d(P),d(S))$. Par ailleurs, si $d(P) = p > s > j \geq d(S)$, on a

4 On voit ici l'utilité de la définition [illegible]

$$\begin{aligned} \mathrm{cd}(P)^{p-s-1}\ \mathbf{Sres}_j(P,p,\ S,s) &= \mathbf{Sres}_j(P,p,\ S,p-1) && \text{(prop 1 c (i))}\\ &= 0 \text{ si } d(S) < j < p-1 && \text{(prop 2 a)}\\ &\quad (\ \mathrm{cd}(P)\ \mathrm{cd}(S)\ )^{p-s-1}\ S \text{ si } j=d(S) && \text{(prop 2 b)}\\ &\quad \text{(et par définition on a } \mathbf{Rst}_{d(S)}(P,S) = S\ ) \quad \square \end{aligned}$$

Corollaire : Supposons que $s = d(S)$ ou $p = d(P)$, et que S ne divise pas P (c.-à-d. $\mathbf{Sres}_{s-1}(P,p,\ S,s) \neq 0$) . Alors le dernier sous-résultant non nul $\mathbf{Sres}_n(P,p,S,s)$ est de degré n (c.-à-d.: non défectueux). Il est égal au PGCD de P et S dans $\mathbf{K}[X]$.

démonstration:

Cela résulte du théorème 3 et du fait que le dernier reste non nul dans la suite des restes est le PGCD de P et S . $\square$

Le théorème des sous-résultants

Le théorème suivant complète le théorème de Habicht dans le cas défectueux.

Théorème 4 (théorème des sous-résultants [Hab], [Loo]) :

Nous supposons $d(P) \leq p = s+1$, $d(S) \leq s$, l'une des 2 inégalités étant une égalité.

a) Si $j < s-1$ avec $\mathbf{Sres}_{j+1}(P,p,\ S,s)$ non défectueux et $\mathbf{Sres}_j(P,p,\ S,s)$ défectueux, de degré k , alors $\mathbf{Sres}_k(P,p,\ S,s)$ est proportionnel à $\mathbf{Sres}_j(P,p,\ S,s)$ avec un facteur non nul. (en particulier $\mathbf{Sres}_k(P,p,\ S,s)$ n'est pas défectueux).

b) Plus précisément , avec les mêmes hypothèses, en notant $S_h := \mathbf{Sres}_h(P,p,\ S,s)$ ($h < s$) on a les relations :

(i) $\quad \mathrm{cd}(S_j)^{(j-k)}\ S_j = \mathrm{cd}(S_{j+1})^{(j-k)}\ S_k.$

(ii) $\quad S_{k+1} = \ldots\ldots = S_{j-1} = 0 \qquad$ (si $k < j-1$).

(iii) $\quad (\ -\mathrm{cd}(S_{j+1}))^{(j-k+2)}\ S_{k-1} = \mathbf{Prst}(S_{j+1},S_j).$

démonstration :

a) et b) (ii) : déjà énoncés (sous une autre forme) dans le théorème 3 lorsqu'on est dans l'une des hypothèses de ce théorème. De manière générale, le a) résulte du b) qui se démontre directement à partir du théorème de Habicht comme suit :

b) (i) le th. de Habicht nous donne : $\mathrm{cd}(S_{j+1})^{2(j-k)}\ S_k = \mathbf{Sres}_k(S_{j+1},j+1,\ S_j,j)$, et la prop 2b :

$$\mathbf{Sres}_k\ (S_{j+1}\ ,\ j+1,\ S_j\ ,\ j\ ) = (\ \mathrm{cd}(S_j).\mathrm{cd}(S_{j+1})\ )^{j-k}\ S_j$$

b) (iii) le th. de Habicht nous donne : $\mathrm{cd}(S_{j+1})^{2(j-k+1)}\ S_{k-1} = \mathbf{Sres}_{k-1}(S_{j+1},j+1,\ S_j,j)$, et la proposition 4 (ii) :

$$\mathbf{Sres}_{k-1}\ (S_{j+1}\ ,\ j+1,\ S_j\ ,\ j\ ) = (-\mathrm{cd}(S_{j+1})\ )^{j-k}\ \mathbf{Prst}(S_{j+1},S_j)$$

b) (ii) on applique le théorème de Habicht comme ci-dessus et on conclut par la prop 2 a) .

$\square$

c) Spécialisation des polynômes sous-résultants

Nous venons de voir que la suite des sous-résultants nous donne la suite des restes. Etant donnée une spécialisation (i.e. un homomorphisme d'anneaux) $Sp: \mathbf{A} \rightarrow \mathbf{A}'$, nous étudions la possibilité de calculer "facilement" les polynômes sous-résultants standards de $Sp(P)$ et $Sp(S)$ lorsqu'on connaît les polynômes sous-résultants standards de P et S (polynômes de $\mathbf{A}[X]$). La situation typique de spécialisation que nous avons en tête est naturellement l'application définie par l'évaluation de certaines variables indépendantes en des

nombres algébriques. On aura ainsi la suite des restes dans la situation spécialisée sans avoir besoin de refaire un nouveau calcul.

Comportement des polynômes sous-résultants par spécialisation

1er cas : *les degrés de P et S sont conservés au cours d'une spécialisation*

Les polynômes sous-résultants standards se spécialisent en les polynômes sous-résultants standards.

2ème cas : *un seul des deux degrés de P ou S s'abaisse au cours d'une spécialisation*

Supposons que nous ayons déjà calculé les polynômes sous-résultants $\mathbf{Sres}_j(P,p,S,p-1)$.

Si $d(Sp(P)) = d(P)$, on obtient en spécialisant ces polynômes sous-résultants une suite de polynômes sous-résultants non tous nuls, même si $d(Sp(S)) < d(S)$.

Par contre, si $d(Sp(S)) = d(S) = s < p-1$ et $d(Sp(P)) < d(P)$, on a pour tout j $Sp(\mathbf{Sres}_j(P,p, S,p-1)) = 0$. Il suffit cependant de calculer $\mathbf{Sres}_j(P,p, S,s)$ à partir de $\mathbf{Sres}_j(P,p, S,p-1)$ en utilisant la proposition 1 pour obtenir par spécialisation des polynômes sous-résultants non nuls.

3ème cas : *les degrés de P et S s'abaissent de 1 pour une raison commune*

Nous supposons que cd(P) et cd(S) s'écrivent respectivement: $cd(P) = a.c_p$ et $cd(S) = a.d_s$ avec $Sp(a) = 0$. Plus précisément nous écrivons:

$P = a.c_p X^p + a_{p-1} X^{p-1} + \ldots$, $S = a.d_s X^s + b_{s-1} X^{s-1} + \ldots$ et nous supposons que le déterminant $\boxed{d = c_p b_{s-1} - d_s a_{p-1}}$ se spécialise non nul.

Cette situation se rencontre souvent dans l'important cas particulier où S est égal à la dérivée de P (lorsque $Sp(a_p) = 0$ et $Sp(a_{p-1}) \neq 0$) .

Proposition 9 : Avec les hypothèses ci-dessus, et $p \geq s$

a) $Sp(\mathbf{Sres}_{s-1}(P,p, S,s) / a) = Sp(d \,.\, b_{s-1}{}^{p-s-1} \,.\, S)$.

b) $Sp(\mathbf{Sres}_j(P,p, S,s) / a) = (-1)^{s-j+1}.Sp(d).\, \mathbf{Sres}_j(Sp(P),p-1,\, Sp(S),s-1)$

pour $j < s-1$

démonstration:

L'étude détaillée de la structure des matrices $\mathbf{Sylv}_{s-1}(P,p, S,s)$ et $\mathbf{Sylv}_j(P,p, S,s)$ après spécialisation donne les égalités a) et b). ❑

4ème cas : *les degrés de P et S s'abaissent de manière "incontrôlée"*

On n'obtient rien par spécialisation "directe".

Néanmoins, si les divisions exactes sont nettement plus faciles dans A que dans A', on aura intérêt à poser S_s:= S tronqué au dessus du degré de Sp(S), P_p:= P tronqué au dessus du degré de Sp(P), à calculer les polynômes sous-résultants de P_p et S_s , et spécialiser pour terminer.

d) Algorithmes de calculs et complexité

Algorithmes de calcul

Présentons maintenant les algorithmes de calculs qui se déduisent des résultats précédents. *Ces algorithmes utilisent uniquement des calculs de pseudo-restes et des divisions exactes.*

Nous commençons par un algorithme qui se déduit directement du théorème de Habicht et du théorème des sous-résultants (théorème 4):

Algorithme 1: [5]

Nous supposons $d(P) = p = n+1$, $d(S) = s \leq n$.

Nous posons $S_{n+1} := P$, $S_n := S$, et $S_j := \mathbf{Sres}_j(P,n+1, S,n)$ pour $j < n$.

entrées : les polynômes P et S

sortie : la suite des sous-résultants S_j $\quad (0 \leq j \leq s)$

initialisation :

– si $s = n$	$S_{s-1} := \mathbf{Prst}(P,S)$; $\quad S_s := S$		(0)
– si $s < n$	$S_s := (cd(P)\, cd(S))^{n-s}\, S$		(1)
	$S_{s-1} := (-cd(P))^{n-s} \,.\, \mathbf{Prst}(P,S)$		(2)
	en outre si $s < n-1$ et $s < k < n$: $S_k := 0$		(3)
–	$j := s - 1$		

étape suivante : {$1 \leq j \leq s-1$, S_{j+1} et S_j sont supposés déjà calculés, avec $d(S_{j+1}) = j+1$ et $h = d(S_j)$. On va calculer les S_k manquants jusqu'à S_{h-1} }

–	$h := d(S_j)$		
– si $h = j$	$S_{h-1} := \mathbf{Prst}(S_{j+1}, S_j) / cd(S_{j+1})^2$		(4)
– si $h < j$	$S_h := S_j . cd(S_j)^{j-h} / cd(S_{j+1})^{j-h}$		(5) (*)
	$S_{h-1} := \mathbf{Prst}(S_{j+1}, S_j) / (-cd(S_{j+1}))^{j-h+2}$		(6) (*)
	en outre si $h < j-1$ et $h < k < j$: $\quad S_k := 0$		(7)
–	$j := h - 1$		

fin : l'algorithme se termine lorsqu'on a calculé S_0 c.-à-d. lorsque $j \leq 0$

(*) (5) n'est pas exécuté si $h = -1$ (6) n'est pas exécuté si $h \leq 0$ ❑

démonstration:
L'initialisation est conséquence des propositions 2 et 4 et la suite des théorèmes de Habicht et des sous-résultants. ❑

Remarque 4 :
Si $j = h$ l'affectation (5) donnerait $S_j := S_j$. Et l'affectation (6) produirait le même effet que la (4)

---

[5] Cet algorithme calcule les polynômes sous-résultants $\mathbf{Sres}_j(P,n+1, S,n)$ lorsque $d(P) = n+1 > d(S)$. Le Subresultant Theorem p 122 de [Loo] semble, en première lecture, concerner ces sous-résultants, puisque p 121, ce sont ces sous-résultants (obtenus par spécialisation d'une suite où P et S sont formellement de degrés n+1 et n) qui sont considérés ... En fait le Subresultant Theorem est correct avec les $\mathbf{Sres}_j(P,n+1, S,s)$ lorsque $n = p-1 \geq s$, il est par contre incorrect lorsque $p \leq s$. (Cf la note bas de page n° 9 au sujet de l'algorithme n°3)

On remarque maintenant que les formules récurrentes (4) (5) (6) (7) sont homogènes. Si , en dessous d'un certain degré k , on sait que les S_j sont tous multiples d'une constante c de A , les formules sont encore valables si on remplace les polynômes S_j par les S_j / c. Nous en déduisons, lorsque p = d(P) , s = d(S) ≤ n = p − 1 , un algorithme pour calculer les sous-résultants standards $\mathbf{Sres}_j(P,p, S,s) = \mathbf{Sres}_j(P,p, S,n) / cd(P)^{n-s}$ (cf. proposition 1 c)) . On notera que l'algorithme ne diffère du précédent que lorsque s < n , et seulement dans la partie "initialisation".

Algorithme 2 : Calcul des polynômes sous-résultants standards
(cas d(S) < d(P))

Nous supposons d(P) = p = n+1 , d(S) = s ≤ n. Nous posons $S_p := P$, $S_n := S$, $S_s := cd(S)^{n-s} S$, et $S_j := \mathbf{Sres}_j(P,p, S,s)$ pour j < s.

entrées : les polynômes P et S

sortie : la suite des sous-résultants standards S_j (0 ≤ j ≤ s)

initialisation :

- p := d(P), s := d(S) , n := p − 1 ,
- $S_s := cd(S)^{n-s} S$ (1)
- $S_{s-1} := (-1)^{n-s}$. **Prst** (P,S) (2)
- j := s-1

étape suivante et **fin** : comme dans l'algorithme n°1 ❑

On peut maintenant essayer de faire rentrer les affectations (1) et (2) dans le moule: (5) et (6). C'est possible en prenant j = n , h = s , et en faisant l'affectation $cd(S_{n+1}) := 1$ (qui est "fausse"). Avec cette philosophie, la suite des sous-résultants commence à $S_{n+1} = P$ et il faut poser $S_k := 0$ si s < k < p-1. L'avantage est que les seules initialisations sont : $S_{n+1} := P$, $S_n := S$, "$cd(S_{n+1}) := 1$" . Et on passe directement à "étape suivante". Aussi ferons nous désormais la convention suivante:

Définition (convention) : Si p ≥ d(P) , s = d(S) et p > s, on pose:

$\mathbf{Sres}_p(P,p, S,s) := P$, $\mathbf{Sres}_{p-1}(P,p, S,s) := S$,

$\mathbf{Sres}_s(P,p, S,s) := cd(S)^{p-1-s} . S$,

$\mathbf{Sres}_k(P,p, S,s) := 0$ si s < k < p-1,

$\mathbf{sr}_p(P,p, S,s) := 1$, $\mathbf{sr}_j(P,p, S,s) := \mathbf{cf}_j(\mathbf{Sres}_j(P,p, S,s))$ si j < p.

Remarque 5 :
On notera qu'avec cette convention, de nombreux "cas distincts" dans les propositions établies précédemment "fusionnent" :

- proposition 2 : a) et b) sont des cas particuliers de c)
- proposition 5 : a) est un cas particulier de b)
- théorème de Habicht : définition "uniforme" pour les S_j et les C(j)
- proposition 7 : a) (i) est un cas particulier de a) (ii) , b) (i) et b) (ii) sont des cas particuliers de b) (iii)
- proposition 9 : a) est un cas particulier de b)

En outre remarquons que

- la proposition 1 c) (i) reste vraie dans les cas j = s = d(S) < p et d(S) = s < j < inf(s',p − 1)

– la proposition 1 c) (ii) reste vraie dans le cas $j = p < s$ mais serait fausse pour $p < j = s < s'$ ou $p < j = s - 1 < s < s'$ [6]

Nous donnons maintenant une généralisation de l'algorithme précédent, conformément à la définition-convention ci-dessus.

Algorithme 3 : Algorithme généralisé des polynômes sous-résultants [7]

Nous supposons $p \geq d(P)$, $s = d(S)$ et $p > s$

Nous posons pour $j \leq p$: $S_j := \mathbf{Sres}_j(P,p,S,s)$, $t_j := \mathbf{sr}_j(P,p,S,s)$

entrées : les polynômes P et S , l'entier $p \geq d(P)$

sortie : la suite des polynômes sous-résultants S_j $(0 \leq j \leq p)$

initialisation :

– $S_p := P$; $t_p := 1$

– $S_{p-1} := S$

– $j := p - 1$

étape suivante : { $1 \leq j \leq n$, S_{j+1} , t_{j+1} et S_j sont supposés déjà calculés, S_{j+1} et t_{j+1} non nuls, avec $h = d(S_j)$. On va calculer les S_k manquants jusqu'à S_{h-1} }

– $h := d(S_j)$

– si $h = j$ $S_{h-1} := \mathbf{Sres}_{h-1}(S_j, h, S_{j+1}, j+1) / t_{j+1}^2$; (4)

– si $h < j$ $S_h := S_j . \mathbf{cf}_h(S_j)^{j-h} / t_{j+1}^{j-h}$; (5) (*)

$S_{h-1} := \mathbf{Sres}_{h-1}(S_j, h, S_{j+1}, j+1) / (-t_{j+1})^{j-h+2}$ (6) (*)

en outre si $h < j-1$ et $h < k < j$: $S_k := 0$ (7)

– $j := h - 1$; $t_{j+1} := \mathbf{cf}_{j+1}(S_{j+1})$ [8]

fin : l'algorithme se termine lorsqu'on a calculé S_0 c.-à-d. lorsque $j \leq 0$

(*) (5) n'est pas exécuté si $h = -1$ (6) n'est pas exécuté si $h \leq 0$

NB: On notera que dans (4) et (6) on peut toujours remplacer $\mathbf{Sres}_{h-1}(S_j,h,S_{j+1},j+1)$ par $\mathbf{Prst}(S_{j+1},S_j)$ sauf lors du premier passage[9] si $d(P) < p$. En particulier, si $d(P) = p > s = d(S)$, le théorème 4 (théorème des sous-résultants) reste vrai avec tout $j < p$ (au lieu de $j < s - 1$) . Dans le cas $p > s = d(S)$, $p \geq d(P)$, le théorème 4 reste vrai à condition de remplacer dans b) (iii) $\mathbf{Prst}(S_{j+1},S_j)$ par $\mathbf{Sres}_{h-1}(S_j,h,S_{j+1},j+1)$.
En outre, on a toujours l'égalité: $\mathbf{Sres}_{h-1}(S_j,h,S_{j+1},j+1) = \mathbf{cf}_h(S_j)^{j-h+2}\,\mathbf{Rst}(S_{j+1},S_j)$

---

6 Ainsi la convention concernant $\mathbf{Sres}_s(P,p,S,s)$ pour $s = d(S) < p$ tient correctement la route par rapport aux égalités générales données dans la prop 1 . Il en va de même avec les polynômes sous-résultants identiquement nuls pour $s < j < p - 1$. La lecture des propositions 1 c) et 2 a) et b) pouvait d'ailleurs inciter à poser ces conventions au tout début de l'article. Il en va tout différemment en ce qui concerne la convention $\mathbf{Sres}_{p-1}(P,p,S,s) = S$. Supposons en effet $p = d(P)$, $s = d(S)$, $p > s+1$: l'égalité $\mathbf{Sres}_{p-1}(P,p,S,p) = cd(P)\,S$ inciterait à poser, vue la proposition 1 c(i) , $\mathbf{Sres}_{p-1}(P,p,S,s) := S/cd(P)^{p-s-1}$ tandis que l'égalité $\mathbf{Sres}_{p-1}(P,p+1,S,s) = 0$ inciterait à poser, elle, vue 1 c(ii) , $\mathbf{Sres}_{p-1}(P,p,S,s) := 0$. La même critique vaut pour la convention concernant le sous-résultants $\mathbf{Sres}_p(P,p,S,s)$.

7 Le Subresultant Chain Algorithm dans [Loo] est celui-ci lorsque $p = d(P) > d(S)$.

8 Cette affectation pourrait aussi s'écrire $t_h := \mathbf{cf}_h(S_h)$

9 Dans le Subresultant Theorem et le Subresultant Chain Algorithm de [Loo] , c'est toujours $\mathbf{Prst}(S_{j+1},S_j)$ qui intervient. Or ce polynôme n'est défini que pour $d(S_{j+1}) \geq d(S_j)$. En conséquence le Subresultant Theorem et le Subresultant Chain Algorithm sont "illisibles" pour $d(P) < d(S)$ et incorrects pour $d(P) = d(S)$. On notera également que l'on ne trouve pas dans [Loo] de définition explicite des

On peut déduire de l'algorithme précédent un algorithme pour les sous-résultants standards dans le cas où $d(P) = d(S)$. Il ne diffère de celui donné pour le cas $d(P) > d(S)$ que dans la partie "initialisation".

Algorithme 4 : Calcul des polynômes sous-résultants standards (cas où $d(S) = d(P)$)

Nous supposons $d(P) = d(S) = s$.

Nous posons $S_j := \mathbf{Sres}_j(P,s, S,s)$ pour $j < s$.

entrées : les polynômes P et S

sortie : la suite des sous-résultants standards S_j ($0 \leq j < s$)

initialisation :

–	$S_{s-1} := \mathbf{Prst}(S,P)$, $t := d(S_{s-1})$		(1)
– si $t = s-1$	$S_{s-2} := \mathbf{Prst}(P, S_{s-1}) / cd(P)$		(2)
– si $t < s-1$	on calcule S_t et S_{t-1} comme suit		
	$S_t := cd(S_{s-1})^{s-1-t} . S_{s-1}$		(1 bis)
	$S_{t-1} := (-1)^{s-1-t} . \mathbf{Prst}(P, S_{s-1}) / cd(P)$		(2 bis)
	en outre si $t < s-2$ et $t < k < s-1$:	$S_k := 0$	(3)
–	$j := t-1$		

étape suivante et **fin** : comme dans l'algorithme n°1

Nous présentons enfin un algorithme qui constitue une amélioration de l'algorithme n°2 lorsque cd(P) et cd(S) sont divisibles par un même élément c de **A** .

Algorithme n°5 : (cas $d(S) < d(P)$, cd(P) et cd(S) divisibles par un même élément c de **A**)

Nous supposons $d(P) = p = n+1$, $d(S) = s \leq n$, cd(P) et cd(S) divisibles par un même élément c de **A** : $cd(P) = c.\gamma$, $cd(S) = c.\chi$

Nous posons $S_j := \mathbf{Sres}_j(P,p, S,s)/c$ pour $j < n$.

entrées : les polynômes P et S

sortie : la suite des S_j définis ci-dessus ($0 \leq j \leq n-1$)

initialisation :

	1er cas : d(S) + 1 < d(P)	(c.-à-d. $p > s+1$)	
–	$S_s := \chi^{n-s} . c^{n-s-1} . S$		(1)
–	$S_{s-1} := (-1)^{n-s} . \mathbf{Prst}(P,S) / c$		(2)
–	$j := s-1$		
–	si $s < p-2$ et $s < k < p-1$:	$S_k := 0$	(3)
	2ème cas : d(S) + 1 = d(P)	(c.-à-d. $p = s+1$)	
–	$S_s := S$		
–	$S_{s-1} := \mathbf{Prst}(P,S) / c$		(1)
–	$t := d(S_{s-1})$		
– si $t = s-1$	$S_{s-2} := \mathbf{Prst}(S, S_{s-1}) / (c.\chi^2)$		(2)
– si $t < s-1$	on calcule S_t et S_{t-1} comme suit		
	$S_t := cd(S_{s-1})^{s-1-t} . S_{s-1} / \chi^{s-1-t}$		(1 bis)

$S_{t-1} := (-1)^{p-t}.\ \mathbf{Prst}\ (S, S_{s-1}) / (c.\chi^{p-t})$ (2 bis)

en outre si $t < s-2$ et $t < k < s-1$: $S_k := 0$ (3)

– $j := t-1$

étape suivante et **fin** : comme dans l'algorithme n°1

Comparaison des différents algorithmes proposés

Les algorithmes n°2 et 4 sont ceux qu'on utilisera en pratique pour calculer les sous-résultants. En effet les sous-résultants généraux sont des multiples des sous-résultants standards: ils occupent en général plus de place et occasionnent des calculs plus longs. Notons cependant que l'algorithme n°3 avec $p = d(P) > s = d(S)$ peut remplacer le n°2 (il effectue exactement les mêmes calculs) et est plus facile à écrire. L'algorithme n°5 est une amélioration de l'algorithme n°2 , pour les deux raisons suivantes : primo, si le facteur c qu'on connait dans cd(P) et cd(S) est "grand" (du point de vue de la taille occupée), les calculs seront a priori plus rapides avec les coefficients divisés par ce facteur commun; secundo, si le facteur c s'annule par spécialisation, la suite calculée par l'algorithme n°5 peut s'avérer utile tandis que celle calculée par l'algorithme n°2 serait inutilisable (cf. la proposition 9)

L'algorithme n°1 est une sorte d'algorithme intermédiaire qui permet de démontrer facilement les algorithmes n°2 et 4 à partir du théorème de Habicht .

L'algorithme n°3 est sans doute celui qui éclaire le mieux la question des sous-résultants : les polynômes P et S font partie ici de la suite des sous-résultants de manière tout à fait naturelle, et l'étape d'initialisation est réduite au strict minimum. Il n'est donc pas étonnant de voir dans la suite certaines démonstrations (celle du théorème 1 § II.1.a par exemple) reposer sur la correction de cet algorithme n°3 .

Complexité

Une suite de sous-résultants est beaucoup plus facile à calculer que la suite des restes, notamment pour les raisons suivantes:

– le calcul des sous-résultants n'utilise que des additions, multiplications et divisions exactes dans l'anneau **A** , et les coefficients obtenus restent de taille polynomiale si les déterminants sont de taille polynomiale dans **A** (par exemple avec $\mathbf{A} = \mathbb{Z}$ ou $\mathbf{A} = \mathbb{Z}[X_1, \ldots, X_n]$),

– les sous-résultants se spécialisent bien: si les divisions exactes dans **A'** ne sont pas aisées, on peut utiliser l'algorithme des sous-résultants avant spécialisation

– si on essaye de calculer la suite des restes directement dans le corps des fractions de **A** , on est confronté à l'alternative suivante: ou bien ne pas simplifier les fractions obtenues au fur et à mesure, mais alors la taille des coefficients explose presque à tout coup, ou bien simplifier les fractions obtenues, mais cela exige un calcul de pgcd dans **A** (en général nettement plus coûteux qu'une division exacte dans **A**), et on n'est même pas prémuni contre une possible explosion de la taille des fractions réduites (cf. [Lom]).

Si on désire vraiment avoir les restes sans facteur multiplicatif, le mieux sera en général de calculer la suite des sous-résultants puis de retrouver les restes en utilisant la proposition 8 .

Supposons qu'on a une notion de taille pour les éléments de **A** , et que les déterminants de matrices formées d'éléments de **A** sont de taille polynomiale en m , qui est un majorant de la dimension de la matrice et des tailles des coefficients de **A** . C'est le cas pour les

$\mathbf{A} = \mathbb{Z}$ ou $\mathbf{A} = \mathbb{Z}[X_1, ..., X_k]$ d'après l'inégalité d'Hadamard ([Mig]). Supposons enfin que ces déterminants se calculent en temps polynomial en m : c'est le cas pour les anneaux $\mathbf{A} = \mathbb{Z}$ ou $\mathbf{A} = \mathbb{Z}[X_1, ..., X_k]$ d'après la complexité des opérations arithmétiques dans ces anneaux et la méthode du pivot améliorée à la Bareiss[10] ([Bar] ou [Loo] ou [Ait]). Alors il est clair d'après la définition des polynômes sous-résultants comme déterminants polynomiaux que ceux-ci sont calculables en temps polynomial .

Si n est une borne sur les degrés de P et S le nombre d'opérations arithmétiques sur $\mathbf{A} = \mathbb{Z}$ ou $\mathbf{A} = \mathbb{Z}[X_1, ..., X_k]$ pour calculer les polynômes sous-résultants comme déterminants polynomiaux est alors en $O(n^5)$ (n polynômes sous-résultants, avec pour chacun d'entre eux n calculs de déterminants (leurs coefficients), chaque calcul de déterminant étant en n^3 opérations arithmétiques sur $\mathbf{A}$ par la méthode de Bareiss).

Il est toutefois plus efficace de les calculer en utilisant un des algorithmes précédents, car le nombre d'opérations arithmétiques sur $\mathbf{A}$ est alors en $O(n^2)$, les tailles des éléments de $\mathbf{A}$ à considérer étant de même nature dans les deux calculs[11]. Par exemple si $\mathbf{A} = \mathbb{Z}$ et si $t = \sup(\log(\Sigma a_i^2) , \log(\Sigma b_j^2))$, la complexité totale du calcul est en $O(n^4 t^2)$.

Le seul calcul du résultant par la méthode de Bareiss appliquée à la matrice de Sylvester est plus coûteux que le calcul de toute la suite des sous-résultants faite en utilisant un des algorithmes précédents.

Si on le souhaite, les polynômes sous-résultants peuvent être calculés en utilisant des méthodes modulaires puisque leurs coefficients sont des déterminants.

Remarquons enfin qu'on utilise le fait que les coefficients des polynômes sous-résultants sont des déterminants pour les majorer en taille, mais qu'on les calcule par une autre méthode. Ce phénomène est fréquent en calcul formel.

---

[10] En fait l'algorithme de Bareiss remonte au moins à [Ait] de 1932. La méthode du pivot améliorée à la Bareiss est basée sur l'étude des valeurs des coefficients successifs obtenus lors d'une triangulation par la méthode du pivot: tout coefficient obtenu est le quotient de 2 déterminants extraits de la matrice de départ. Dans [Gan] tome 1 chap. 2, Gantmacher, met clairement en évidence comment l'analyse détaillée de la méthode du pivot permet une démonstration simple des identités de Sylvester concernant les déterminants, identités qui garantissent la possibilité d'opérer les divisions exactes dans $\mathbf{A}$ qui interviennent dans la méthode de Bareiss. Notons qu'en 1932 , Aitken ([Ait]) signale "en passant" comment obtenir une triangulation entièrement dans $\mathbb{Z}$ en utilisant des divisions exactes (produit en croix divisé par le pivot précédent) ... c.-à-d. par la méthode de Bareiss .

[11] En fait, si on réordonne convenablement les lignes de la matrice de Sylvester, le calcul de son déterminant par la méthode de Bareiss fournit, en cours de route, tous les coefficients de tous les polynômes sous-résultants (cf. [Lom]) . C'est néanmoins en $O(n^3)$ opérations élémentaires (additions, multiplications, divisions exactes dans $\mathbf{A}$) , donc plus coûteux

La numérotation des théorèmes et propositions est indépendante dans les parties (I) et (II).

II.1.) Suite de Sturm-Habicht et spécialisation

a) Suite de Habicht

Le nombre de changements de signes dans la suite des restes signés permet, comme nous l'avons vu dans les théorèmes de Sturm et de Sylvester, de calculer le nombre de racines dans $\mathbb{R}$ d'un polynôme P (éventuellement "rendant le polynôme Q > 0 "), sur un intervalle] a , b [. Il s'avère en fait que la suite des sous-résultants (modifiée par des changements de signe convenables) fait aussi bien l'affaire que la suite des restes et permet d'obtenir les mêmes résultats. Ceci peut se déduire de résultats de Habicht (cf. [Gon]) . Nous en donnons ici une preuve directe.

Nous considérons dans ce paragraphe une version formelle de la suite des restes signés, que nous appelons *la suite de Habicht* . Nous démontrons que les différences de changements de signes dans la suite des restes signés et dans la suite de Habicht coïncident.

Définition:

Soit P un polynôme de degré p et S un polynôme de degré s , v := sup(p,s+1) .

La suite de Habicht est la suite formée des

$$\mathbf{Ha}_j(P,S) := (-1)^{\frac{k(k-1)}{2}}\ \mathbf{Sres}_j(P,v,S,s) \quad (j+k = v) \quad \text{pour } j \text{ variant de } 0 \text{ à } v .$$

On prend donc la suite des sous-résultants de P (considéré comme de degré v) et S qu'on modifie en multipliant les deux premiers polynômes par +1 , les deux suivants par -1 , etc.... , *de manière automatique* (sans tenir compte du fait que les polynômes sous-résultants sont éventuellement défectueux ou nuls).

Les polynômes de la suite de Habicht sont donc des multiples des polynômes de la suite $[\ \mathbf{Rss}^k(P,S)\ ]_{k=0,1,...}$ des restes signés, avec des dédoublements et des changements de signes, ou sont nuls. Plus précisément, en appliquant le théorème 3 de I.2 , et vues les conventions concernant les $\mathbf{Rss}_j(P,S)$ et les $\mathbf{Ha}_j(P,S)$ pour $j \geq \inf(d(P),d(S))$, on voit que :

> Pour tout $j \leq \sup(d(P),d(S)+1)$ les polynômes $\mathbf{Ha}_j(P,S)$ et $\mathbf{Rss}_j(P,S)$ sont égaux, à un facteur non nul près

Supposons que $\mathbf{K}$ est muni d'un ordre $\leq$ et soit $\mathbf{R}$ sa clôture réelle pour cet ordre.

On définit $\mathbf{V_{Ha}}(P,S;\ a) = V([\ \mathbf{Ha}_j(P,S)\ ]_{j=v,v-1,...,0}\ ;\ a)$

$\mathbf{V_{Ha}}(P,S;\ a,b) = V([\ \mathbf{Ha}_j(P,S)\ ]_{j=v,v-1,...,0}\ ;\ a,b\ )$

En fait, nous avons besoin d'introduire une convention particulière pour le décompte du nombre de changements de signes en a dans le cas de la suite de Habicht lorsqu'un polynôme sous-résultant défectueux s'annule en a . D'où les 2 définitions qui suivent :

Définition :

Soient $\mathbf{K}$ un corps ordonné, $a \in \mathbf{K} \cup \{+\infty\} \cup \{-\infty\}$, $[f_0,f_1,...,f_n]$ une liste de polynômes de $\mathbf{K}[X]$. On note $V'(f_0,f_1,...,f_n ; a)$ le nombre entier défini comme suit :

- on extrait tout d'abord la suite $[g_0,g_1,...,g_m] = [f_{j0},f_{j1},...,f_{jm}]$ formée des polynômes non identiquement nuls
- on compte ensuite le nombre de changements de signes dans la suite $[g_0(a),g_1(a),...,g_m(a)]$ *en adoptant les conventions suivantes concernant les 0 :*
  - * comptent pour 1 changement de signe les segments suivants
    $-,0,+$ ou $+,0,-$ ou $+,0,0,-$ ou $-,0,0,+$
  - * comptent pour 2 changements de signe les segments suivants
    $+,0,0,+$ ou $-,0,0,-$

Le nombre $V'(f_0,f_1,...,f_n ; a)$ reste donc non défini pour des suites comportant des segments avec des 0 non couverts par la convention ci-dessus. Il est cependant clair qu'il est défini lorsque $f_0,f_1,...,f_n$ est une suite de restes signés (un 0 est toujours isolé et entouré de 2 signes opposés) ou une suite de Habicht (les 0 isolés sont entourés de 2 signes opposés, et il n'y a pas de 0 triples)

Définition :

Soient $\mathbf{K}$ un corps ordonné, P et S des polynômes de $\mathbf{K}[X]$,
a et $b \in \mathbf{K} \cup \{+\infty\} \cup \{-\infty\}$, non racines du pgcd de P et S, on définit

$$\mathbf{V'_{Ha}}(P,S;a) := V'([\,\mathbf{Ha}_j(P,S)\,]_{j=v,v-1,...,0} ; a)$$
$$\mathbf{V'_{Ha}}(P,S;a,b) := \mathbf{V'_{Ha}}(P,S;a) - \mathbf{V'_{Ha}}(P,S;b)$$

NB: On a $\mathbf{V'_{Ha}}(P,S) := \mathbf{V_{Ha}}(P,S)$, plus généralement $\mathbf{V'_{Ha}}(P,S;a,b)$ ne diffère de $\mathbf{V_{Ha}}(P,S;a,b)$ que dans le cas où un polynôme sous-résultant défectueux s'annule en a ou en b.

Théorème 1 ([Hab])

En tous points a et b de $\mathbf{R}$ non racines du pgcd de P et S on a l'égalité :

$$\mathbf{V'_{Ha}}(P,S;a,b) = \mathbf{V_{Rss}}(P,S;a,b).$$

démonstration :

Le théorème 1 est une conséquence immédiate du lemme suivant :

Lemme 1 : Sous les hypothèses du théorème il existe une constante c qui dépend seulement de P et S telle que:

$$\mathbf{V'_{Ha}}(P,S;a) = \mathbf{V_{Rss}}(P,S;a) + c \quad .$$

La preuve du lemme 1 utilise le lemme 2 suivant :

Lemme 2 :

Si $v \geq j = d(\mathbf{Rss}_j(P,S)) > 0$, alors

$$\frac{\mathbf{Ha}_{j-1}(P,S)}{\mathbf{Rss}_{j-1}(P,S)} \cdot \frac{\mathbf{Ha}_j(P,S)}{\mathbf{Rss}_j(P,S)} \quad \text{est un carré dans } \mathbf{K}.$$

Notations: $t = \sup(d(P)\ ,\ d(S)+1)$, $q = d(S)$, $T_j = \mathbf{Sres}_j(P,t,\ S,q)$, $R_j = \mathbf{Rst}_j(P,S)$, $\mathbf{Rss}_j = \mathbf{Rss}_j(P,S)$, $\mathbf{Ha}_j = \mathbf{Ha}_j(P,S)$, $T_j / R_j = r_j$.

Montrons tout d'abord que le lemme 1 résulte du lemme 2.

Si $j = t$ ou est le degré d'un reste $\mathbf{Rss}^m$, alors $\mathbf{Rss}_j$ et $\mathbf{Rss}_{j-1}$ sont deux polynômes successifs dans la suite des restes signés (les $\mathbf{Rss}^m$). Par ailleurs, tout polynôme non identiquement nul dans la suite de Habicht est de la forme $\mathbf{Ha}_j$ ou $\mathbf{Ha}_{j-1}$ avec j comme ci-avant. D'après le lemme 2, en un point a où tous les $\mathbf{Rss}_j(P,S)(a)$ sont non nuls, il y a changement de signe entre $\mathbf{Rss}_j$ et $\mathbf{Rss}_{j-1}$ si et seulement si il y a changement de signe entre $\mathbf{Ha}_j$ et $\mathbf{Ha}_{j-1}$. Dans la suite de Habicht, s'ajoutent d'éventuels changements de signes entre $\mathbf{Ha}_{j-1}$ et $\mathbf{Ha}_h$ si $h = d(\mathbf{Ha}_{j-1}) < j-1$: mais les deux polynômes étant proportionnels, ce changement de signe "supplémentaire" éventuel a lieu indépendamment du point a où sont évalués les polynômes.

Voyons maintenant le cas où l'un des polynômes, non défectueux dans la suite de Habicht, s'annule en a : par exemple $d(\mathbf{Ha}_j) = j$, $d(\mathbf{Ha}_{j-1}) = j-1$, et $\mathbf{Ha}_{j-1}(a) = 0$. On sait alors que $\mathbf{Rss}_j(a).\mathbf{Rss}_{j-2}(a) < 0$, ce qui compte pour un changement de signe dans la suite des restes signés.

En outre, pour a' suffisamment proche de a et distinct de a , on a $\mathbf{V}_{\mathbf{Rss}}(P,S,a) = \mathbf{V}_{\mathbf{Rss}}(P,S,a')$ et tous les $\mathbf{Rss}^j(P,S)(a')$ sont non nuls .

En appliquant deux fois le lemme 2 on voit que $\dfrac{\mathbf{Ha}_{j-2}}{\mathbf{Rss}_{j-2}} \cdot \dfrac{\mathbf{Ha}_j}{\mathbf{Rss}_j}$ est un carré dans $\mathbf{K}$, et on obtient donc également un changement de signe dans la suite de Habicht. Et pour a' suffisamment proche de a , on a $\mathbf{V}_{\mathbf{Ha}}(P,S,a) = \mathbf{V}_{\mathbf{Ha}}(P,S,a')$.

Donc $\mathbf{V}_{\mathbf{Ha}}(P,S,a) = \mathbf{V}_{\mathbf{Rss}}(P,S,a) + c$ avec la même valeur de c en a qu'en a' .

Voyons enfin le cas où l'un des polynômes défectueux dans la suite de Habicht, s'annule en a . Soit donc j avec $\mathbf{Ha}_{j+1}$ non défectueux (de degré j+1), $\mathbf{Ha}_j$ défectueux de degré $h < j$ et tel que $\mathbf{Ha}_j(a) = 0$. D'après le lemme 2

$\dfrac{\mathbf{Ha}_j}{\mathbf{Rss}_j} \cdot \dfrac{\mathbf{Ha}_{j+1}}{\mathbf{Rss}_{j+1}}$ est un carré dans $\mathbf{K}$ et

$\dfrac{\mathbf{Ha}_h}{\mathbf{Rss}_h} \cdot \dfrac{\mathbf{Ha}_{h-1}}{\mathbf{Rss}_{h-1}}$ est un carré dans $\mathbf{K}$.

Ceci signifie que les polynômes $\mathbf{Ha}_{j+1} . \mathbf{Ha}_j . \mathbf{Ha}_h . \mathbf{Ha}_{h-1}$ et $\mathbf{Rss}_{j+1} . \mathbf{Rss}_j . \mathbf{Rss}_h . \mathbf{Rss}_{h-1}$ sont de même signe en tout point a' non racine de $\mathbf{Ha}_j$. Or $\mathbf{Rss}_j = \mathbf{Rss}_h$, et $\mathbf{Rss}_{j+1}$ et $\mathbf{Rss}_{h-1}$ sont de signe opposé en a . Si on considère donc un point a' non racine de $\mathbf{Ha}_j$ et suffisamment proche de a (tel qu'il n'y ait aucune racine d'un polynôme de la suite des restes signés de P et Q entre a et a'), le polynôme $\mathbf{Ha}_{j+1} . \mathbf{Ha}_j . \mathbf{Ha}_h . \mathbf{Ha}_{h-1}$ est négatif en a' et le nombre des changements de signe dans la suite $\mathbf{Ha}_{j+1}$, $\mathbf{Ha}_j$, $\mathbf{Ha}_h$, $\mathbf{Ha}_{h-1}$ en a' vaut 2 si $\mathbf{Ha}_{j+1} . \mathbf{Ha}_{h-1} > 0$, 1 si $\mathbf{Ha}_{j+1} . \mathbf{Ha}_{h-1} < 0$.

On a donc $\mathbf{V'}_{\mathbf{Ha}}(P,S;\ a) = \mathbf{V'}_{\mathbf{Ha}}(P,S;\ a') = \mathbf{V}_{\mathbf{Rss}}(P,S;\ a')$ ❑

Voyons maintenant la preuve du lemme 2.

Lorsque $j = t$, le lemme 2 est trivial :

$$P = T_j = R_j = \mathbf{Rss}_j = \mathbf{Ha}_j \quad \text{et} \quad S = T_{j-1} = R_{j-1} = \mathbf{Rss}_{j-1} = \mathbf{Ha}_{j-1}.$$

On utilise ensuite l'algorithme généralisé des polynômes sous-résultants et on regarde comment les choses évoluent lors de "étape suivante" , lorsqu'on passe de j+1, j à h, h−1. Si on pose $c_{j+1} := \mathbf{sr}_{j+1}(P,t,S,q)$ et $c_j := \mathbf{cd}(T_j)$, on trouve:

$$\frac{r_h}{r_{h-1}} = \frac{r_j}{r_{j+1}} \cdot \left(\frac{c_{j+1}}{c_j} \right)^2 . (-1)^{j-h}$$

Comme $\mathbf{Rss}_{j+1}$, $\mathbf{Rss}_j = \mathbf{Rss}_h$ et $\mathbf{Rss}_{h-1}$ sont 3 restes successifs on a :

$$(\mathbf{Rss}_{j+1}/R_{j+1}).(\mathbf{Rss}_j/R_j).(\mathbf{Rss}_h/R_h).(\mathbf{Rss}_{h-1}/R_{h-1}) = -1$$

Enfin, on a:

$$(\mathbf{Ha}_{j+1}/T_{j+1}).(\mathbf{Ha}_j/T_j).(\mathbf{Ha}_h/T_h).(\mathbf{Ha}_{h-1}/T_{h-1}) = (-1)^{j-h+1}$$

Ce qui montre le lemme 2 en h, h–1 s'il était vrai en j+1, j . ❑

Contre-exemple:

Avec $\mathbf{V_{Ha}}$ au lieu de $\mathbf{V'_{Ha}}$ le théorème ne serait plus valable si un des deux points a ou b annule un polynôme sous-résultant défectueux. Considérons en effet les polynômes suivants:

$P = X^5 + 2X + 2$

$S = X^4 + 1$

La suite de Habicht est alors

$\mathbf{Ha}_5(P,S) = X^5 + 2X + 2$ $\quad \mathbf{Ha}_4(P,S) = X^4 + 1$ $\quad \mathbf{Ha}_3(P,S) = -X - 2$

$\mathbf{Ha}_2(P,S) = 0$ $\quad \mathbf{Ha}_1(P,S) = X + 2$ $\quad \mathbf{Ha}_0(P,S) = 17$

et choisissons $a = -2$, $b = -1$ .on a $\mathbf{V_{Ha}}(P,S; -2, -1) = 2$.

Or la suite des restes signés est:

$\mathbf{Rss}^0(P,S) = X^5 + 2X + 2$ $\quad \mathbf{Rss}^1(P,S) = X^4 + 1$

$\mathbf{Rss}^2(P,S) = -X - 2$ $\quad \mathbf{Rss}^3(P,S) = -17$

et $\mathbf{V_{Rss}}(P,S; -2, -1) = 0$.

b) Suite de Sturm-Habicht

Rappelons que nous avons défini en I.1. la suite de Sturm de P et Q à partir des restes signés de P et de R (reste de la division de P'Q par P).

Nous donnons maintenant des définitions et notations analogues . concernant cette fois-ci la suite de Habicht. Nous obtenons ainsi un analogue formel de la suite de Sturm, appelée suite de Sturm-Habicht. Nous montrerons que les variations de signes dans la suite de Sturm-Habicht donnent aussi la différence entre le nombre de racines dans **R** de P rendant Q positif et le nombre de racines dans **R** de P rendant Q négatif. Nous avons simplifié les définitions données dans [GLRR1], mais elles ne sont pas substantiellement différentes.

Définitions

Nous définissons la

suite de Sturm-Habicht de P et Q

en séparant différents cas :

Définition :

On note $p := d(P)$, $q := d(Q)$, $R := Rst(P'Q,P)$, $r := d(R)$. *La suite de Sturm-Habicht est définie pour les indices* $j = p, p-1, \ldots, 0$.

– *si* $cd(P) = 1$ (cas où P est unitaire)

$$\mathbf{StHa}_j(P,Q) := \mathbf{Ha}_j(P,R) = (-1)^{\frac{(p-j)(p-j-1)}{2}} \mathbf{Sres}_j(P,p,R,r) .$$

– *si* $cd(P) \neq 1$ (cas où P n'est pas unitaire)

– *si* $q = d(Q) \geq 1$

$$\mathbf{StHa}_p(P,Q) := \mathrm{cd}(P)^{(q+1) \bmod 2} \cdot P$$

et pour $j < p$

$$\mathbf{StHa}_j(P,Q) := (-1)^{\frac{(p-j)(p-j-1)}{2}} \mathbf{Sres}_j(P,p,P'Q,p+q-1) \,/\, \mathrm{cd}(P) =$$
$$(-1)^{\frac{(p-j)(p-j+2q-1)}{2}} \mathbf{Sres}_j(P'Q,p+q-1,P,p) \,/\, \mathrm{cd}(P)$$

–*si* $Q = 1$ on note $\mathbf{StHa}_j(P)$ pour $\mathbf{StHa}_j(P,1)$ et on définit :

$$\mathbf{StHa}_p(P) := \mathrm{cd}(P).P$$
$$\mathbf{StHa}_{p-1}(P) := \mathrm{cd}(P).P'$$

et pour $j < p-1$

$$\mathbf{StHa}_j(P) := \mathbf{Ha}_j(P,P') \,/\, \mathrm{cd}(P) = (-1)^{\frac{(p-j)(p-j-1)}{2}} \mathbf{Sres}_j(P,p,P',p-1) \,/\, \mathrm{cd}(P)$$

Remarque 1 :

Si P est unitaire, les définitions données pour le cas P non unitaire coïncident avec celles données pour le cas P unitaire. Si on appliquait la définition du cas P non unitaire $q \geq 1$ pour le cas $Q = 1$ on retrouverait la même chose sauf pour $\mathbf{StHa}_{p-1}(P)$ (P' serait divisé par cd(P) au lieu d'être multiplié par cd(P) et on risquerait de quitter l'anneau des coefficients). Lorsque P est unitaire la suite de Sturm-Habicht de P et Q est tout simplement la suite de Habicht de P et R . Les complications techniques qui se présentent dans les autres cas sont dues au fait que l'on veut

– que les coefficients des polynômes de la suite de Sturm-Habicht soient dans l'anneau des coefficients de P et Q ,

– que la suite de Sturm-Habicht se comporte bien par spécialisation, même dans certains cas où il y a chute du degré de P ou de Q ,

– que la suite de Sturm-Habicht soit calculée par un algorithme aussi performant que possible.

Définition :

On appellera **coefficient de Sturm-Habicht** et on notera $\mathbf{sth}_j(P,Q)$ le coefficient de X^j dans $\mathbf{StHa}_j(P,Q)$. On dira que $\mathbf{StHa}_j(P,Q)$ est *défectueux* s'il est de degré $< j$, c'est-à-dire si $\mathbf{sth}_j(P,Q)$ est nul.

Enfin, on appellera **suite de Sturm-Habicht du polynôme P** la suite de Sturm-Habicht de P et 1 .

Définitions et notations:

Si **K** est muni d'un ordre $\leq$ et si a et b sont deux éléments de $\mathbf{K} \cup \{+\infty\} \cup \{-\infty\}$ on note :

$$\mathbf{V}_{\mathbf{StHa}}(P,Q;a) := V([\,\mathbf{StHa}_j(P,Q)\,]_{j=p,p-1,\ldots,0}\,;\,a)$$
$$\mathbf{V}_{\mathbf{StHa}}(P,Q;a,b) := \mathbf{V}_{\mathbf{StHa}}(P,Q;a) - \mathbf{V}_{\mathbf{StHa}}(P,Q;b)$$
$$\mathbf{V}_{\mathbf{StHa}}(P,Q) := \mathbf{V}_{\mathbf{StHa}}(P,Q,-\infty) - \mathbf{V}_{\mathbf{StHa}}(P,Q,+\infty).$$

Soient **K** un corps ordonné, P et Q des polynômes de **K**[X] , de degrés p et q a et $b \in \mathbf{K} \cup \{+\infty\} \cup \{-\infty\}$, non racines du pgcd de P et Q , on définit

$$\mathbf{V'_{StHa}}(P,Q;a) := V'([\ \mathbf{StHa}_j(P,Q)\ ]_{j=p,p-1,\ldots,0}\ ;\ a\ )$$
$$\mathbf{V'_{StHa}}(P,Q;a,b) := \mathbf{V'_{StHa}}(P,Q;a) - \mathbf{V'_{StHa}}(P,Q;b).$$

Principales propriétés

Les définitions des $\mathbf{StHa}_j(P,Q)$ ci-dessus sont choisies de manière à ce que soit vérifiée la proposition suivante.

Proposition 1 : (étude du cas où P n'est pas unitaire)

a) Si $d(R) = p-1$, les polynômes $\mathbf{StHa}_j(P,Q)$ et $\mathbf{Ha}_j(P,R)$ (où $R = \mathbf{Rst}(P'Q,P)$) sont proportionnels dans un facteur de signe constant (même résultat si $p-1-d(R)$ est pair).

b) Dans tous les cas, il existe une constante c' qui ne dépend que de P et Q telle que:

$$\mathbf{V'_{Ha}}(P,R;a) = \mathbf{V'_{StHa}}(P,Q;a) + c'$$

démonstration : Si $Q = 1$ le résultat est trivial. Reste à voir avec $d(Q) = q \geq 1$. Les propositions et remarques citées dans la suite de la preuve sont dans la partie (I).

On a $\mathbf{Ha}_j(P,R) = (-1)^{\frac{(p-j)(p-j-1)}{2}}\ \mathbf{Sres}_j(P,p,R,r)$, avec en particulier $\mathbf{Ha}_p(P,R) = P$ et $\mathbf{Ha}_{p-1}(P,R) = R$.

On a $\mathbf{StHa}_j(P,Q) := (-1)^{\frac{(p-j)(p-j-1)}{2}}\ \mathbf{Sres}_j(P,p,R,p+q-1)\ /\ cd(P)$ pour $j \leq p-1$, par application de la proposition 3 .

Pour $j < p-1$ on a, d'après la proposition 1 c) (i) et la remarque 5 :

$$\mathbf{Sres}_j(P,p,R,p+q-1) = (\ (cd(P)\ )^{p+q-1-r}\ \mathbf{Sres}_j(P,p,R,r)$$

Enfin, on voit facilement que $\mathbf{Sres}_{p-1}(P,p,R,p+q-1) = (\ (cd(P)\ )^q\ R$.

Ainsi lorsque $r = p-1$, on a pour tout $j \leq p-1$ $\mathbf{StHa}_j(P,Q) = (\ (cd(P)\ )^{q-1}\ \mathbf{Ha}_j(P,R)$, d'où le résultat a) .

Lorsque $r < p-1$, on a pour tout $j < p-1$ $\mathbf{StHa}_j(P,Q) = (\ (cd(P)\ )^{p+q-2-r}\ \mathbf{Ha}_j(P,R)$ et le polynôme proportionnel à R est dédoublé dans les deux suites considérées: une fois avec l'indice $p-1$, l'autre fois avec l'indice r . Avant le dédoublement (sur le morceau P, R) les deux suites sont proportionnelles à un facteur près de signe constant : le même que celui de $cd(P)^{q-1}$. Après le dédoublement ($2^{ème}$ occurrence de R et jusqu'à la fin), les deux suites sont proportionnelles au facteur constant près : $(\ (cd(P)\ )^{p+q-2-r}$. D'où le b) .

❑

Exemple 1 :

Considérons de nouveau l'exemple du polynôme général de degré 4 ,

$$P = X^4 + pX^2 + qX + r.$$

La suite de Sturm-Habicht de P et P' , calculée dans $\mathbb{Z}[p,q,r][X]$ est

$\mathbf{StHa}_4(P) = X^4 + pX^2 + qX + r$ $\qquad$ $\mathbf{StHa}_3(P) = 4\ X^3 + 2pX + q$

$\mathbf{StHa}_2(P) = -\ 4(2pX^2 + 3qX + 4r)$

$\mathbf{StHa}_1(P) = -\ 4((2p^3 - 8pr + 9q^2)X + p^2q + 12qr)$

$\mathbf{StHa}_0(P) = 16p^4r - 4p^3q^2 - 128\ p^2r^2 + 144\ pq^2r - 27\ q^4 + 256\ r^3$

A des carrés de $\mathbb{Q}(p,q,r)$ près, elle coïncide avec la suite de Sturm générique (voir exemple 1 du § I.1).

Si $p = 0$, la suite de Sturm-Habicht de $P = X^4 + qX + r$, obtenue en substituant 0 à p dans la suite de Sturm-Habicht de P est donc:

$\mathbf{StHa}_4(P) = X^4 + qX + r$ $\quad$ $\mathbf{StHa}_3(P) = 4X^3 + q$
$\mathbf{StHa}_2(P) = -4(3qX + 4r)$ $\quad$ $\mathbf{StHa}_1(P) = -12q(3qX + 4r)$
$\mathbf{StHa}_0(P) = 27q^4 + 256r^3$

Comparer avec ce qu'on obtenait dans l'exemple 1 du § I.1 : la suite de Sturm-Habicht est formée de multiples des polynômes de la suite de Sturm, avec certains changements de signes et répétitions.

Nous donnons maintenant des résultats concernant le cas P unitaire qui nous seront utiles par la suite .

Proposition 2 :

Soient P et Q deux polynômes à coefficients dans un anneau intègre **A** , avec P unitaire.

(i) Si $\mathbf{sth}_j(P,Q) \neq 0$, $\mathbf{sth}_{j-1}(P,Q) = \ldots = \mathbf{sth}_{j-h}(P,Q) = 0$, $\mathbf{sth}_{j-h-1}(P,Q) \neq 0$ alors $\mathbf{StHa}_j(P,Q)$ est de degré j , $\mathbf{StHa}_{j-1}(P,Q)$ est défectueux de degré $j-h-1$ et tous les $\mathbf{StHa}_k(P,Q)$, $j-h \leq k < j-1$, sont nuls.

(ii) Sous la même hypothèse nous avons, en notant $c_{j-h-1} := cd(\mathbf{StHa}_{j-1})$,

$$\mathbf{sth}_j(P,Q)^h \, \mathbf{StHa}_{j-h-1} = (-1)^{h(h+1)/2} \, (c_{j-h-1})^h \, \mathbf{StHa}_{j-1} .$$

(iii) $\mathbf{StHa}_p(P,Q) = P$, $\mathbf{StHa}_{p-1}(P,Q) = R = \mathbf{Rst}(P'Q,P)$, et pour $j < p-1$, $k = p-j$:

$$\mathbf{StHa}_j(P,Q) = (-1)^{\frac{k(k-1)}{2}} \mathbf{Sres}_j(P,p,R,d(R)) = (-1)^{\frac{k(k-1)}{2}} \mathbf{Sres}_j(P,p,R,p-1)$$

En conséquence la suite de Sturm-Habicht est invariante par spécialisation.

démonstration:
Immédiat d'après le théorème 4 de I.2 et la définition de la suite de Sturm-Habicht.

La suite de Sturm-Habicht est la version formelle de la suite de Sturm. Dans le cas ordinaire, où P est unitaire et où les degrés descendent de 1 en 1 dans la suite de Sturm, les deux suites sont formées des mêmes polynômes, à des facteurs carrés près. Dans les cas défectueux la suite de Sturm de P et Q possède moins de termes que la suite de Sturm-Habicht . La suite de Sturm-Habicht est beaucoup plus facile à calculer que la suite de Sturm. Le théorème analogue au théorème 1 s'avère donc fort utile: c'est le théorème 2 suivant.

Théorème 2 ([Hab]):

Soient P et Q deux polynômes quelconques à coefficients dans un corps ordonné **K** et a et b (avec $a < b$) des points de **K** non racines de P .

(i) On a l'égalité $\mathbf{V'_{StHa}}(P,Q;a,b) = \mathbf{V_{Stu}}(P,Q;a,b)$.

(ii) On a l'égalité $\mathbf{V_{StHa}}(P,Q) = \mathbf{V_{Stu}}(P,Q)$.

démonstration:
Notons $p := d(P)$, $q := d(Q)$, $R := \mathbf{Rst}(P,P'Q)$, $r := d(R)$.
Le (ii) résulte du (i) .
Voyons le (i). D'après le théorème 1, on a le résultat suivant :

$$\boxed{\mathbf{V_{Stu}}(P,Q;a,b) = \mathbf{V'_{Ha}}(P,R;a,b).}$$

On conclut par la proposition 1 . ❑

Corollaire:

Soient P et Q deux polynômes quelconques à coefficients dans un corps ordonné **K** de

clôture réelle **R** et a et b (avec a < b) des points de **R** non racines de P.

(i) On a l'égalité $\mathbf{V'_{StHa}}(P,Q,a,b) = \mathbf{c}_+(P,Q,a,b) - \mathbf{c}_-(P,Q,a,b)$.

(ii) On a l'égalité $\mathbf{V_{StHa}}(P,Q) = \mathbf{c}_+(P,Q) - \mathbf{c}_-(P,Q)$.

démonstration:
Résulte du théorème 2, et du théorème 1 de I.1. ❑

Algorithmes

Les $\mathbf{StHa}_j(P,Q)$ peuvent être calculés au moyen des algorithmes donnés au § I.2 :
Si P est unitaire on utilisera l'algorithme généralisé des polynômes sous-résultants (algorithme 3).
Si P n'est pas unitaire on utilisera l'algorithme 5 avec, dans le cas $d(Q) \geq 1$, la deuxième formule donnée dans la définition.

c) Spécialisation de la suite de Sturm-Habicht

On considère deux polynômes P et Q à coefficients dans un anneau **A** , un homomorphisme Sp de **A** dans **A'** où **A'** est un anneau intègre de corps de fractions **K'** . On considère un ordre ≤ sur **K'** et la clôture réelle **R'** de **K'** pour cet ordre.

On note $p = d(P)$, $q = d(Q)$, $P_1 = Sp(P)$, $Q_1 = Sp(Q)$, $p_1 = d(P_1)$, $q_1 = d(Q_1)$.

1er cas : $p_1 = p$, $q \geq 1$

Proposition 3 : (Notations ci-dessus) Supposons $p_1 = p$, $q \geq 1$.

a) Si P est unitaire, on a $Sp(\mathbf{StHa}_j(P,Q)) = \mathbf{StHa}_j(P_1,Q_1)$

b) Dans tous les cas, la différence des changements de signes dans la suite obtenue par spécialisation de la suite de Sturm-Habicht de P et Q entre a et b coïncide avec la différence des changements de signes dans la suite de Sturm-Habicht de Sp(P) et Sp(Q) entre a et b (a et b sont des éléments de $\mathbf{K'} \cup \{+\infty\} \cup \{-\infty\}$). Autrement dit, on a l'égalité :

$$\mathbf{V'_{StHa}}(P_1,Q_1; a,b) = V'([\, Sp(\, \mathbf{StHa}_j(P,Q)\,)\,]_{j=p,p-1,\ldots,0} ; a,b)$$

démonstration:
Si P est unitaire ,

a) est donné par la prop 2 (iii), b) s'en déduit

Si P n'est pas unitaire

on remarque que théorème 2 se déduit de la proposition 1 et du théorème 1. Mais dans la proposition 1, la preuve utilise seulement $q \geq d(Q)$ et non pas $q = d(Q)$. ❑

2ème cas : $p_1 = p - 1$, $q_1 = q$:

On applique la proposition 9 de I.1. Les démonstrations résultent de calculs immédiats.

Proposition 4 : Nous supposons $p_1 = p - 1$, $q_1 = q \geq 1$.

On a alors pour $j < p_1$, l'égalité :

$$Sp(\mathbf{StHa}_j(P,Q)) = (-1)^q.cd(P_1)^2.cd(Q_1).\, \mathbf{StHa}_j(P_1,Q_1) \quad .$$

Proposition 5 : Nous supposons $p_1 = p - 1$.

On a alors pour $j < p_1 - 1$, l'égalité:

$$Sp(\mathbf{StHa}_j(P)) = cd(P_1)^2 .\mathbf{StHa}_j(P_1) \quad .$$

Il sera donc facile, dans les deux cas envisagés, de calculer des polynômes égaux, à un facteur constant près, à ceux de la suite de la suite de Sturm-Habicht de Sp(P) et Sp(Q). (on prendra garde seulement à l'initialisation de la suite, à calculer directement).

3ème cas : $p_1 < p - 1$, ou $p_1 = p - 1$, $q_1 < q$,

On a $Sp(\mathbf{StHa}_j(P,Q)) = 0$. Si on veut calculer la suite de Sturm-Habicht avant spécialisation, on doit faire un nouveau calcul : on considère les polynômes

P_p := "P tronqué au delà du degré d(Sp(P))",

Q_q := "Q tronqué au delà du degré d(Sp(Q))"

on a $Sp(P) = Sp(P_p)$, $Sp(Q) = Sp(Q_q)$. On calcule alors les $\mathbf{StHa}_j(P_p,Q_q)$.

II.2.) Les différentes méthodes pour calculer le nombre de racines réelles d'un polynôme (et généralisation)

On a déjà vu la méthode de Sturm et la méthode de Sturm-Habicht, qui s'en déduit si on connait la théorie des sous-résultants. Une autre méthode d'inspiration a priori très différente, due à Hermite, utilise la signature d'une forme quadratique. Nous allons expliquer cette méthode d'Hermite avant d'indiquer les relations entre les différentes méthodes, qui se comprennent bien en utilisant la suite de Sturm-Habicht. Pour les paragraphes a) et c) de cette section, nous avons utilisé abondamment l'excellent article [KrN] qui nous a été signalé par E. Becker.

Dans tout le II.2. le polynôme P sera *unitaire* .

a) Méthode d'Hermite

On considère toujours un anneau intègre **A** de corps de fraction **K** .

Soit $P = X^p + a_{p-1} X^{p-1} + ... + a_0$ un polynôme unitaire à coefficients dans **A** et $Q = b_q X^q + b_{q-1} X^{q-1} + ... + b_0$ un polynôme à coefficient dans **A** . On note $(\alpha_i)_{i=1,...,p}$ les racines de P dans une clôture algébrique **C** de **K** .

On définit une forme quadratique à p variables $x_0,x_1,...,x_{p-1}$, B(P,Q) , par :

$$B(P,Q) = \Sigma_{i=1,...,p}\ Q(\alpha_i)\ (x_0 + x_1\alpha_i + ... + x_{p-1}\ \alpha_i^{p-1})^2.$$

Il est clair que B(P,Q) est à coefficients dans **A** , puisque l'expression est symétrique en les α_i .

En désignant par $s(P,Q)_k$, pour k = 0, ..., 2p − 2 la somme $\Sigma_{i=1,...,p}\ Q(\alpha_i)\ \alpha_i^k$ on a :

$$B(P,Q) = \Sigma_{k=0,...,p-1;j=0,...,p-1}\ s(P,Q)_{k+j}\ x_k\ x_j .$$

Lorsque Q = 1 , on note B(P) la forme B(P,1) ; on a

$$B(P) = \Sigma_{i=1,...,p}\ (x_0 + x_1\alpha_i + ... + x_{p-1}\ \alpha_i^{p-1})^2.$$

Il est clair que B(P,Q) est à coefficients dans **A** , puisque l'expression est symétrique en les α_i .

En désignant par s_k la somme de Newton $\Sigma_{i=1,...,p} \alpha_i^k$ on a :

$B(P) = \Sigma_{k=0,...,p-1;j=0,...,p-1} s_{k+j} x_k x_j$.

Si $\leq$ est un ordre sur $\mathbf{K}$ on note $\mathbf{R}$ la clôture réelle de $\mathbf{K}$ pour l'ordre $\leq$. Rappelons qu'on note $c_+(P,Q)$ le nombre de racines de P dans $\mathbf{R}$ avec $Q > 0$, $c_-(P,Q)$ le nombre de racines de P dans $\mathbf{R}$ avec $Q < 0$, $c(P)$ le nombre de racines de P dans $\mathbf{R}$. La forme quadratique B(P,Q) a une signature dans le corps $\mathbf{R}$ (cette signature dépend du choix de l'ordre $\leq$ sur $\mathbf{K}$). On prend alors pour corps $\mathbf{C}$ le corps $\mathbf{R}[i]$ (avec $i^2 = -1$) . On appelera *racines réelles* celles qui sont dans $\mathbf{R}$ et *racines complexes* celles qui sont dans $\mathbf{C} - \mathbf{R}$.

Théorème 3 (méthode d'Hermite [Her]) :

Avec les notations ci-dessus

(i) le rang de B(P,Q) est égal au nombre de racines distinctes de P non racines de Q dans $\mathbf{C}$.

(ii) la signature de B(P,Q) est égale à $c_+(P,Q) - c_-(P,Q)$.

démonstration : La démonstration est élémentaire (voir [Gan] ou [KrN] ou [GLRR2]). ❑

Corollaire: Avec les notations précédentes, la signature de B(P) est égale à $c(P)$.

b) Bezoutiens et coefficients sous-résultants

Définition (et notation)

On appelle **bezoutiens** et on note $b(P,Q)_k$ les mineurs principaux[1] de la matrice symétrique $A = (s(P,Q)_{i+j-2})_{i=1,...,p;j=1,...,p}$ associée à la forme quadratique B(P,Q) .

Considérons le développement en 1/X de la fonction rationnelle P'Q/P . Si $P = \Pi_{i=1,...,p}(X-\alpha_i)$ on a $P'/P = \Sigma_{i=1,...,p} 1/(X-\alpha_i)$, et en posant $Q = Q(\alpha_i) + (X-\alpha_i)A_i$ $P'Q/P = \Sigma_{i=1,...,p} A_i + \Sigma_{i=1,...,p} Q(\alpha_i)/(X-\alpha_i)$. On en déduit que le coefficient de $1/X^k$ dans le développement de P'Q/P en 1/X est , avec les notations précédentes $s(P,Q)_{k-1}$.

Par ailleurs, si R est le reste de la division de P'Q par P , R/P est la partie fractionnaire de la fraction rationnelle P'Q/P de sorte que $s(P,Q)_{k-1}$ est le coefficient de $1/X^k$ dans le développement en 1/X de R/P .

On a donc : (*) $R/P = \Sigma_{i=1,...,p} Q(\alpha_i)/(X-\alpha_i)$.

Tout ceci permet d'établir par identification du membre gauche et du membre droit de (*) des relations entre les $s(P,Q)_k$, les coefficients de $P = X^p + a_{p-1} X^{p-1} + ... + a_0$ et ceux de $R = c_{p-1} X^{p-1} + ... + c_0$ (c_{p-1} éventuellement nul), à savoir :

$s(P,Q)_0 = c_{p-1}$

$s(P,Q)_1 + a_{p-1}\ s(P,Q)_0 = c_{p-2}$

...

$s(P,Q)_{p-1} + ... + a_1\ s(P,Q)_0 = c_0$

$s(P,Q)_{n-1} + ... + a_1\ s(P,Q)_{n-p} = 0$ pour $n > p$.

On désignera les relations précédentes par (**) dans la suite .

---

[1] définition donnée au début du §c qui suit

Proposition 6 :

Soient P et Q deux polynômes avec :

$$P = X^p + a_{p-1} X^{p-1} + ... + a_0 \qquad Q = b_q X^q + b_{q-1} X^{q-1} + ... + b_0$$

En notant $\mathbf{sth}_j(P,Q))$ le coefficient en degré j de $\mathbf{StHa}_j(P,Q)$ on a pour tout k=1,...,p :

$$\mathbf{sth}_{p-k}(P,Q)) = b(P,Q)_k$$

démonstration:

Notons $R = c_{p-1} X^{p-1} + ... + c_0$ le reste de la division euclidienne de P par P'Q .D'après la définition de la suite de Sturm-Habicht et la proposition 2 (iii) :

$$\mathbf{sth}_{p-k}(P,Q)) = (-1)^{k(k-1)/2} \mathbf{sr}_{p-k}(P,p,R,p-1).$$

Rappelons la définition de $\mathbf{sr}_{p-k}(P,p,R,p-1)$, noté $\mathbf{sr}_{p-k}$.

$$sr_{p-k} = \begin{vmatrix} 1 & a_{p-1} & \cdots & a_{p-2k+2} \\ 0 & 1 & a_{p-1} & \cdots & a_{p-2k+3} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & 0 & 1 & a_{p-1} & \cdots & a_{p-k} \\ c_{p-1} & c_{p-2} & \cdots & c_{p-2k+1} \\ 0 & c_{p-1} & c_{p-2} & \cdots & c_{p-2k+2} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & 0 & c_{p-1} & \cdots & c_{p-1-k} \end{vmatrix}$$

Les équations de (**) permettent d'écrire, en notant $s'_k := s(P,Q)_k$:

$$\mathbf{sr}_{p-k} = \begin{vmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\ s'_0 & s'_1 & \cdots & s'_{k-1} & \cdots & s'_{2k-2} \\ 0 & s'_0 & s'_1 & \cdots & s'_{2k-3} \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & s'_0 & s'_1 & \cdots & s'_{k-1} \end{vmatrix} \begin{vmatrix} 1 & a_{p-1} & \cdots & a_{p-2k+2} \\ 0 & 1 & a_{p-1} & \cdots & a_{p-2k-2} \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & 0 & 1 & a_{p-1} & \cdots & a_{p-k} \\ 0 & \cdots & 0 & 1 & \cdots & a_{p-k+1} \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & 0 & 1 \end{vmatrix}$$

d'où $\mathbf{sr}_{p-k} = \begin{vmatrix} s'_{k-1} & \cdots & s'_{2k-2} \\ \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots \\ s'_0 & s'_1 & \cdots & s'_{k-1} \end{vmatrix}$

et enfin, en tenant compte de la permutation des lignes,

$$\mathbf{sr}_{p-k} = (-1)^{k(k-1)/2} b(P,Q)_k \ .$$ ❑

c) Mineurs principaux et signature d'une forme quadratique

On appelle **mineurs principaux d'une matrice** $A = (a_{i,j})_{i=1,...,p,j=1,...,p}$ les déterminants $\det(A_k)$ des matrices $A_k = (a_{i,j})_{i=1,...,k,j=1,...,k}$ pour $k = 1,...,p$.

Si A est une matrice symétrique à coefficients dans un corps ordonné on a le résultat suivant dû à Jacobi .

Proposition 7 (théorème de Jacobi):

Avec les notations précédentes, si les $\det(A_k)$ sont tous non nuls, la signature de la forme quadratique associée à une matrice symétrique A est égale à la différence entre le nombre d'éléments positifs et le nombre d'éléments négatifs dans la suite $(1, (\det(A_k))_{k=1,...,p})$.

Si des mineurs principaux de la matrice s'annnulent il n'est plus vrai en général que les mineurs principaux de la matrice symétrique déterminent la signature de la forme quadratique (pour tout ceci voir [Gan] tome I chap. 10).

Il est possible de généraliser le théorème de Jacobi et d'obtenir la signature grâce aux seuls signes des mineurs principaux dans le cas particulier des formes de Hankel. Les **formes de Hankel** sont les formes quadratiques du type $B = \Sigma_{k=0,...,p-1;l=0,...,p-1} c_{k+l} x_k x_l$. La matrice symétrique $A = [a_{i,j}]_{i=1,...,p;j=1,...,p}$ qui est associée à B est définie par $a_{i,j} = c_{i+j-2}$.

Faisons tout d'abord une remarque: considérons une suite $(a_0,...,a_n)$ d'éléments tous non nuls de **K** . Rappelons qu'on note $V(a_0,...,a_n)$ le nombre de changements de signes dans $(a_0,...,a_n)$. On définit maintenant le **nombre de permanences de signes** $\Pi(a_0,...,a_n)$ dans $(a_0,...,a_n)$ par récurrence sur n :

$\Pi(a_0) = 0$,

$\Pi(a_0,...,a_{n+1}) = \Pi(a_0,...,a_n) + 1$ si a_{n+1} a le même signe que le dernier élément non nul de $(a_0,...,a_n)$

$\Pi(a_0,...,a_{n+1}) = \Pi((a_0,...,a_n)$ sinon.

On a alors la relation suivante.

Remarque 2 : Si les éléments de $(a_0,...,a_n)$ sont tous non nuls, alors on a

$\Pi(a_0,...,a_n) = V((-1)^n a_0 , (-1)^{n-1} a_1 , ... , - a_{n-1} , a_n)$.

La différence $C(a_0,...,a_n)$ entre le nombre d'éléments positifs et le nombre d'éléments négatifs dans la suite $(a_0,...,a_n)$ est égale à $\Pi(a_0,...,a_n) - V(a_0,...,a_n)$ si $a_0 > 0$.
On peut donc réénoncer ainsi le théorème de Jacobi :

> Avec les notations précédentes, si les $\det(A_k)$ sont tous non nuls, la signature de la forme quadratique associée à une matrice symétrique A est égale à $C(1 , (\det(A_k))_{k=1,...,p})$.

La proposition suivante indique comment se généralise le théorème de Jacobi. On doit tout d'abord généraliser la définition du nombre $C(a_0,...,a_n)$ au cas d'une suite comportant des zéros.

Définition : On définit la quantité $C(a_0,...,a_n)$ où $(a_0,...,a_n)$ est une suite d'éléments de $\mathbf{K}$ et $a_0 \neq 0$ de la manière suivante:

- faisons apparaître les éléments nuls de $(a_0,...,a_n)$

  $(a_0,...,a_n) = (a_0,..., a_{i(1)},0,....,0,a_{i(1)+k(1)+1}, ..., a_{i(2)},0,...,0,a_{i(2)+k(2)+1}, ...,$

  $a_{i(t-1)+k(t-1)},0,...,0,a_{i(t-1)+k(t-1)+1}, ...,a_{i(t)}, 0,...,0)$

  (tous les éléments a_j , tels que $i(h-1) + k(h-1) < j \leq i(h)$, $h = 1,...,t$ sont non nuls)
- définissons $C(a_0,...,a_n) := \Sigma_{h=1,...,t}\, C(a_{i(t-1)+k(t-1)+1},...,a_{i(t)}) + \Sigma_{h=1,...,t}\, \varepsilon_h$

  avec $\varepsilon_h = 0$ si $k(h)$ est impair

  $(-1)^{k(h)/2}$ signe$(a_{i(h)+k(h)+1} \cdot a_{i(h)})$ si $k(h)$ est pair .

Proposition 8 : Avec les notations précédentes, la signature d'une forme de Hankel dont la matrice symétrique associée est A , est égale à $C(1, (\det(A_k))_{k=1,...,p})$.

démonstration:
due à Frobenius [Fro] . Il semble difficile d'exposer ceci plus clairement que [Gan], tome 1, chapitre 10 . ❑

Les résultats précédents nous permettent d'énoncer la proposition suivante:

Proposition 9 :

La signature $\mathbf{S_B}(P,Q)$ de $B(P,Q)$ est égale à la quantité $C(1, (b(P,Q)_k)_{k=1,...,p})$.

démonstration:
On utilise la proposition 8 et le fait que la matrice associée à $B(P,Q)$ est une matrice de Hankel. ❑

Remarque 3 :
A cause de la relation entre bezoutiens et coefficients sous-résultants, il est clair que si le rang de la forme quadratique $B(P,Q)$ est r , alors le bezoutien $b(P,Q)_r$ est non nul (utiliser le corollaire du théorème 3 de I.2). Ceci permet d'obtenir plus facilement la proposition 8 dans le cas particulier de $B(P,Q)$ (on n'a pas besoin du théorème 23 page 344 de [Gan]).

Théorème 4 (méthode des bezoutiens [Her], [Syl]):

La quantité $C(1, (b(P,Q)_k)_{k=1,...,p})$ est égale à $\mathbf{c_+}(P,Q) - \mathbf{c_-}(P,Q)$.

démonstration:
On applique le théorème 3 et la proposition 9 . ❑

Remarque 4 :

1) Les calculs des $(b(P,Q)_k)_{k=1,...,p}$ se font dans l'anneau $\mathbf{A}$. La quantité $C(1, (b(P,Q)_k)_{k=1,...,p})$ dépend évidemment du choix de l'ordre sur $\mathbf{K}$.
2) Considérons maintenant un homomorphisme d'anneau Sp de $\mathbf{A}$ dans $\mathbf{A'}$.
   Les $b(Sp(P),Sp(Q))_k$ sont les spécialisés des $b(P,Q)_k$
   Il faut recalculer $C(1, (b(Sp(P),Sp(Q))_k)_{k=1,...,p})$ en évaluant les signes des $b(Sp(P),Sp(Q))_k$ et en utilisant la définition de C .
   Notons que dans toute la théorie de Hermite et des bezoutiens il est essentiel que le degré de P soit fixé.

d) De la méthode de Sturm-Habicht à la méthode d'Hermite

Nous allons maintenant indiquer comment calculer $\mathbf{V_{StHa}}(P,Q)$ à partir des coefficients $\mathbf{sth}_k(P,Q)_{\,k=1,\ldots,p}$, en l'absence des polynômes $\mathbf{StHa}_k(P,Q)$, ce qui finira d'expliciter le rapport entre la méthode de Sturm et la méthode d'Hermite.

Proposition 10 :

$\mathbf{V_{StHa}}(P,Q)$ est égal à $C(\ (\mathbf{sth}_{p-k}(P,Q)\ )_{k=0,\ldots,p}\ )$.

Ce résultat reste valable même si P n'est pas unitaire

démonstration:

voyons le cas où P est unitaire

Il est clair que si tous les $\mathbf{sth}_{p-k}(P,Q)$ sont non nuls on a :

$$\begin{aligned} V_{\mathbf{StHa}}(P,Q;\ +\infty) &= V(\ \mathbf{sth}_{p-k}(P,Q)_{\,k=0,\ldots,p}\ ) \\ V_{\mathbf{StHa}}(P,Q;\ -\infty) &= V(\ (-1)^{p-k}\ \mathbf{sth}_{p-k}(P,Q)_{\,k=0,\ldots,p}\ ) \\ &= \Pi(\ \mathbf{sth}_{p-k}(P,Q)_{\,k=0,\ldots,p}\ ) \quad \text{en utilisant la remarque 2,} \end{aligned}$$

d'où : $\mathbf{V_{StHa}}(P,Q) = \mathbf{V_{StHa}}(P,Q;\ -\infty) - \mathbf{V_{StHa}}(P,Q;\ +\infty) = C(\ \mathbf{sth}_{p-k}(P,Q)_{\,k=0,\ldots,p}\ )$.

d'où : $\mathbf{V_{StHa}}(P,Q) = \mathbf{V_{StHa}}(P,Q;\ -\infty) - \mathbf{V_{StHa}}(P,Q;\ +\infty) = C(\ \mathbf{sth}_{p-k}(P,Q)_{\,k=0,\ldots,p}\ )$.

Le cas non trivial est celui d'un polynôme défectueux dans la suite de Sturm-Habicht car alors il y a un zéro de plus dans la suite des $\mathbf{sth}_{p-k}(P,Q)$ $(k=0,\ldots,p)$ que dans la suite de Sturm-Habicht.

Rappelons (proposition 2) que si

$$\mathbf{sth}_j(P,Q) \neq 0,\quad \mathbf{sth}_{j-1}(P,Q) = \ldots = \mathbf{sth}_{j-h}(P,Q) = 0\ ,\quad \mathbf{sth}_{j-h-1}(P,Q) \neq 0$$

alors $\mathbf{StHa}_j(P,Q)$ est de degré j , $\mathbf{StHa}_{j-1}(P,Q)$ est défectueux de degré j-h-1 et tous les $\mathbf{StHa}_k(P,Q)$, $j-h \leq k < j-1$, sont nuls.

Nous allons montrer, en notant $\mathbf{StHa}_j(P,Q)$, $\mathbf{StHa}_{j-1}(P,Q)$ et $\mathbf{StHa}_{j-h-1}(P,Q)$ respectivement $\mathbf{StHa}_j$, $\mathbf{StHa}_{j-1}$ et $\mathbf{StHa}_{j-h-1}$ que

$V(\ (\mathbf{StHa}_j,\mathbf{StHa}_{j-1},\mathbf{StHa}_{j-h-1})\ ;\ -\infty\ ) - V(\ (\mathbf{StHa}_j,\mathbf{StHa}_{j-1},\mathbf{StHa}_{j-h-1})\ ;\ +\infty\ ) = \varepsilon_h$

avec $\varepsilon_h = 0$ si h est impair,

$\varepsilon_h = (-1)^{h/2}$ signe$(\ \mathbf{sth}_j(P,Q)\ \mathbf{sth}_{j-h-1}(P,Q)\ )$ sinon .

D'après la proposition 2 nous avons, en notant c_{j-h-1} le coefficient dominant de $\mathbf{StHa}_{j-1}$,

$$\mathbf{sth}_j(P,Q)^h\ \mathbf{StHa}_{j-h-1} = (-1)^{h(h+1)/2}\ (c_{j-h-1}\ )^h\ \mathbf{StHa}_{j-1},$$

d'où $$\mathbf{sth}_j(P,Q)^h\ \mathbf{sth}_{j-h-1}(P,Q) = (-1)^{h(h+1)/2}\ (c_{j-h-1}\ )^{h+1}\quad (***)\ .$$

Il est maintenant facile de voir avec (***) que

- si h est impair et $(-1)^{(h+1)/2} = 1$ alors

$V(\ \mathbf{StHa}_j,\ \mathbf{StHa}_{j-1},\ \mathbf{StHa}_{j-h-1}\ ;\ -\infty) - V(\ \mathbf{StHa}_j,\ \mathbf{StHa}_{j-1},\ \mathbf{StHa}_{j-h-1}\ ;\ +\infty) = 0$

- si h est impair et $(-1)^{(h+1)/2} = -1$ alors

$V(\ \mathbf{StHa}_j,\ \mathbf{StHa}_{j-1},\ \mathbf{StHa}_{j-h-1}\ ;\ -\infty) - V(\ \mathbf{StHa}_j,\ \mathbf{StHa}_{j-1},\ \mathbf{StHa}_{j-h-1}\ ;\ +\infty) = 0$

- si h est pair et $(-1)^{h/2} = 1$ alors

$V(\ \mathbf{StHa}_j,\ \mathbf{StHa}_{j-1},\ \mathbf{StHa}_{j-h-1}\ ;\ -\infty) - V(\ \mathbf{StHa}_j,\ \mathbf{StHa}_{j-1},\ \mathbf{StHa}_{j-h-1}\ ;\ +\infty) = 1$

- si h est pair et $(-1)^{h/2} = -1$ alors

$V(\ \mathbf{StHa}_j,\ \mathbf{StHa}_{j-1},\ \mathbf{StHa}_{j-h-1}\ ;\ -\infty) - V(\ \mathbf{StHa}_j,\ \mathbf{StHa}_{j-1},\ \mathbf{StHa}_{j-h-1}\ ;\ +\infty) = -1$

et de vérifier que dans les quatre cas le résultat est égal à ε_h .

Le cas où P n'est pas unitaire se déduit du cas P unitaire et de la proposition 1 . ❑

Théorème 5

Les deux nombres $\mathbf{V_{StHa}}(P,Q)$ et $\mathbf{S_B}(P,Q)$ coincident.

démonstration:
mettre bout à bout les proposions 6 , 9 et 10 . ❑

e) Conclusions et remarques

Résumé des résultats obtenus

On peut résumer dans le théorème suivant les résultats obtenus

Théorème 6

a) (i) Les 2 nombres $\mathbf{V_{Stu}}(P,Q;a,b)$, $\mathbf{V'_{StHa}}(P,Q;a,b)$ coïncident.
(ii) Ils sont égaux à $\mathbf{c_+}(P,Q;a,b) - \mathbf{c_-}(P,Q;a,b)$.

b) (i) Les 3 nombres $\mathbf{V_{Stu}}(P,Q)$, $\mathbf{V_{StHa}}(P,Q)$, $C((\mathbf{sth_{p-k}}(P,Q))_{k=0,...,p})$ coïncident, et coïncident avec $\mathbf{S_B}(P,Q)$ lorsque P est unitaire.
(ii) Ils sont égaux à $\mathbf{c_+}(P,Q) - \mathbf{c_-}(P,Q)$.

démonstration:
a) (i) voir le théorème 2
a) (ii) voir le théorème 1 (i) de I.1
b) (i) voir les théorèmes 2 et 5 et la proposition 10.
b) (ii) : a) et au choix le théorème 1(ii) de I.1, ou le théorème 3. ❑

Dans la démonstration du point b) on a donc produit une démonstration du point (ii) du théorème 1 de I.1 (cas où l'intervalle est **R** tout entier) à partir du théorème 3 (méthode d'Hermite), ou inversement, et ceci essentiellement par des méthodes d'algèbre linéaire . Il est intéressant de noter que les preuves - toutes deux élémentaires - de ces deux théorèmes reposent sur des principes distincts : théorème des valeurs intermédiaires dans un cas, existence de racines complexes conjuguées dans l'autre. On pourrait aussi considérer qu'à partir des théorèmes 1 (ii) de I.1 et du théorème 3 on a produit une preuve de la proposition 9 sans utiliser les résultats de Frobenius sur les formes de Hankel.

Discussion

En définitive, quelle est donc la meilleure méthode pour calculer $\mathbf{c_+}(P,Q) - \mathbf{c_-}(P,Q)$?

La méthode de Sturm-Sylvester n'a que des inconvénients par rapport à la méthode de Sturm-Habicht : calculs dans un corps plutôt que dans un anneau, défauts de spécialisation, temps de calcul plus long . La méthode de Sturm-Habicht est en temps polynomial (si on travaille sur les entiers naturels, ou plus généralement sur un anneau où les déterminants se calculent en temps polynomial).
Etant obtenue par des changements de signes automatiques à partir de la suite des sous-résultants, la suite de Sturm-Habicht peut, elle aussi, se calculer par des méthodes modulaires.

La méthode d'Hermite donne elle aussi un algorithme (la méthode de réduction des formes quadratiques de Gauss donne naissance à des calculs explicites); il est toutefois plus intéressant de calculer la signature de B(P,Q) par la méthode des bezoutiens. En utilisant alors la méthode de Bareiss pour calculer les déterminants on a alors affaire (sur les entiers ou sur un anneau où les déterminants se calculent en temps polynomial) à un algorithme en temps polynomial. Du point de vue des spécialisations, rappelons que la méthode des bezoutiens se spécialise bien à condition qu'on travaille toujours en degré fixé pour P (voir remarque 4) .

Si on compare maintenant la méthode de Sturm-Habicht à celle des bezoutiens, on observe que la méthode de Sturm-Habicht donne des calculs plus rapides :

- en utilisant les relations entre sous-résultants et restes on donne un algorithme de calcul de toute la suite des sous-résultants plus rapide que le calcul d'un seul coefficient sous-résultant par la méthode de Bareiss (voir le point " complexité" dans le § 2), donc également plus rapide que le calcul des bezoutiens (qui est essentiellement le même que celui des sous-résultants). De plus la méthode de Sturm-Habicht s'applique au cas où P n'est pas unitaire et permet de calculer directement $\mathbf{c}_+(P,Q;a,b) - \mathbf{c}_-(P,Q;a,b)$.
- les propriétés de spécialisation de la suite de Sturm-Habicht sont meilleures : on peut en particulier traiter le cas où le degré de P baisse exactement de 1 alors que celui de Q ne change pas.
- pour calculer $\mathbf{c}_+(P,Q) - \mathbf{c}_-(P,Q)$, il faut noter que *la méthode la plus rapide est la suivante: calculer la suite des polynômes sous-résultants par un des algorithmes du § 2, en déduire la suite de Sturm-Habicht par des changements de signes automatiques, et évaluer les signes des seuls coefficients de Sturm-Habicht et appliquer la proposition 10* . (valable même pour P non unitaire). Ce qui donne un calcul en $O(n^2)$ opérations arithmétiques suivies de n évaluations de signes.

Dans l'état actuel des choses, on peut donc conclure en général à la supériorité de la méthode de Sturm-Habicht. La méthode des bezoutiens pourra toutefois peut-être s'avérer plus efficace dans certains cas, car elle repose sur les sommes de Newton qui sont des fonctions symétriques de calcul rapide (voir [Val]).

Remarque 5 :

On vient de voir que les calculs pour trouver le nombre de racines de P (resp.. la différence entre le nombre de racines de P rendant $Q > 0$ et le nombre de racines de P rendant $Q < 0$) sont essentiellement les mêmes dans la méthode d'Hermite (plus précisément celle des bezoutiens) et celle de Sturm (plus précisément celle de Sturm-Habicht).
Une différence essentielle entre la méthode d'Hermite (ou la méthode des bezoutiens) et celle de Sturm (ou de Sturm-Habicht) est que dans la méthode d'Hermite on traite globalement toutes les racines et qu'on ne peut étudier avec les seuls polynômes P et Q ce qui se passe sur un intervalle $]a,b[$. Une manière de pallier à cet inconvénient est d'introduire les polynômes $(a - x)\,Q$, $(b - x)\,Q$.

Nous allons voir sur un exemple que ces différents calculs donnent des résultats différents, et que les résultats les plus simples sont obtenus pour la suite de Sturm-Habicht de P et P' .

Exemple 3 :

Comparons donc les différents calculs qui permettent de déterminer la condition (C) pour que le nombre de racines réelles comprises strictement entre -1 et 1 d'un polynôme du troisième degré $P = x^3 + px + q$ sans racines doubles soit égale à trois :

1) calcul de la suite de Sturm-Habicht de P et évaluation en -1 et 1 :
on trouve que (C) est équivalente à:

$$p+q+1 > 0\,,\quad q-p-1 < 0\,,\quad p+3 > 0\,,\quad 2p+3q < 0\,,\quad -2p+3q > 0\,,$$
$$4p^3+27q^2 < 0\,,$$

2) calcul des suites de Sturm-Habicht de $x^3 + px + q$ et $1-x$, puis de $x^3 + px + q$ et $-1-x$ (ou méthode des bezoutiens pour $x^3 + px + q$ et $1-x$, puis pour $x^3 + px + q$ et $-1-x$):

on trouve que (C) est équivalente à:

$$4p^2+6p-9q < 0\ ,\quad 4p^2+6p+9q < 0\ ,\quad (p+q+1)(4p^3+27q^2) < 0\ ,$$
$$(q-p-1)(4p^3+27q^2) > 0\ ,$$

Il n'est pas immédiat que ces systèmes d'inégalités soient équivalents. Le résultat 1) est le plus simple, et ne peut être obtenu par la méthode des bezoutiens.

Bibliographie

Nous remercions M. Jouanolou pour nous avoir signalé la référence [Bor].

[Ait] Aitken A. C. : On the evaluation of determinants, the formation of their adjugates, and the practical solution of simultaneous linear equations. Proc. Edinburgh Math. Soc. ser 2 III , 207-219 , (1932)

[Bar] Bareiss E. H. : Sylvester's identity and multistep integer preserving Gaussian elimination. Math. Comp. 22, 565-578 (1968).

[Bor] Borchardt : Zur Theorie der Elimination und Kettenbruch-Entwichlung. Math. Abh. der Akad. der Wissenschaften zu Berlin, 1878, p 1-17.

[Bro] Brown W. S. : On Euclid's Algorithm and the Computation of Polynomial Greatest Common Divisors. JACM 18, 476-504 (1971)

[BroT] Brown W. S., Traub J. F. : On Euclid's Algorithm and the Theory of Subresultants. JACM 18, 505-514 (1971)

[Cha] Chardin M. : Contributions à l'algèbre commutative effective et à la théorie de l'élimination. Thèse à l'Université de Paris VI (1990). Centre de Mathématiques et Laboratoire d'informatique. Ecole Polytechnique. F-91128 Palaiseau Cédex

[Col] Collins G.E. Subresultants and Reduced Polynomial Remainder Sequences. JACM 14, 128-142 (1967)

[CoR] Coste M., Roy M.-F. : Thom's lemma, the coding of real algebraic numbers and the computation of the topology of semi-algebraic sets. J. Symbolic Computation 5 , 121-129 (1988).

[Fro] Frobenius : Uber das Traegheitsgesetz des quadratishen Formen, S-B Pruss. Akad. Wiss. 241-256 (Marz 1984) und 403-431 (Mai 1984)

[Gan] Gantmacher Fr. :Théorie des matrices, tome I. Dunod 1966.

[GLRR1] Gonzalez L., Lombardi H., Recio T., Roy M.-F. : Sturm-Habicht sequences. Proceedings ISSAC 1989 pages 136-146 .

[GLRR2] Gonzalez L., Lombardi H., Recio T., Roy M.-F. : spécialisation de la suite de Sturm et sous-résultants. Version détaillée, dans CALSYF journées du GRECO de Calcul Formel 1989.

[Gon] Gonzalez L. : The proof of the Sylvester theorem through Habicht sequences. Premrint Université de Santander 1988.

[Hab] Habicht W. : Eine Verallgemeinerung des Sturmschen Wurzelzählverfahrens. Comm. Math. Helvetici 21 , 99-116 (1948).

[Her] Hermite C. : Remarques sur le théorème de Sturm, C. R. Acad. Sci. Paris 36 , 52-54 (1853).

[KrN] Krein M. G. Naimark M.A. : The method of symmetric and hermitian forms on the theory of the separation of the roots of algebraic equations . Originalement publié à Kharkov (1936). Lin. Multilinear algebra 1981, 10 265-308 (1981).

[Las] Lascoux Alain : La résultante de deux polynômes. Séminaire d'Algèbre M.P. Malliavin (1984-85). (Lecture Notes in Mathematics)

[Lom] Lombardi Henri : Sous-résultants, suite de Sturm, spécialisation. in Thèse, 1989, à l'Université de Nice.

[Loo] Loos R. : Generalized poynomial reaminder sequences. Dans Computer Algebra, Symbolic and Algebraic Computation 115-138. Edité par Buchberger, Collins, Loos . Springer Verlag 1982.

[Mig] Mignotte M.: Some useful bounds. Dans Computer Algebra, Symbolic and Algebraic Computation 259-263. Edité par Buchberger, Collins, Loos . Springer Verlag 1982.

[Stu] Sturm C.: Mémoire sur la résolution des équations numériques. Inst. France Sc. Math. Phys. 6 (1835)

[Syl] Sylvester J. J. : On a theory of syzygetic relations of two rational integral functions,comprising an application to the theory of Sturm's function. Trans. Roy. Soc. London (1853).
reprint dans : Sylvester : Collected Math Papers. Chelsea Pub. Comp. NY 1983 vol 1 429-586

[Val] Vallibouze A.: Fonctions symétriques et changements de base, Thèse, Université Paris VI, 1987.

Théorie constructive élémentaire des corps ordonnés

THEORIE CONSTRUCTIVE ELEMENTAIRE DES CORPS ORDONNES

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

Marie-Françoise ROY
I R M A R
Université de Rennes 1
Campus de Beaulieu
35 042 Rennes cédex
France

Résumé On donne le développement constructif des bases de la théorie des corps ordonnés, jusqu'à la construction de la clôture réelle d'un corps ordonné. L'article peut être lu du point de vue des mathématiques classiques (preuves sans axiome du choix), ou des mathématiques récursives (algorithmes "à oracles" uniformément primitifs récursifs), ou des mathématiques constructives dans le style Bishop (théorie des corps ordonnés discrets).

Mots clés Corps ordonnés, Mathématiques constructives, Preuve par algorithme, Algorithme uniformément primitif récursif, Théorème algébrique des accroissements finis, Algorithme de Hörmander, Algorithme IF (inégalités formelles), Corps ordonné d-clos.

Abstract Classical theory of ordered fields (Artin-Schreier theory) makes an intensive use of non constructive methods, using in particular the axiom of choice. However since Tarski (and even since Sturm and Sylvester) one knows how to compute in the real closure of an ordered field **K** by computations only in **K**. This apparent contradiction is solved in this paper.
We give here a constructive proof of the first results of the theory of ordered fields, including the existence of the real closure.
The proofs can be interpreted in the particular philosophy of each reader. In a classical point of view for example, the effective procedures in the definitions may be interpreted as given by oracles. Hence one gets the existence of the real closure of an arbitrary ordered field without the axiom of choice. In a constructive framework "à la Bishop" one gets the existence of the real closure of a discrete ordered field. From the point of view of recursive theory the proofs give uniformly primitive recursive algorithms.

Key-words Ordered fields, Constructive Mathematics, Uniformly primitive recursive algorithms, Algebraic mean value theorem, Hörmander algorithm, Algorithm IF (formal inequalities), d-closed ordered fields.

1) Introduction

La théorie classique élémentaire des corps ordonnés (théorie d'Artin Schreier) fait un usage intensif des méthodes non constructives, notamment par un recours à l'axiome du choix. Par ailleurs, on sait depuis Tarski (d'une certaine manière depuis Sturm et Sylvester) calculer de manière explicite dans la clôture réelle d'un corps ordonné **K** en n'effectuant que des calculs dans **K** . Cette contradiction apparente est levée dans l'article qui suit.

Nous donnons en effet une preuve constructive des premiers résultats de la théorie des corps ordonnés, y compris l'existence de la clôture réelle d'un corps ordonné.

Nous renvoyons à **[MRR]** pour la théorie constructive des corps discrets.

Toutes les preuves peuvent être lues avec des lunettes adaptées à la philosophie ou au cadre de travail de chaque lecteur (lectrice) 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*, de l'existence de la clôture réelle d'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 (cf. **[KI]**) sous forme de Machines de Turing à oracles.

Si on adopte le point de vue constructif, on obtient la preuve de l'existence de la clôture réelle d'un corps ordonné discret.

Les outils essentiels pour constructiviser la théorie classique sont les suivants: une version constructive du théorème des accroissements finis pour un polynôme sur un corps ordonné; la notion d'algorithme cohérent d'attribution de signes dans un anneau de polynômes sur un corps ordonné **K**; la notion de corps ordonné d-clos.
L'utilisation de l'algorithme IF présenté dans **[CR]** permet en outre de donner une présentation particulièrement concrète de la preuve d'existence de la clôture réelle.
Nous donnons dans les paragraphes "commentaires" quelques précisions sur le point de vue constructif "à la Bishop".

A travers le papier "A real root calculus", de H. Zassenhaus [Za], nous avons découvert récemment la thèse de Hollkott [Ho]. Il y développe une problématique assez voisine de celle que nous donnons, mais en restant à un niveau très algorithmique. Ainsi, il n'introduit pas la notion de corps ordonné d-clos. Par ailleurs, il ne dispose pas de la version algébrique du théorème des accroissements finis, et cela le conduit à une acrobatie que nous pouvons interpréter en disant qu'il prouve le théorème de Rolle dans un corps ordonné d-clos pour les polynômes de degré $\leq d+1$, ceci par récurrence sur d . Notre papier peut être considéré comme une présentation moderne, et nous l'espérons, plus claire, des résultats de Hollkott. Merci à L. Gonzalez pour nous avoir communiqué la référence [Za] et à T. Sander pour nous avoir traduits quelques parties décisives de la thèse de Hollkott. Tomas Sander a pour sa part étudié récemment l'indépendance de l'existence de la clôture réelle par rapport à l'axiome du choix, dans le cadre de la théorie ordinaire des ensembles ZF ([Sa]).

Une version anglaise et moins détaillée de ce papier paraît dans les conférences du colloque MEGA 90 (édité chez Birkhaüser).

↖ Como pueden hacer esto chingada madre!

2) Préliminaires

Corps ordonnés discrets

Définitions

Nous renvoyons à **[MRR]** pour la théorie constructive des corps discrets. Néanmoins, les définitions qui suivent sont formulées de manière à être comprises aussi bien d'un point de vue classique que constructif.

Définitions 1 :

Un ensemble est dit *discret* lorsqu'il est donné dans une présentation où l'égalité de deux éléments de l'ensemble est décidable.

On appelle *corps discret*, un corps **K** donné dans une présentation où il est discret et où les lois de composition $(+ , \times , x \longmapsto -x , x \longmapsto 1/x)$ sont calculables.

On appelle *corps ordonné discret*, un corps ordonné **K** donné dans une présentation où les lois de composition $(+ , \times , x \longmapsto -x , x \longmapsto 1/x)$ sont calculables et où le signe d'un élément est décidable.

Un *intervalle ouvert* est par définition un ensemble $]a,b[$ où a et b sont dans **K** ou égaux à $+\infty$ ou $-\infty$.

Désormais, les corps ordonnés que nous considérons sont tous "ordonnés discrets" et les corps que nous considérons sont tous des "corps discrets".

Théorème des accroissements finis

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

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

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

Plus généralement on a les résultats suivants :

Lemme :

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

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

Very important!

Théorème 1 : (théorème des accroissements finis)

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

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

En particulier,

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

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

preuve> Le théorème est une conséquence immédiate du lemme: ce dernier fournit en effet des identités algébriques concernant les variables " a, b, et les coefficients du polynôme " qui s'appliquent alors dans tout anneau commutatif qui est une $\mathbb{Q}$-algèbre, et en particulier dans les corps commutatifs de caractéristique nulle.
Démontrons le lemme.
Par changement de variable affine, on se ramène au cas où $a = -1$ et $b = 1$. Considérons le degré n fixé. L'application $P \longmapsto P(1) - P(-1)$ est une forme linéaire ne faisant pas intervenir le coefficient constant. Les formes linéaires ne faisant pas intervenir le coefficient constant forment un espace de dimension n. Pour tout choix de n rationnels $\lambda_{i,n}$, les formes linéaires $P \longmapsto P'(\lambda_{i,n})$ sont indépendantes et ne font pas intervenir le coefficient constant. Il correspond donc à ce choix des rationnels $r_{i,n}$ qui rendent la formule vraie. La difficulté consiste à déterminer des $\lambda_{i,n} \in]0, 1[$ tels que les $r_{i,n}$ correspondants soient également sur $]0, 1[$. Les formules de quadrature de Gauss correspondent à un tel choix, mais avec des réels alors que nous voulons des rationnels. Il suffit alors de choisir des $\lambda_{i,n}$ rationnels suffisamment voisins des $\lambda_{i,n}$ de Gauss (zéros des polynômes de Legendre) pour que les $r_{i,n}$ correspondants restent positifs. ❑

Remarques 1 :
1) Une majoration et une minoration explicites de P' peuvent être calculées sur un intervalle borné, donc également un module de Lipschitz pour P.
2) Les identités algébriques énoncées dans le théorème 1 sont encore valables lorsque **K** est un anneau commutatif qui est une $\mathbb{Q}$-algèbre.

Lemme de Thom

Définitions et notations 2 :

On appelle *signe* un élément de $\{-1, 0, +1\}$. Un signe est dit *strict* s'il est $\neq 0$. Si x est un élément d'un corps ordonné et σ un signe, on écrira $x \equiv \sigma$ pour signifier que x a le même signe que σ.

Une partie d'un corps ordonné **K** est dite *convexe* si, chaque fois qu'elle contient deux éléments, elle contient tout élément compris entre ces deux éléments. Elle est dite *ouverte* si elle est réunion d'intervalles ouverts. Une fonction de **K** vers **K** est dite continue si l'image réciproque d'un ouvert est un ouvert.

Une *condition de signe* portant sur un élément x est une relation $x \equiv \sigma$. Une *condition de signe généralisée* (en abrégé csg) portant sur un élément x est une des relations $x < 0$, $x \leqslant 0$, $x = 0$, $x > 0$, $x \geqslant 0$, $x \neq 0$. Quand on remplace une condition de signe $x < 0$ ou $x > 0$ par la condition de signe généralisée associée $x \leqslant 0$ ou $x \geqslant 0$, on dit que la condition de signe a été *relâchée*.

Lemme : Une fonction polynôme est continue.

Théorème 2 : (lemme de Thom, version 1, corps ordonné sans hypothèse de clôture)
Soient un corps ordonné **K**, et P un polynôme de **K**[X], de degré n,
$[\sigma_0, \sigma_1, ..., \sigma_n]$ une liste de signes stricts.
L'ensemble $\{x : P(x) \equiv \sigma_0, P'(x) \equiv \sigma_1, ..., P^{(i)}(x) \equiv \sigma_i, ..., P^{(n)}(x) \equiv \sigma_n\}$

ensemble ouvert convexe .

Si on relâche les conditions de signes, et si l'ensemble était non vide, on rajoute au plus une borne inférieure et/ou une borne supérieure.

Si maintenant, on remplace la première condition de signe par $P(x) = 0$, l'ensemble possède au plus un point. En d'autres termes, deux racines distinctes de P attribuent deux signes distincts à au moins l'une des dérivées de P .

preuve> Le lemme résulte par exemple du fait qu'une fonction polynôme est localement lipschitzienne. Pour le théorème, on raisonne par récurrence sur le degré de P . On sait déjà que l'ensemble défini par les conditions de signes "à la Thom" est ouvert. Par hypothèse de récurrence, on peut supposer qu'on est sur un convexe contenant au moins 1 point, défini par les conditions de signe portant sur P', P'' etc... Sur cet ensemble la fonction P est strictement monotone d'après le théorème des accroissements finis. etc... ❑

Commentaire: D'un point de vue constructif, un ensemble qui possède au plus un point est un ensemble pour lequel il est absurde de supposer qu'il possède deux points distincts. Pour autant, on ne peut pas affirmer que l'ensemble possède forcément 0 ou 1 point. Dans un corps réel clos, on pourra par contre affirmer, dans la dernière phrase du théorème, que l'ensemble défini possède 0 ou 1 point, puisqu'un algorithme permettra de tester dans quel cas on se trouve.

Cônes premiers. Construction d'un corps ordonné par attribution d'un signe à tout élément d'un anneau commutatif

Soit $\mathbf{A}$ un anneau commutatif et α une partie décidable de $\mathbf{A}$. On dit que α est un *cône premier* de $\mathbf{A}$ si on a les quatre propriétés

1) $\forall\ x \in \mathbf{A}\ ,\ x^2 \in \alpha\ ,$
2) $\alpha + \alpha \subset \alpha\ ,$
3) $\alpha\ .\ \alpha \subset \alpha\ ,$
4) $\forall\ x, y \in \mathbf{A} \quad xy \in \alpha \Rightarrow [\ x \in \alpha$ **ou** $-y \in \alpha\ ]$

On appelle alors support de α et on note $\mathbf{Supp}(\alpha)$ l'intersection $\alpha \cap -\alpha$. C'est un idéal premier. Le corps de fractions de l'anneau quotient $\mathbf{A/Supp}(\alpha)$ est appelé le corps résiduel de α . On le note $k(\mathbf{Supp}(\alpha))$. C'est de manière naturelle un corps ordonné : les éléments positifs ou nuls de $k(\mathbf{Supp}(\alpha))$ sont les images des éléments de α .

Soit $\mathbf{K}$ un corps ordonné et $\mathbf{A}$ une $\mathbf{K}$-algèbre. Un cône premier α de $\mathbf{A}$ est dit *compatible avec l'ordre de* $\mathbf{K}$ si on a en outre

5) $\alpha \cap \mathbf{K} = \{\ x \in \mathbf{K}\ ;\ x \geqslant 0\ \}$

Le corps $k(\mathbf{Supp}(\alpha))$ est alors une extension ordonnée de $\mathbf{K}$.

Soit $\mathbf{L}$ une extension ordonnée de $\mathbf{K}$ et f un homomorphisme d'anneau de $\mathbf{A}$ dans $\mathbf{L}$. Alors $\mathbf{L}$ est une extension ordonnée de $k(\mathbf{Supp}(\alpha))$ si et seulement si :

$$\mathbf{A} \cap \{\ x \in \mathbf{A} :\ f(x) \geq 0 \text{ dans } \mathbf{L}\ \} = \alpha$$

Si les éléments de $\mathbf{A/Supp}(\alpha)$ sont algébriques sur $\mathbf{K}$, $k(\mathbf{Supp}(\alpha)) = \mathbf{A/Supp}(\alpha)$ et c'est une extension algébrique de $\mathbf{K}$. On dit alors que α est *algébrique sur* $\mathbf{K}$.

Lorsque $\mathbf{A} = \mathbf{K}[X]$ on note X_α l'image de X dans $k(\mathbf{Supp}(\alpha))$. Si de plus α est algébrique sur $\mathbf{K}$, $\mathbf{K}[X_\alpha]$ est le corps ordonné $k(\mathbf{Supp}(\alpha))$ tout entier.

Pour une partie α d'un anneau commutatif $\mathbf{A}$, les propriétés 1), 2), 3) ,4) peuvent être reformulées en considérant les trois parties $\alpha_0 = \alpha \cap -\alpha$, $\alpha_+ = \alpha - \alpha_0$ et $\alpha_- = -\alpha_+$ Les axiomes 1), 2), 3) et 4) se réécrivent alors en

1') $\mathbf{A}$ est réunion disjointe de α_0 , α , α , α , α

2'a) $\alpha_0 + \alpha \subset \alpha$,
2'b) $\alpha_+ + \alpha_+ \subset \alpha_+$,
3'a) $\alpha_0 . \alpha \subset \alpha_0$,
3'b) $\alpha_+ . \alpha_+ \subset \alpha_+$,

On peut enfin reformuler ces résultats en terme d'un *algorithme d'attribution de signes* dans l'anneau **A** . Construire un cône premier dans **A** revient en effet à attribuer un signe à tout élément de **A** , c.-à-d. à construire une fonction Sg: $\mathbf{A} \longrightarrow \{-1, 0, +1\}$.
On pose alors : $\alpha_0 = \{ x \in \mathbf{A} ; Sg(x) = 0 \}$, $\alpha_+ = \{ x \in \mathbf{A} ; Sg(x) = 1 \}$, $\alpha = \alpha_0 \cup \alpha_+$, $\alpha_- = \{ x \in \mathbf{A} ; Sg(x) = -1 \}$.
La condition 1') peut alors être remplacée par la seule condition:
1") $\alpha_- = -\alpha_+$

Définition 3 : Lorsque les conditions 1"), 2'a), 2'b), 3'a), 3'b), 5) sont vérifiées nous dirons que nous avons un *algorithme cohérent d'attribution de signes dans* **A**.

Remarque 2 : Si l'anneau $\mathbf{A}/\alpha$ est une extension algébrique de **K** , alors c'est un corps (un anneau commutatif discret intègre qui est une extension algébrique d'un corps **K** est nécessairement un corps).

Corps ordonnés d-clos

Corps ordonnés 2-clos et corps réels

Définitions

Définitions 4 :

Un corps est dit *réel* si : " 1 + une somme de carrés = 0 " est absurde.

Un corps ordonné est dit *d-clos* (où $d \geq 1$) si tout polynôme P de degré $\leq d$ qui change de signe entre a et b possède une racine sur l'intervalle d'extrémités a et b .

Remarques 3 : Tout corps ordonné est réel et 1-clos. Tout corps réel est de caractéristique nulle. Dans un corps ordonné d-clos, tout polynôme qui se décompose en facteurs de degrés $\leq$ d possède une racine sur tout intervalle où il change de signe.

Dans le cadre classique, la notion de corps ordonné d-clos ci-dessus est équivalente à la notion de corps réel d-clos donnée dans [**Bou**].

Commentaire : Dans la définition précédente "posséder une racine" est pris au sens constructif, c.-à-d. "une racine peut être calculée". Nous ne répèterons pas systématiquement ce genre de remarque dans la suite.

Proposition 3 : (Equivalence de deux notions)

Un corps ordonné est 2-clos si et seulement si tout positif est un carré. En particulier dans un corps ordonné est 2-clos, tout carré est une puissance 4 .

Réciproquement, un corps réel où tout carré est une puissance 4 peut être ordonné de manière unique, en prenant pour positifs les carrés, et il est alors ordonné 2-clos.

preuve> La première affirmation est démontrée comme au lycée. La seule non trivialité ensuite est que les carrés permettent d'ordonner un corps réel où tout carré est une puissance 4 . Si a est un élément non nul, on considère b vérifiant $b^4 = a^2$, puis on teste si $a = b^2$ ou $a = -b^2$. Ceci permet d'attribuer un signe à tout élément. Il s'agit ensuite de vérifier que la somme de deux positifs est un positif, c.-à-d. que la somme de deux carrés est un carré. Cela résulte facilement de la réalité de **K** . □

La proposition précédente justifie la définition qui suit:

Définition 5 : Un corps réel est dit *2-clos* si tout carré est une puissance 4 (c.-à-d. encore si, pour tout x, x ou $-x$ est un carré). Il est dit *d-clos* ($d \geq 3$) si en outre il est d-clos en tant que corps ordonné.

Construction de la 2-clôture d'un corps ordonné

Définition 6 :

Une extension ordonnée $\mathbf{R}$ d'un corps ordonné $\mathbf{K}$ est appelé une *2-clôture ordonnée (ou 2-clôture)* de $\mathbf{K}$ si c'est un corps ordonné 2-clos et si tout élément de $\mathbf{R}$ peut être obtenu à partir d'éléments de $\mathbf{K}$ par répétition des opérations arithmétiques et de l'opération: extraction d'une racine carrée d'un positif.

Nous donnons le théorème qui suit essentiellement à titre de mise en jambe pour la construction de la clôture réelle d'un corps ordonné, qui sera démontrée par une technique analogue.

Théorème 4 :

Tout corps ordonné $\mathbf{K}$ possède une 2-clôture, unique à un $\mathbf{K}$-isomorphisme croissant unique près.

preuve> Si a est un élément positif de $\mathbf{K}$, on constate facilement qu'il existe une extension ordonnée de $\mathbf{K}$ obtenue en "rajoutant" une racine carrée positive de a : sans préjuger du fait que $\mathbf{K}$ possédait déjà ou non une telle racine carrée positive, on peut attribuer sans ambiguïté un signe à toute expression $x + y\sqrt{a}$, où x et y sont dans $\mathbf{K}$ (on procède comme au lycée), donc également à toute expression $Q(\sqrt{a})$ où $Q \in \mathbf{K}[X]$, en considérant le reste de la division de $Q(X)$ par $X^2 - a$; il reste alors à vérifier que l'on a ainsi un algorithme cohérent d'attribution des signes dans $\mathbf{K}[X]$, qui est derechef noté $\mathbf{K}[\sqrt{a}]$.
Cette extension ordonnée est unique à un $\mathbf{K}$-isomorphisme croissant unique près, parce qu'il n'y a pas d'ambiguïté possible dans l'attribution d'un signe à $x + y\sqrt{a}$: plus précisément, on a le résultat suivant : si $\mathbf{L}$ est une extension ordonnée de $\mathbf{K}$ où a possède une racine carrée positive λ, alors il existe un $\mathbf{K}$-isomorphisme croissant unique de $\mathbf{K}[\sqrt{a}]$ vers $\mathbf{K}[\lambda]$ (sous corps de $\mathbf{L}$ engendré par $\mathbf{K}$ et λ). D'où on déduit le :

Lemme : Supposons a et $b > 0$ dans un corps ordonné $\mathbf{K}$, alors il existe un unique $\mathbf{K}$-isomorphisme croissant de $\mathbf{K}[\sqrt{a}][\sqrt{b}]$ vers $\mathbf{K}[\sqrt{b}][\sqrt{a}]$.

En itérant cette construction, on va voir qu'on obtient une extension algébrique ordonnée $\mathbf{R}$ de $\mathbf{K}$ où tous les positifs sont des carrés.
Concrètement, tout élément de $\mathbf{R}$ apparaît comme construit en un nombre fini d'étapes h : il est alors de la forme $x_h + y_h\sqrt{a_h}$ où x_h, y_h, a_h sont 3 éléments d'une extension $\mathbf{K}[\sqrt{a_1}][\sqrt{a_2}]...[\sqrt{a_{h-1}}]$ construite à l'étape $h-1$, avec a_h positif.
Considérons maintenant l'union disjointe de toutes les extensions $\mathbf{K}[\sqrt{a_1}][\sqrt{a_2}]...[\sqrt{a_i}]$ possibles. La 2-clôture cherchée sera un quotient de cette union.
Soient :

$\mathbf{K}_1 = \mathbf{K}[\sqrt{a_1}][\sqrt{a_2}]...[\sqrt{a_i}]$ (avec $a_{h\,(h=1,...,i)}$ positif dans $\mathbf{K}[\sqrt{a_1}][\sqrt{a_2}]...[\sqrt{a_{h-1}}]$)
et $\mathbf{K}_2 = \mathbf{K}[\sqrt{b_1}][\sqrt{b_2}]...[\sqrt{b_j}]$ (avec $b_{h\,(h=1,...,j)}$ positif dans $\mathbf{K}[\sqrt{b_1}][\sqrt{b_2}]...[\sqrt{b_{h-1}}]$).
Définissons $\mathbf{K}' = \mathbf{K}_1[\sqrt{b_1}][\sqrt{b_2}]...[\sqrt{b_j}]$ et $\mathbf{K}'' = \mathbf{K}_2[\sqrt{a_1}][\sqrt{a_2}]...[\sqrt{a_i}]$.

Ces définitions sont possibles parce que, par exemple, le fait que a_h est positif dans $\mathbf{K}[\sqrt{a_1}][\sqrt{a_2}]...[\sqrt{a_{h-1}}]$ peut être testé par des calculs dans $\mathbf{K}$ qui sont a fortiori valable dans $\mathbf{K}_2$.

En utilisant plusieurs fois le lemme on construit un $\mathbf{K}$-isomorphisme croissant de $\mathbf{K}'$ vers $\mathbf{K}''$, et cet isomorphisme est manifestement unique.

Par définition, des éléments de $\mathbf{K}_1$ et de $\mathbf{K}_2$ sont équivalents si ils sont "égaux" via cet isomorphisme. Il faut vérifier que cette relation est bien une relation d'équivalence compatible avec la structure de corps ordonné: la réflexivité et la symétrie sont immédiates. La transitivité s'obtient en considérant les isomorphismes uniques liant des extensions composées obtenues à partir des trois extensions en cause.

La 2-clôture cherchée est alors le quotient de l'union disjointe des $\mathbf{K}[\sqrt{a_1}][\sqrt{a_2}]...[\sqrt{a_i}]$ pour cette relation d'équivalence. ❑

Commentaire: Il est impossible de démontrer constructivement que tout corps réel peut être ordonné, ou plus prosaïquement qu'on puisse, dans un corps réel, soit rajouter une racine carrée de a, soit rajouter une racine carrée de $-a$, et obtenir une extension réelle : il faudrait pour cela être capable d'affirmer que a ou $-a$ n'est pas une somme de carrés. Ceci impliquerait manifestement le "très petit principe d'omniscience" (LLPO), qui n'est pas admissible constructivement (cf. [**MRR**] chap. 1 à ce sujet). On trouvera un exemple de corps réel récursivement présenté mais non récursivement ordonnable dans [**MN**].

Corps ordonnés d-clos

Introduction

Théorème 5 :

Dans un corps ordonné d-clos $\mathbf{K}$, la liste ordonnée $[\alpha_1, ..., \alpha_i]$ des racines d'un polynôme P de degré $\leq d$ peut être calculée.

En outre, si $\alpha_0 = -\infty$, $\alpha_{i+1} = +\infty$, le polynôme P est de signe strict constant sur chaque intervalle $]\alpha_j, \alpha_{j+1}[$ $(0 \leq j \leq i)$ dans n'importe quelle extension ordonnée de $\mathbf{K}$.

NB : $i = 0$ si P ne possède pas de racine dans $\mathbf{K}$.

preuve> On raisonne par récurrence sur le degré de P. On suppose donc qu'on a calculé les racines de P'. Ceci permet déjà d'expliciter les racines communes à P et P'. Si maintenant a et b sont deux racines consécutives de P', le polynôme P' a même signe sur tout l'intervalle $]a,b[$ qu'en $(a+b)/2$. Donc P est strictement monotone sur cet intervalle et s'annule au plus une fois. Il s'annule si et seulement si $P(a).P(b) < 0$, auquel cas la racine peut être calculée dans $\mathbf{K}$ (d'après la définition d'un corps d-clos). Même raisonnement avec le ou les deux intervalles d'extrémité du tableau de variation de P, en remplaçant $+\infty$ ou $-\infty$ par un élément au delà duquel le polynôme est de signe connu. ❑

Pero eso de que se puede calcular es muy relativo

Commentaires: 1) Une formulation constructive plus "provocante" du théorème ci-dessus est la suivante : Dans un corps ordonné d-clos, les racines d'un polynôme de degré $\leq d$ forment un ensemble fini, et le polynôme n'admet pas d'autre racine dans une extension ordonnée de $\mathbf{K}$.

2) La mise à plat de la preuve par récurrence du théorème 5 conduirait à appliquer la méthode de Hörmander à la liste [P] pour déterminer les racines de P (cf. §4).

Algorithmes de Sturm et de Sturm-Sylvester

Rappelons tout d'abord comment est construite la suite de Sturm pour les polynômes P et Q :

$\mathbf{Stu}_0(P,Q) := P$, $\mathbf{Stu}_1(P,Q) := \mathbf{Rst}(P'Q,P)$,

$\mathbf{Stu}_{i+1}(P,Q) := -\mathbf{Rst}(\mathbf{Stu}_i(P,Q),\mathbf{Stu}_{i-1}(P,Q)$ (on s'arrête au dernier reste non nul).

La suite de Sturm de P est obtenue en prenant Q = 1 . On note $V_{St}(P,Q;a)$ le nombre de variations de signes dans la suite des $\mathbf{Stu}_i(P,Q)(a)$ (sans tenir compte des 0) , et $V_{St}(P,Q;a,b)$ la différence $V_{St}(P,Q;a) - V_{St}(P,Q;b)$.
Le théorème de Sturm-Sylvester affirme que, dans le cas d'un corps réel clos, si $a < b$ sont non racines de P , le nombre $V_{St}(P,Q;a,b)$ est égal au nombre de racines de P sur]a,b[rendant $Q > 0$ moins le nombre de racines de P sur]a,b[rendant $Q < 0$.

Théorème 6 : (polynôme de degré ≤ d dans un corps ordonné d-clos)

Soit **K** un corps ordonné sous corps d'un corps ordonné d-clos **L** . Les algorithmes de Sturm (pour le nombre de racines de P sur un intervalle donné, dans **L**) et de Sturm-Sylvester (pour le nombre de racines de P rendant $Q > 0$ sur un intervalle donné, dans **L**) donnent un résultat correct si P est de degré ≤ d .

preuve> la preuve classique fonctionne sans problème, vu le théorème précédent (cf. par exemple [**GLRR**] pour la preuve classique) ❑

Remarque 4 : Il y a des exemples de corps ordonnés avec des polynômes P de signe constant sur un intervalle, mais avec un nombre de racines > 0 prescrit par l'algorithme de Sturm: rajouter à $\mathbb{Q}$ un infiniment petit positif ε , considérer le polynôme $P = (X^2 - \varepsilon^3).(X^3 - \varepsilon^4)$ et l'intervalle $[\varepsilon^2,\varepsilon]$.

Proposition 7 : (polynôme de degré d+1 dans un corps ordonné d-clos)

On suppose que P est un polynôme de degré d+1 à coefficients dans un corps ordonné d-clos **K** . On considère un intervalle I du corps **K** , P ne s'annulant pas aux extrémités de l'intervalle.

Si P est sans facteur carré, l'algorithme de Sturm (pour le nombre de racines de P sur l'intervalle I) compte le nombre de changements de signes de P sur l'intervalle . En particulier, le nombre de racines de P dans **K** sur l'intervalle est au plus égal à celui, positif ou nul, prévu par l'algorithme de Sturm.

Si P est décomposable dans **K**[X] , en particulier s'il possède un facteur carré, l'algorithme de Sturm compte le nombre racines de P dans **K** sur l'intervalle.

preuve> Si P est sans facteur carré, on répète la preuve classique en omettant les racines de P dans le tableau de toutes les racines des polynômes de la suite de Sturm (sauf celles qui sont déjà racines de l'un des autres polynômes). Si P est décomposable on peut répéter la preuve donnée dans [**GLRR**][1] parce que P possède une racine sur tout intervalle où il change de signe, de même que les autres polynômes de la suite de Sturm (qui sont de degré ≤ d). ❑

Le lemme de Thom

Théorème 8 : (lemme de Thom, version 2, corps ordonné d-clos)

Soient un corps ordonné d-clos **K** , P un polynôme de **K**[X], de degré $n \leqslant d$, et $[\sigma_0, \sigma_1, ..., \sigma_n]$ une liste de signes stricts.

L'ensemble $\{ x ; P(x) \equiv \sigma_0 , P'(x) \equiv \sigma_1 , ..., P^{(i)}(x) \equiv \sigma_i , ..., P^{(n)}(x) \equiv \sigma_n \}$ est ou bien vide, ou bien un intervalle ouvert ayant pour chaque extrémité $+\infty$, $-\infty$, ou une racine de l'un des polynômes P , P' , P" etc... .

---

[1] Dans le cas où le Pgcd de P et P'Q est ≠ 1 , la preuve, plus subtile que la preuve ordinaire, est basée sur

Si on relâche les conditions de signes, et si l'ouvert était un intervalle non vide, on obtient l'intervalle fermé correspondant.

Si maintenant, on remplace la première condition de signe par $P(x) = 0$, l'ensemble possède zéro ou un point.

NB: Ce théorème doit être lu d'un point de vue constructif. La première affirmation signifie que les extrémités de l'intervalle sont calculables à partir des données; la dernière signifie qu'il y a un algorithme pour décider si l'ensemble possède zéro ou un point, et dans ce dernier cas, l'algorithme fournit le point.

preuve> Preuve par récurrence sur le degré du polynôme. Quand on coupe un intervalle bien précisé en deux, en un endroit bien précisé, chaque moitié est un intervalle bien précisé. ❑

Définition 7 :

Soit **K** un corps ordonné possédant une d-clôture **R** . Un élément ξ de **R** est dit *codé à la Thom* (dans **K**) s'il est présenté comme racine d'un polynôme P , de degré $\leq d$, de $\mathbf{K}[X]$, en précisant les signes stricts de $P'(\xi)$, $P''(\xi)$, etc...

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

L'algorithme IF

Nous rappelons brièvement dans ce paragraphe l'algorithme IF ("inégalités formelles simultanées") proposé dans **[CR]** en vue de calculer avec des nombres réels algébriques présentés via des systèmes d'équations emboîtées, dont les racines sont spécifiées "à la Thom" pour chaque nouvelle équation introduite (cf. également **[BKR]**) . Vus les théorèmes 6 et 8 déjà établis pour les corps ordonnés d-clos, l'algorithme pourra s'appliquer pour tout corps ordonné **K** qui possède une extension ordonnée d-close **R** .

Petit préliminaire

Un *système d'équations algébriques emboîtées sur le corps* **K** (ou encore *système triangulaire d'équations algébriques sur le corps* **K**) est donné par une liste de polynômes $\mathbf{P} := [P_1,P_2,...,P_k]$ avec

$$P_1 \in \mathbf{K}[X_1] \ , \ P_2 \in \mathbf{K}[X_1,X_2] \ , \ ... \ , \ P_k \in \mathbf{K}[X_1,X_2,...,X_k]$$

chaque P_j étant unitaire de degré d_j en tant que polynôme en X_j

Le système est dit *normalisé* si les conditions suivantes sur les degrés sont réalisées

$$d_j \geq 2 \text{ pour tout } j \text{ et } d_{X_h}(P_j) < d_h \text{ pour tout } h < j$$

Une *solution réelle du système défini par la liste* **P** est un k-uple $\xi = [\xi_1,\xi_2,...,\xi_k]$ dans une extension ordonnée de **K** , avec :

$$P_1(\xi_1) = 0 \ , \ P_2(\xi_1,\xi_2) = 0 \ , \ ... \ , \ P_k(\xi_1,\xi_2,...,\xi_k) = 0 \ .$$

On est alors amené naturellement à travailler dans le corps $\mathbf{K}[\xi_1,\xi_2,...,\xi_k]$.

Si **K** possède une extension ordonnée d-close **R** , et si tous les d_i sont inférieurs ou égaux à d , les solutions réelles dans **R** du système emboîté peuvent être caractérisées "à la Thom", à l'étage i , par la liste des signes des dérivées de $P_i(\xi_1,\xi_2,...,\xi_{i-1},X)$ en $X = \xi_i$

L'algorithme IF proprement dit

Soient $P, Q_1, Q_2, \ldots, Q_n$ des polynômes de $\mathbf{K}[X]$ avec $\deg(P) \leqslant d$, $[\sigma_1, \sigma_2, \ldots, \sigma_n]$ une liste de signes stricts. Supposons que $\mathbf{K}$ possède une extension ordonnée d-close $\mathbf{R}$. On peut déterminer le nombre de racines de P (dans $\mathbf{R}$) qui attribuent les signes $\sigma_1, \sigma_2, \ldots, \sigma_n$ aux polynômes $Q_1, Q_2, \ldots, Q_n$ en calculant le nombre de racines de P rendant R_i positif, le nombre de racines de P rendant R_i négatif et le nombre de racines de P rendant R_i nul, où R_i parcourt les 3^n produits de Q_j pris à la puissance 0, 1 ou 2. (en fait on peut se ramener à un calcul nettement plus court, cf. [**BKR**]). Ceci donne en particulier un test dans $\mathbf{K}$ pour savoir s'il existe une racine de P dans $\mathbf{R}$ vérifiant un codage à la Thom particulier, puis pour calculer le signe de $Q(\xi)$ si ξ est une racine de P dans $\mathbf{R}$ codée à la Thom dans $\mathbf{K}$. Autrement dit cela permet de ramener tous les calculs dans $\mathbf{K}[\xi]$ à des calculs dans $\mathbf{K}$.

Si maintenant, on considère un système d'équations emboîtées, toutes de degré $\leqslant d$, on pourra appliquer l'algorithme précédent de manière itérative (par rapport au nombre de variables) et déterminer, par des calculs dans $\mathbf{K}$ tous les codages à la Thom des solutions $(\xi_1,\xi_2,\ldots,\xi_k)$ dans $\mathbf{R}^k$ du système considéré.

Pour une de ces solutions, soit $(\xi_1,\xi_2,\ldots,\xi_k)$, l'algorithme IF permet alors de calculer le signe de $Q(\xi_1,\xi_2,\ldots,\xi_k)$ où $Q \in \mathbf{K}[X_1,X_2,\ldots,X_k]$.

Autrement dit les calculs dans $\mathbf{K}[\xi_1,\xi_2,\ldots,\xi_k]$ sont ramenés à des calculs dans $\mathbf{K}$. D'où le :

Théorème 9 : Si un corps ordonné $\mathbf{K}$ possède une extension ordonnée d-close $\mathbf{R}$, on peut, uniquement par des calculs dans le corps ordonné $\mathbf{K}$, expliciter la structure de corps ordonné de toute extension $\mathbf{K}[\xi_1,\xi_2,\ldots,\xi_k]$ contenue dans $\mathbf{R}$ et définie par un système d'équations emboîtées, où chaque ξ_i est spécifié "à la Thom" comme racine d'un polynôme de degré $\leq d$ et à coefficients dans l'extension précédente $\mathbf{K}[\xi_1,\xi_2,\ldots,\xi_{i-1}]$.
L'existence, à chaque étage, d'une racine dans $\mathbf{R}$ répondant à la spécification "à la Thom" choisie, se vérifie également par des calculs dans le corps ordonné $\mathbf{K}$.

Remarques 5 : On entend par "calculs dans le corps ordonné $\mathbf{K}$ " des calculs qui font intervenir exclusivement la structure de corps ordonné de $\mathbf{K}$. On notera que le théorème 9 implique que, si elle existe, la d-clôture de $\mathbf{K}$ est essentiellement unique.

Corps réels clos

Définition 8 : Un corps $\mathbf{K}$ est dit *réel clos* s'il est ordonné et d-clos pour tout entier d, c.-à-d. encore s'il possède un ordre unique défini par ses carrés et si tout polynôme qui change de signe sur un intervalle possède une racine sur l'intervalle.

Théorème 10 : Soit $\mathbf{K}$ un corps. Les propriétés suivantes sont équivalentes

a) $\mathbf{K}$ est ordonné, tout positif est un carré, tout polynôme de degré impair possède une racine

a') $\mathbf{K}$ est réel, tout carré est une puissance 4, tout polynôme de degré impair possède une racine

b) $\mathbf{K}$ est ordonné et tout polynôme possède le nombre de racines que lui prescrit l'algorithme de Sturm (ceci sous entend que le nombre prescrit est toujours positif ou nul)

c) $\mathbf{K}$ est réel et tout polynôme est décomposable en facteurs de degré un ou deux

d) -1 n'est pas un carré et $\mathbf{K}[\sqrt{-1}]$ est algébriquement clos

e) $\mathbf{K}$ est réel clos

preuve> e) $\Rightarrow$ a) $\Rightarrow$ a') immédiat. a') $\Rightarrow$ a) cf. proposition 3
a) $\Rightarrow$ d)la preuve classique fonctionne ([**BCR**] p 9) . On peut également répéter la preuve donnée dans [**MRR**] p 189-191 pour les nombres algébriques complexes.
d) $\Rightarrow$ c)Il est clair que tout polynôme se décompose en facteurs de degré 1 ou 2 . Ensuite, pour tout a dans $\mathbf{K}$, a ou $-a$ est un carré : il suffit de décomposer le polynôme $T^4 - a$ en un produit de 2 polynômes unitaires de degré 2 et d'identifier. Enfin, la somme de deux carrés est un carré : on écrit $a + b\sqrt{-1} = (c + d\sqrt{-1})^2$, d'où : $a^2 + b^2 = (c^2 + d^2)^2$
c) $\Rightarrow$ e)Pour tout a , a ou $-a$ est un carré (comme ci-dessus); donc $\mathbf{K}$ est ordonné 2-clos; on construit ensuite facilement le tableau des signes d'un polynôme arbitraire, et il est alors clair qu'il s'annule sur tout intervalle où il change de signe (les facteurs irréductibles de degré 2 n'influent pas sur le tableau de signes).
e) $\Rightarrow$ b) résulte d'un théorème déjà démontré dans le cadre des corps ordonnés d-clos
b) $\Rightarrow$ e)$\mathbf{K}$ est 2-clos parce que l'algorithme de Sturm prescrit 2 racines à un polynôme $X^2 - a$ si $a > 0$; puis par récurrence sur d on prouve que $\mathbf{K}$ est ordonné d-clos, en utilisant la proposition 7 pour passer de d à d+1 . ❑

3) Construction de la clôture réelle d'un corps ordonné

Rajout d'une racine à un polynôme de degré d+1 dans un corps ordonné d-clos

Théorème 11 : Soit $\mathbf{K}$ un corps ordonné d-clos, P un polynôme de degré d+1 , $a < b$ deux éléments de $\mathbf{K}$. On suppose $P(a).P(b) < 0$ et P' de signe constant sur $]a,b[$ (ce qui est décidable).

Il est possible d'attribuer un signe à tout élément de $\mathbf{K}[X]$ de manière à obtenir une extension ordonnée, notée $\mathbf{K}[X_\alpha]$ (X_α est la classe d'équivalence de X), de $\mathbf{K}$, où X_α est racine de P sur l'intervalle $]a,b[$.

En outre cette extension est unique à $\mathbf{K}$-isomorphisme croissant unique près, c.-à-d. : pour toute extension ordonnée $\mathbf{L}$ de $\mathbf{K}$ qui possède un élément ξ racine de P sur $]a,b[$, il existe un unique $\mathbf{K}$-isomorphisme croissant de $\mathbf{K}[X_\alpha]$ vers $\mathbf{K}[\xi]$

preuve> Supposons par exemple que P' soit positif sur l'intervalle.
Soit Q un polynôme de $\mathbf{K}[X]$, imaginons qu'il ait une racine ξ sur l'intervalle $]a,b[$ dans une extension ordonnée de $\mathbf{K}$ et cherchons à attribuer un signe à $Q(\xi)$.
Soit Q_1 le reste de la division de Q par P . Si Q_1 est nul, (cas 1), on doit poser $Sg(Q) := 0$.
Sinon, calculons les racines de Q_1 situées sur l'intervalle $]a,b[$, d'où la liste ordonnée $[a=u_0, u_1, ..., u_n=b]$. Les valeurs successives de P sont en ordre strictement croissant. Si $P(u_i) = 0$ pour un certain i , (cas 2), on pose $Sg(Q) := 0$. Sinon, (cas 3), P passe du signe $-$ au signe $+$ sur un et un seul des sous intervalles $[u_i, u_{i+1}]$, et Q_1 est de signe constant connu σ sur l'intervalle $]u_i, u_{i+1}[$. On pose alors $Sg(Q) := \sigma$.

Comme nous n'avions pas la liberté de faire une autre affectation de signe dans le cadre d'une extension ordonnée de **K** où P admet une racine ξ sur l'intervalle]a,b[, cela montre l'unicité de l'extension à **K**-isomorphisme croissant unique près. Et on a aussi établi :

Lemme: Si P possède une racine c dans **K** ou dans une extension ordonnée de **K** sur l'intervalle]a,b[, l'affectation de signe définie ci-dessus vérifie : Sg(Q) = Signe de (Q(c)), et donc c'est une affectation de signe cohérente.

Nous allons voir que nous avons dans tous les cas une affectation cohérente de signes dans **K**[X] . Les conditions 1") et 5) sont trivialement vérifiées. Avant de passer aux autres conditions, faisons une remarque préliminaire: si au cours de la démonstration, nous sommes amenés à affecter 0 à un $R(\alpha)$ avec $\deg(R) < d$, cela signifie que $P(c) = 0$ pour une racine c de R sur]a,b[, donc c dans **K** , nous pouvons alors court-circuiter la démonstration en faisant appel au lemme précédent (notez que nous ne faisons pas pour autant l'hypothèse non constructive selon laquelle P admet ou n'admet pas de racine dans **K** sur l'intervalle]a,b[ ). Nous pouvons supposer en particulier que nous ne sommes jamais dans le cas 2) où P admet une racine dans **K** sur l'intervalle considéré.

2'a) et 3'a) : supposons Q dans α_0 , et S dans α_0 ou α_+ ; comme nous évitons le cas 2), Q est multiple de P, donc QR également, et par ailleurs Q + S et S ont le même reste modulo P .

2'b) : $\alpha_+ + \alpha_+ \subset \alpha_+$: $Sg(S) = +1$, $Sg(Q) = +1$, le reste de la division de Q+S par P est Q_1+S_1 . Notons $[u_0, u_1, \ldots, u_n]$, $[v_0, v_1, \ldots, v_m]$ et $[w_0, w_1, \ldots, w_p]$ les subdivisions introduites avec les racines de S_1 , Q_1 et Q_1+S_1 respectivement. On peut les fusionner en une seule subdivision, les 2 polynômes S_1 et Q_1 ont le signe + sur l'intervalle ouvert où P change de signe (ce sont des sous-intervalles des intervalles considérés séparément pour S_1 et Q_1) donc également Q_1+S_1 , et cet intervalle est un sous-intervalle de celui qui doit être considéré pour l'attribution d'un signe à Q+S via Q_1+S_1 .

3'b) : $\alpha_+ \times \alpha_+ \subset \alpha_+$: le reste de la division de Q.S par P est égal au reste R de la division de $Q_1.S_1$ par P , ce qui donne $Q_1.S_1 = A.P + R$, avec $\deg(A) < d$. Si A_1 est nul, nous raisonnons comme au cas précédent. Sinon, nous fusionnons les subdivisions associées aux polynômes R , A , Q_1 et S_1 . Sur l'intervalle ouvert minimum ( ]c,d[ ) de la subdivision où P change de signe, on sait déjà que Q_1 et S_1 ont le signe + 1 . Soit σ le signe de A sur cet intervalle. Le polynôme P a le signe $-\sigma$ en l'une des extrémités c, d, et également, vue la continuité de la fonction P, en un point c' intérieur à]c,d[. On a :

$$R(c') = (-A.P + Q_1.S_1)(c') > 0 . \quad \square$$

Commentaire : Notons que si **K** est une partie détachable de $\mathbf{K}[X_\alpha]$, alors on est capable de dire si P admet ou non une racine dans **K** sur l'intervalle. Inversement, si on est capable de calculer un facteur irréductible (dans **K**[X]) de P , changeant de signe sur l'intervalle, alors **K** est une partie détachable de $\mathbf{K}[X_\alpha]$. Fort heureusement, la construction de $\mathbf{K}[X_\alpha]$ est indépendante de telles hypothèses, qui ne sont en général pas vérifiées d'un point de vue constructif.

Une preuve "abstraite"

Définitions 9 :

On appelle clôture réelle d'un corps ordonné **K** une extension ordonnée algébrique de **K** qui est un corps réel-clos.

Une extension ordonnée **R** d'un corps ordonné **K** est appelé une *d-clôture (ordonnée)* de **K** si c'est un corps ordonné d-clos et si tout élément de **R** peut être obtenu à partir

d'éléments de $\mathbf{K}$ par répétition des opérations arithmétiques et de l'opération: calcul d'une racine d'un polynôme de degré $\leq d$.

Théorème 12 : Tout corps ordonné $\mathbf{K}$ possède une clôture réelle, unique à $\mathbf{K}$-isomorphisme croissant unique près.

preuve> Nous raisonnons par récurrence sur d pour montrer que:

H(d) : Pour tout corps ordonné $\mathbf{K}$, on peut construire une d-clôture ordonnée $\mathbf{K}^{(d)}$ de $\mathbf{K}$. En outre, pour toute extension ordonnée d-close $\mathbf{L}$ de $\mathbf{K}$, il existe un unique $\mathbf{K}$-homomorphisme croissant de $\mathbf{K}^{(d)}$ vers $\mathbf{L}$.

Pour $d=1$, il n'y a rien à prouver.

Supposons l'hypothèse vraie pour d. Si $\mathbf{K}$ est un corps ordonné, si P est un polynôme unitaire de degré $d+1$ dans $\mathbf{K}^{(d)}[X]$, et si a et b sont deux racines consécutives de P' vérifiant $P(a).P(b) < 0$, nous noterons :

$\alpha :=$ le cône construit comme au théorème 11 à partir de (P,a,b),

et donc, conformément aux notations précédemment définies :

$\mathbf{K}^{(d)}[X_\alpha]$ l'extension de $\mathbf{K}^{(d)}$ définie à partir de α

$\mathbf{K}^{(d)}[X_\alpha]^{(d)}$ la d-clôture du corps $\mathbf{K}^{(d)}[X_\alpha]$

Nous avons une construction analogue pour le premier, le dernier ou l'unique intervalle du tableau de variation de P, c.-à-d. que nous pouvons prendre $a = -\infty$ et $b =$ la première racine de P' etc...

Cette dirons que "$\mathbf{K}^{(d)}[X_\alpha]$ est bien défini" pour signifier que les conditions requises pour P, a, b sont bien vérifiées.

Nous itérons maintenant cette construction et utilisons la notation :

$$\mathbf{K}^{(d)}[X_{\alpha 1}]^{(d)}[X_{\alpha 2}]^{(d)}...[X_{\alpha i}]^{(d)}.$$

Pour obtenir $\mathbf{K}^{(d+1)}$ nous allons "recoller" entre elles toutes ces extensions: ce qui revient à introduire une bonne relation d'"égalité" sur leur réunion disjointe.

Nous établissons tout d'abord un lemme (sous l'hypothèse de récurrence H(d)).

Lemme : Si $\mathbf{L}$ est une extension ordonnée d-close de $\mathbf{K}$ et si $\mathbf{K}^{(d)}[X_\alpha]$ est bien défini, alors $\mathbf{L}[X_\alpha]$ est bien défini, et il existe un unique $\mathbf{K}$-homomorphisme croissant de $\mathbf{K}^{(d)}[X_\alpha]^{(d)}$ vers $\mathbf{L}[X_\alpha]^{(d)}$.

Supposons $\alpha = (P,a,b)$. Comme il y a un unique $\mathbf{K}$-homomorphisme croissant de $\mathbf{K}^{(d)}$ vers $\mathbf{L}$, les points a et b et le polynôme P sont définis sans ambiguïté dans $\mathbf{L}$, qui peut être vue comme une extension ordonnée de $\mathbf{K}^{(d)}$. En outre, comme P' est de degré d, ses racines dans $\mathbf{K}^{(d)}$ sont ses seules racines dans $\mathbf{L}$ (cf. théorème 5). Donc a et b sont bien deux racines consécutives de P' dans $\mathbf{L}$ (raisonnement analogue dans les cas avec ∞). On applique ensuite le théorème 11 et H(d) pour obtenir l'existence et l'unicité du $\mathbf{K}$-homomorphisme croissant de $\mathbf{K}^{(d)}[X_\alpha]^{(d)}$ vers $\mathbf{L}[X_\alpha]^{(d)}$. ❑

Nous pouvons maintenant recoller nos extensions :

si $\mathbf{K}_1 = \mathbf{K}^{(d)}[X_{\alpha 1}]^{(d)}[X_{\alpha 2}]^{(d)}...[X_{\alpha i}]^{(d)}$ et $\mathbf{K}_2 = \mathbf{K}^{(d)}[X_{\beta 1}]^{(d)}[X_{\beta 2}]^{(d)}...[X_{\beta j}]^{(d)}$ sont deux extensions construites sur le modèle précédent, les deux extensions "composées"

$$\mathbf{K'} = \mathbf{K}_1[X_{\beta 1}]^{(d)}[X_{\beta 2}]^{(d)}...[X_{\beta j}]^{(d)} \text{ et } \mathbf{K''} = \mathbf{K}_2[X_{\alpha 1}]^{(d)}[X_{\alpha 2}]^{(d)}...[X_{\alpha i}]^{(d)}$$

sont bien définies, par application répétée du lemme. De même, il existe un unique $\mathbf{K}$-homomorphisme croissant de $\mathbf{K'}$ vers $\mathbf{K''}$, et un autre de $\mathbf{K''}$ vers $\mathbf{K'}$, qui par composition ne peuvent donner que l'identité. D'où un isomorphisme canonique de $\mathbf{K'}$ vers $\mathbf{K''}$.

Un élément x de l'extension $\mathbf{K}_1$ devra donc être considéré comme égal (dans $\mathbf{K}^{(d+1)}$) à un élément y de l'extension $\mathbf{K}_2$, si et seulement si x a pour image y par l'isomorphisme

canonique de **K'** vers **K"** . Il faut vérifier que cette relation ("être considéré comme égal à") est bien une relation d'équivalence : la réflexivité et la symétrie sont immédiates. La transitivité s'obtient en considérant les isomorphismes uniques liant des extensions composées obtenues à partir des 3 extensions en cause.

Il est clair que l'on obtient, avec le recollement de toutes les extensions du type initial, une extension (d+1)-close et qu'elle est unique à **K**-isomorphisme croissant unique près. ❑

On notera que l'unicité d'une d-clôture résulte également du théorème 9 .
Il serait intéressant de fournir une preuve plus directe du corollaire suivant du théorème 12 .

Corollaire : Dans tout corps ordonné, les algorithmes de Sturm et de Sturm-Sylvester prescrivent des nombres de racines positifs ou nuls.

Explicitation de l'algorithme sous-jacent, une preuve plus concrète

Examen de la preuve

Si nous examinons les calculs impliqués récursivement dans la preuve "abstraite" donnée au paragraphe précédent, nous voyons que tout élément de la clôture réelle est présenté comme élément $Q(\xi_1,\xi_2,...,\xi_k)$ d'une "extension emboîtée normalisée réellement spécifiée", avec $Q \in \mathbf{K}[X_1,X_2,...,X_k]$: une extension emboîtée réellement spécifiée est définie par un système d'équations emboîtées et une spécification de la racine réelle considérée à chaque étage (dans cette preuve, elle est spécifiée comme unique racine sur un intervalle où P change de signe et où P' est de signe constant).

Le théorème 11 nous dit que, si $d_k = d+1$, l'attribution d'un signe à $Q(\xi_1,\xi_2,...,\xi_k)$ peut être faite par un algorithme où n'interviennent que des calculs dans une d-clôture réelle $\mathbf{L}_{k-1}$ de $\mathbf{K}[\xi_1,\xi_2,...,\xi_{k-1}]$, (la spécification réelle de ξ_k est elle-même explicitée et vérifiable dans $\mathbf{L}_{k-1}$). Le théorème 11 nous dit aussi que, dès qu'une d-clôture réelle existe belle et bien, l'algorithme d'attribution de signes est cohérent (c.-à-d. fournit bien une nouvelle extension ordonnée) et unique. Mais en fait, la d-clôture réelle n'est jamais manipulée en entier (pas plus que **K** lui-même).

Si nous appliquons le théorème 11 à chacun des calculs de signe impliqués dans l'attribution du signe à un polynôme particulier, nous sommes amenés à introduire des systèmes d'équations emboîtées (réellement spécifiées) *plus gros* que $[P_1,P_2,...,P_{k-1}]$ mais où les polynômes qui sont rajoutés (comme par exemple la dérivée de P_k , dont il faut expliciter les racines) sont tous de degré $\leq d$ (en les nouvelles variables introduites). En fait, tout nouveau polynôme introduit par l'algorithme d'attribution de signe est ou bien la dérivée d'un polynôme précédemment introduit, ou bien le reste de la division de 2 polynômes déjà introduits[2].

La récurrence sous-jacente

Ceci nous suggère une recopie plus évidemment algorithmique de la preuve "abstraite" :
- examinons d'abord l'assertion suivante :

---

[2] a) un pseudo-reste ferait aussi bien l'affaire, ce qui évite alors toute division dans les extensions considérées
b) mis à plat, l'algorithme d'attribution de signe dans $\mathbf{K}[\xi_1,\xi_2,...,\xi_k]$ par utilisation récursive du

l'algorithme d'attribution des signes dans $\mathbf{K}[\xi_1,\xi_2,...,\xi_k]$ par utilisation récursive du théorème 11 est cohérent chaque fois que les d_i sont tous $\leq d$ et qu'au plus n d'entre eux sont égaux à d.

Cette phrase n'est pas "autodestructrice" parce que l'algorithme d'attribution des signes du théorème 11 n'implique que des systèmes emboîtés où tous les polynômes sont de degré $\leq d$ et où les seuls polynômes de degré d sont ceux du départ. Néanmoins, nous ne pouvons pas la démontrer directement par le théorème 11 et une récurrence double (sur (d,n) muni du bon ordre lexicographique) parce que, si le dernier polynôme n'est pas de degré d, l'algorithme d'attribution des signes implique des systèmes d'équations emboîtées ayant aussi n polynômes de degré d. Le théorème 12 fait donc appel à une récurrence plus compliquée[3].

– considérons maintenant l'assertion suivante :

l'algorithme d'attribution des signes dans $\mathbf{K}[\xi_1,\xi_2,...,\xi_k]$ par utilisation récursive du théorème 11 est cohérent chaque fois que :
les d_i sont tous $\leq d$,
au plus n_1 d'entre eux sont de degré d,
après le dernier polynôme de degré d, au plus n_2 d'entre eux sont de degré $d-1$,
après le dernier polynôme de degré $d-1$, au plus n_3 d'entre eux sont de degré $d-2$,
etc ...,
après le dernier polynôme de degré 3, au plus n_{d-1} d'entre eux sont de degré 2.

L'ensemble des listes $[d; n_1, n_2, ..., n_{d-1}]$ est muni de l'ordre lexicographique et on peut prouver l'assertion encadrée par récurrence sur ce bon ordre grâce au théorème 11.

Une preuve analogue basée sur l'algorithme IF

Vus les théorèmes 6 et 8 déjà établis pour les corps ordonnés d-clos, l'algorithme IF peut s'appliquer pour tout corps ordonné $\mathbf{K}$ qui possède une extension ordonnée d-close $\mathbf{R}$, à condition que tous les polynômes du système triangulaire d'équations considéré soient de degré $\leq d$. En fait, on peut voir l'algorithme IF comme un algorithme de calcul dans la d-clôture ordonnée de $\mathbf{K}$ et on a l'équivalence suivante :

(1) $\mathbf{K}$ possède une extension ordonnée d-close $\mathbf{R}$
si et seulement si
Pour tout système triangulaire de n équations à coefficients dans $\mathbf{K}$ de degrés $\leq d$, l'algorithme IF est un algorithme cohérent d'attribution de signes dans $\mathbf{K}[X_1,X_2,...,X_k]$ (ceci pour chacune des solutions $(\xi_1,\xi_2,...,\xi_k)$ du système triangulaire, caractérisée à la Thom par l'algorithme IF lui-même)

Si P est un polynôme de degré $d+1$ à coefficients dans un corps d-clos $\mathbf{R}$ nous appellerons *racine réelle de P* toute racine de P telle que définie au théorème 11. Toujours d'après le théorème 11, si Q est un polynôme de $\mathbf{R}[X]$ et α une racine réelle de P, nous pouvons parler sans ambiguïté du signe de $Q(\alpha)$. On obtient alors l'amélioration suivante du théorème 6 et de la proposition 7, avec le même raisonnement qu'à la proposition 7 :

---

[3] et on peut sans doute voir là la vraie raison pour laquelle

(2) On suppose qu'on est dans un corps ordonné d-clos $\mathbf{R}$. Si P est degré $d+1$, l'algorithme de Sturm compte le nombre de racines réelles de P (définition ci-dessus) sur l'intervalle précisé. En outre si $Q \in \mathbf{R}[X]$, l'algorithme de Sturm-Sylvester appliqué à P et Q détermine le nombre de racines réelles de P rendant Q positif et le nombre de racines réelles de P rendant Q négatif (sur l'intervalle précisé).

NB: Pour énoncer et démontrer (2), il n'est pas nécessaire de supposer l'existence d'une extension ordonnée de $\mathbf{K}$ contenant toutes les racines réelles de P (existence qui ne résulte pas de manière immédiate du théorème 11).

D'après le théorème 11 et (2), on obtient ensuite le résultat suivant :

(3) Si le corps ordonné $\mathbf{K}$ possède une d-clôture ordonnée et si on a un système d'équations emboîtées spécifiées à la Thom, toutes de degré $\leq d$ sauf la dernière de degré $d+1$, alors l'algorithme IF appliqué à ce système est un algorithme cohérent d'affectations de signes.

Notons bien ici ce qu'on entend par cohérence de l'algorithme IF, c'est d'une part, qu'il aboutit bien à un résultat, d'autre part qu'il est alors un algorithme cohérent d'attribution de signes, au sens où nous l'avons défini dans les préliminaires. Pour que l'algorithme IF aboutisse bien à un résultat, il faut, par exemple entre autres choses, que l'algorithme de Sturm-Sylvester aboutisse toujours à un nombre ≥ 0 de racines de P rendant $Q > 0$.
On déduit du (3):

(4) Si *tout* corps ordonné $\mathbf{K}$ possède une d-clôture ordonnée, alors pour *tout* système d'équations emboîtées spécifiées à la Thom dans un corps ordonné, toutes de degré $\leq d+1$, l'algorithme IF appliqué à ce système est un algorithme cohérent d'affectations de signes.

En effet, on peut faire une récurrence sur le nombre n d'équations de degré $d+1$ intervenant dans le système. Supposons la cohérence jusqu'à n. Fixons les m premières équations, parmi lesquelles n équations de degré $d+1$. Soit $\mathbf{L}$ l'extension de $\mathbf{K}$ qui correspond à ces m premières équations. Par hypothèse $\mathbf{L}$ possède une d-clôture. On peut donc autoriser après la $m^{\text{ème}}$ équation des équations de degré $\leq d$: les affectations de signe par l'algorithme IF sont cohérentes et construisent la d-clôture de $\mathbf{L}$. D'après le résultat (3) on peut donc introduire en position $m+1$ une $(n+1)^{\text{ème}}$ équation de degré $d+1$ et l'algorithme IF sera cohérent. Il correspond donc à ces $m+1$ équations une extension ordonnée $\mathbf{M}$. Et comme tout corps ordonné possède une d-clôture, on peut de nouveau rajouter des équations de degré $\leq d$ en nombre arbitraire après la $(m+1)^{\text{ème}}$. On obtient ainsi un système arbitraire avec $n+1$ équations de degré $d+1$.
Enfin, on déduit de (4), vu (1):

(5) Si *tout* corps ordonné $\mathbf{K}$ possède une d-clôture ordonnée, alors *tout* corps ordonné $\mathbf{K}$ possède une $(d+1)$-clôture ordonnée.

Puis par récurrence sur d, vu (5):

(6) Tout corps ordonné $\mathbf{K}$ possède une clôture réelle.

4) Théorie constructive des corps réels clos

L'algorithme de Hörmander

Soit $L = [P_1, P_2, ..., P_k]$ une liste de polynômes de $\mathbf{K}[X]$, où $\mathbf{K}$ est un sous-corps d'un corps réel clos $\mathbf{R}$. On dit qu'on a dressé le tableau complet des signes de la liste L lorsqu'on a calculé toutes les racines des P_i dans $\mathbf{R}$, qu'on les a rangées par ordre croissant, et qu'on a déterminé le signe de chacun des polynômes, en chacun des points et sur chacun des intervalles.

Théorème 13 :

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 polynômes de $\mathbf{K}[X]$.

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

1) $\mathcal{P}$ est finie.

2) On peut établir le tableau complet des signes pour $\mathcal{P}$ en utilisant les seules informations suivantes : le degré de chaque polynôme de la famille; les diagrammes des opérations $P \longmapsto P'$, et $(P,Q) \longmapsto \mathbf{Rst}(P,Q)$ (où $\deg(P) \geqslant \deg(Q)$) dans $\mathcal{P}$; et les signes des constantes de $\mathcal{P}$[4].

preuve> 1) A priori, pour construire $\mathcal{P}$ on prend la liste L et on applique systématiquement l'opération "reste de tous les couples de polynômes 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 $\mathcal{P}_n$ la sous-famille de $\mathcal{P}$ constituée des polynômes numérotés de 1 à n. Elle est évidemment stable par les opérations 'dérivation' et 'reste de division', qui abaissent le degré. Notons enfin $\mathcal{T}_n$ le tableau de Hörmander correspondant.

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

Supposons vrai jusqu'à n. Soit P le polynôme de numéro $n+1$ dans $\mathcal{P}$. Sur chacun des intervalles du tableau $\mathcal{T}_n$, le polynôme P est strictement monotone, d'après le théorème des accroissements finis. Chacun des points ξ du tableau $\mathcal{T}_n$ est ou bien $+\infty$, ou bien $-\infty$, ou bien une racine d'un certain polynôme Q de numéro $\leq n$, et dans ce cas, si $R = \mathbf{Rst}(P,Q)$, on a $P(\xi) = R(\xi)$. Le signe de $P(\xi)$ est donc connu dans tous les cas à partir des informations autorisées. On en déduit sur quels intervalles ouverts de $\mathcal{T}_n$ le polynôme P reste de signe constant, en quels points déjà introduits s'annule P et sur quels intervalles

---

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

ouverts de $\mathcal{T}_n$ sont les racines de P dans **R** qui ne figuraient pas encore dans $\mathcal{T}_n$. Soit ζ une racine de P sur l'un de ces intervalles ouverts $I =]\xi,\xi'[$. Si Q est un polynôme de numéro $\leq n$ dans $\mathcal{P}$, son signe sur I est connu donc aussi en ζ ,sur $]\xi,\zeta[$ et sur $]\zeta,\xi'[$. Quant à P ,son signe sur $]\xi,\zeta[$ et celui sur $]\zeta,\xi'[$ sont également connus . On a donc construit le tableau complet des signes pour $\mathcal{P}_{n+1}$ à partir des informations autorisées et du tableau complet des signes pour $\mathcal{P}_n$. ❑

On notera que les intervalles ouverts minimaux du *tableau de Hörmander* (défini dans la preuve précédente) sont tous spécifiés à la Thom dans **K** à partir d'un ou de deux polynômes de $\mathcal{P}$, et les points du tableau de Hörmander sont également spécifiés à la Thom.

Le principe de Tarski-Seidenberg

Théorème 14 :

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

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

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

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

Théorème 15 : (principe de Tarski-Seidenberg)

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

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

$\tau = [\tau_1 ,\tau_2 , ..., \tau_k] \in \{ < , \leqslant , = , \geqslant , > \}^k$

On peut construire une famille finie $\mathcal{F}$ de polynômes de $\mathbf{K}[U_1, U_2, ..., U_n]$ et une partie finie $\mathcal{B}$ de $\{ -1 , 0 , +1 \}^{\mathcal{F}}$ telles que, pour tout $u_1, u_2, ..., u_n$ dans **K** , en posant $P_i(X) = Q_i(u_1, u_2, ..., u_n;X)$, on ait :

$[\exists \xi \in \mathbf{R} : P_1(\xi)\ \tau_1\ 0$ et .... et $P_k(\xi)\ \tau_k\ 0\ ] \iff (\mathrm{Sign}(S(u_1, u_2, ..., u_n))_{S \in \mathcal{F}} \in \mathcal{B}$

preuve> On raisonne comme au théorème précédent, la famille $\mathcal{F}$ étant définie de la même manière. On établit tous les tableaux de Hörmander possibles , selon les familles $\mathcal{P}$ et selon les signes attribués aux constantes de la famille $\mathcal{P}$ choisie. Il ne reste plus qu'à sélectionner les tableaux de Hörmander pour lesquels $\exists \xi \in \mathbf{R}\ P_1(\xi) \equiv \sigma_1$ et .... et $P_k(\xi) \equiv \sigma_k$, et cela fournit la partie $\mathcal{B}$ cherchée. ❑

Théories formelles des corps réels clos discrets, intuitionniste et classique

Il n'est pas difficile de reproduire les preuves précédentes dans le cadre de la théorie formelle intuitionniste des corps réels clos discrets. On n'utilise pas le principe du tiers exclus général, mais on a un tiers exclu restreint donné par l'axiome:

$$\forall x \quad x>0 \text{ ou } x=0 \text{ ou } x<0$$

qui traduit le caractère discret de l'ordre considéré.
Par ailleurs, on peut admettre pour constantes de la théorie formelle les éléments d'un corps ordonné discret donné $\mathbf{K}$, avec les axiomes correspondants qui explicitent la structure de corps ordonné sur les constantes. Alors toute formule sans quantificateur F vérifie le tiers exclu (" $F \vee \neg F$ " est un théorème de la théorie formelle intuitionniste).
On ne peut pas dans ce cadre ramener d'emblée tout formule à sa forme prénexe. Néanmoins, comme toute formule sans quantificateur vérifie le tiers exclu, et comme le principe de Tarski-Seidenberg montre le principe d'élimination du quantificateur $\exists$ placé devant une formule sans quantificateur, on en déduit qu'on peut éliminer les quantificateurs même dans une formule non prénexe, donc que la théorie est complète, et donc qu'elle possède les mêmes théorèmes que la théorie classique correspondante. L'existence d'un modèle (la clôture réelle de $\mathbf{K}$) fournit une preuve constructive de la cohérence de la théorie formelle considérée. Il semble que ce soit la première preuve constructive du résultat. En résumé, tant qu'il ne s'agit que d'énoncés du premier ordre, on peut utiliser la logique classique dans un corps réels clos discret.
Notons également qu'une preuve directe ("purement métamathématique") de la cohérence et de la complétude de la théorie formelle intuitionniste considérée ne fournirait pas pour autant une méthode pour construire la clôture réelle de $\mathbf{K}$, comme le montre l'exemple de la théorie des corps algébriquement clos discrets. (le "théorème de complétude" n'est pas valable constructivement; par contre la cohérence de la théorie formelle avec constantes dans $\mathbf{K}$ est assurée dès que tout sous-corps dénombrable de $\mathbf{K}$ possède une clôture algébrique).

Théorème 16 :

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

Bibliographie :

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

[BKR] Ben-Or M., Kozen D., Reif J. : The complexity of elementary algebra and geometry. J. of Computation and Systems Sciences 32. 251-264 (1986).

[Bou] Boughattas S. : L'arithmétique ouverte et ses modèles non standards. Thèse, Université de Paris VI. 1987.

[CR] Coste M., Roy M.-F. :Thom's lemma, the coding of real algebraic numbers and the computation of the topology of semi-algebraic sets. J. Symbolic Computation 5 , 121-129 (1988).

[GLRR] Gonzalez L., Lombardi H., Recio T., Roy M.-F. : Spécialisation de la suite de Sturm et sous-résultants. Version détaillée, dans CALSYF journées du GRECO de Calcul Formel 1989.

[Kl] S. C. Kleene. :Introduction to Metamathematics (Van Nostrand; 1952)

[Ho] Hollkott A. :Finite Konstruktion geordneter algebraischer Erweiterungen von geordneten Grundkörpen. Dissertation.Hamburg, 1941, pp.1-65.

[MN] Metakides G., Nerode A. : Effective content of field theory. Annals of Math. Logic 17, p 289-320, 1979.

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

[Sa] T. Sander. Existence and uniqueness of the real closure of an ordered field. A paraître dans le Journal of Pure and Applied Algebra.

[Za] H. Zassenhaus . A real root calculus. pp. 383-392 in: Computational aspects in abstract algebra. Proceedings of a conference held at Oxford: 29th. August - 2nd September 1967. Ed. John Leech. Pergamon Press.

Théorème des zéros réel effectif et variantes (avec une majoration explicite des degrés)

THEOREME DES ZEROS REEL 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 $\mathbf{K}$, 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 $\mathbf{K}$, 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 $\mathbf{K}$, 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 $\mathbf{K}$ ", 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.

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 $\mathbf{K}$ lorsqu'on dispose d'un test pour le signe d'un élément de $\mathbf{K}$.

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

nous notons F^{*2} l'ensemble des carrés d'éléments de F .

le *monoïde multiplicatif engendré* par F est l'ensemble des produits d'éléments de $F \cup \{1\}$, nous le noterons $\mathcal{M}(F)$, et $\mathcal{M}_2(F) := \mathcal{M}(F^{*2})$. Nous noterons $\mathcal{M}_1(F)$ la partie de $\mathcal{M}(F)$ formée des produits où chaque élément intervient au plus une fois.

le *cône positif engendré* par F est l'ensemble des sommes d'éléments du type $p.P.Q^2$ où p est positif dans $\mathbf{K}$, P est dans $\mathcal{M}(F)$, Q est dans $\mathbf{K}[\mathbf{X}]$. Nous le noterons $Cp(F)$[1] . On remarque que dans la définition, on pourrait supposer que P est dans $\mathcal{M}_1(F)$, ce qu'on fera désormais.

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

Définition 1 : Etant donnés 4 parties finies de $\mathbf{K}[\mathbf{X}]$: $F_>$, $F_\geq$, $F_=$, $F_\neq$, contenant des polynômes auxquels on souhaite imposer respectivement les conditions de signes >0 ,

---

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

$\geqslant 0$, $= 0$, $\neq 0$, on dira que $\mathbf{F} = [F_> ; F_\geq ; F_= ; F_\neq]$ est *fortement incompatible* dans $\mathbf{K}$[1] si on a une égalité dans $\mathbf{K}[\mathbf{X}]$ du type suivant :

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

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

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

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

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

Si on considère la clôture réelle $\mathbf{R}$ de $\mathbf{K}$, 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 " $P = 0$, $-Q \geqslant 0$ est impossible". Nous parlerons donc de manière indifférente d'incompatibilité forte, d'implication forte, ou d'évidence forte. En nous ramenant toujours implicitement à une incompatibilité forte.

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

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

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

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

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 $\mathbf{K}$ un corps ordonné et $\mathbf{R}$ une extension réelle close de $\mathbf{K}$. Les trois faits suivants, concernant un système de csg portant sur des polynômes de $\mathbf{K}[\mathbf{X}]$, sont équivalents :

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

l'impossibilité dans $\mathbf{R}$

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

---

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

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 $\mathbf{K}$ un corps ordonné et $\mathbf{R}$ une extension réelle close de $\mathbf{K}$. Soit A l'ensemble semi algebrique dans $\mathbf{R}^n$ defini par :

$A = \{\mathbf{x} \in \mathbf{R}^n : S_1(\mathbf{x}) > 0,...,S_i(\mathbf{x}) > 0,\ P_1(\mathbf{x}) \geqslant 0,...,P_j(\mathbf{x}) \geqslant 0,\ Z_1(\mathbf{x}) = 0,...,Z_k(\mathbf{x}) = 0,$
$N_1(\mathbf{x}) \neq 0,...,N_h(\mathbf{x}) \neq 0\ \}$

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 $\mathbf{K}[\mathbf{X}]$: $Cp(S_1,...,S_i, P_1,...,P_j)$

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

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

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.

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

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 :

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

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

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" : $\vdash_{cons}$

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

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

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

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

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 **K[X]** , Q un élément de **K[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 : ${}^*(\ \mathbb{H} \Rightarrow Q > 0\ )^* \vdash_{cons} {}^*(\ \mathbb{H} \Rightarrow Q \geqslant 0\ )^*$

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

$$[\ {}^*(\ \mathbb{H} \Rightarrow Q \leqslant 0\ )^*\ \text{et}\ {}^*(\mathbb{H} \Rightarrow Q \geqslant 0)^*\ ] \vdash_{cons} {}^*(\ \mathbb{H} \Rightarrow Q = 0\ )^*.$$

De même :

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

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

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 , $\geqslant 0$, $=0$, $\neq 0$ dans l'hypothèse $\mathbb{H}$
L'hypothèse $^*(\mathbb{H} \Rightarrow Q \leqslant 0)^*$ se réécrit $^*([\mathbb{H}, Q>0] \Rightarrow 1=0)^*$ et signifie qu'on a une égalité :
$S + P + Z = 0$ avec $S \in \mathcal{M}(F_>^{*2} \cup F_\neq^{*2} \cup \{Q^2\})$, $P \in Cp(F_\geq \cup F_> \cup \{Q\})$, $Z \in I(F_=)$
c.-à-d. encore :

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

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

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

On récrit les 2 égalités obtenues sous forme :

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

d'où $-Q^2.P_1.P_2 = Q^{2n+2m}.S_1.S_2 + [Q^{2n}.S_1.R_2 + Q^{2m}.S_2.R_1 + R_1.R_2] + W$ où $W \in I(F_=)$
d'où $Q^{2n+2m}.S_1.S_2 + V + W = 0$ avec :
$S_1.S_2 \in \mathcal{M}(F_>^{*2} \cup F_\neq^{*2})$, $V \in Cp(F_\geq \cup F_>)$, $W \in I(F_=)$
ce qui est précisément l'implication forte cherchée : $^*(\mathbb{H} \Rightarrow Q=0)^*$.

Voyons maintenant la construction:

$$[^*(\mathbb{H} \Rightarrow Q \leqslant 0)^* \text{ et } ^*(\mathbb{H} \Rightarrow Q \neq 0)^*] \underset{cons}{\vdash} ^*(\mathbb{H} \Rightarrow Q<0)^*$$

L'implication forte $^*(\mathbb{H} \Rightarrow Q \leqslant 0)^*$ correspond à une équation :
$Q^{2m}.S_1 + Q.P_1 + R_1 + Z_1 = 0$ avec $S_1 \in \mathcal{M}(F_>^{*2} \cup F_\neq^{*2})$, $P_1, R_1 \in Cp(F_\geq \cup F_>)$, $Z_1 \in I(F_=)$
L'implication forte $^*(\mathbb{H} \Rightarrow Q \neq 0)^*$ correspond à une équation :
$S_3 + P_3 + Q.Y_3 + Z_3 = 0$ avec $S_3 \in \mathcal{M}(F_>^{*2} \cup F_\neq^{*2})$, $P_3 \in Cp(F_\geq \cup F_>)$, $Z_3 \in I(F_=)$
équation qu'on réécrit $-Q.Y_3 = S_3 + P_3 + Z_3$
En élevant cette égalité à la puissance 2m on obtient $Q^{2m}.(Y_4)^2 = S_4 + P_4 + Z_4$ avec de nouveau $S_4 \in \mathcal{M}(F_>^{*2} \cup F_\neq^{*2})$, $P_4 \in Cp(F_\geq \cup F_>)$, $Z_4 \in I(F_=)$
On multiplie la première équation par $(Y_4)^2$ et la dernière par S_1 et on conclut :

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

$S_1.S_4 \in \mathcal{M}(F_>^{*2} \cup F_\neq^{*2})$, $P_1.(Y_4)^2$, $S_1.P_4 + R_1.(Y_4)^2 \in Cp(F_\geq \cup F_>)$,
$S_1.Z_4 + Z_1.(Y_4)^2 \in I(F_=)$, ce qui est bien l'implication forte cherchée : $^*(\mathbb{H} \Rightarrow Q<0)^*$

Voyons enfin la construction:

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

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: $[\ {}^*(\ \mathbb{H} \Rightarrow \mathbb{H}'\ )^*$ et ${}^*(\ [\ \mathbb{H}\ ,\ \mathbb{H}'] \Rightarrow \mathbb{H}''\ )^*\ ]\ \underset{cons}{\vdash}\ {}^*(\ \mathbb{H} \Rightarrow \mathbb{H}''\ )^*$

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

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

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) : ${}^*(\ \mathbb{H} \Rightarrow [\ P.Q > 0\ ,\ Q \geqslant 0\ ]\ )^*\ \underset{cons}{\vdash}\ {}^*(\ \mathbb{H} \Rightarrow P > 0\ )^*$

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

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

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

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

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

Supposons maintenant que U et V "attribuent un même signe strict" σ à P' , et un même signe strict σ'' à P'' . Alors, chaque fois qu'on attribue un signe à Δ et à $P^{(3)}$, l'une des 4 formules de Taylor mixtes constitue une évidence forte que $P(U) - P(V)$ et $\Delta.\sigma$ ont le même

---

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

signe. Par exemple, si $\sigma = +1$, $\sigma'' = -1$ et si $\Delta > 0$, $P^{(3)} < 0$, la troisième formule de Taylor mixte peut se relire :

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

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

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

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

Comme toutes les combinaisons de signes possibles se présentent, on obtient : si U et V 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.

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 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:

---

1 Même preuve, en vérifiant pour U^4 .

$P(U) - P(V) = \gamma_1 \Delta P'(U) - \Delta^2 \sum_{i,j} r_{i,j} P''(U_{i,j})$ avec γ_1 et les $r_{i,j}$ 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:

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

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

Théorème 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 : $P^{(s)}(\mathbf{X},T) > 0$, $P^{(i)}(\mathbf{X},T) \geqslant 0$, i = 1, ..., s–1 .

On a alors les évidences fortes suivantes :

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

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

$^*([\mathbb{H}(U), \mathbb{H}(V), P^{(i)}(Z)\ \sigma_i\ 0] \Rightarrow (Z-U).(Z-V) > 0)^*$ (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 $\mathbf{R}$ codé à la Thom dans $\mathbf{K}$ et v un élément de $\mathbf{K}$.

Un exemple : Considérons le polynôme générique de degré 4

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

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

On écrit les formules de Taylor mixtes suivantes :

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

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

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

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

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 :

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

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

Nous dirons que *les hypothèses* $\mathbb{H}_1$ *autorisent l'existence des* T_i *vérifiant* $\mathbb{H}_2$ lorsque, pour tout système de csg $\mathbb{H}$ portant sur des polynômes de $\mathbf{K[X,Y]}$[1] , on a la construction d'implication forte :

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

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 :

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

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 $\mathbf{L}$ est une extension ordonnée de $\mathbf{K}$ il n'y a pas de relation évidente a priori entre un énoncé $^*(\mathbb{H}_1(\mathbf{X}) \Rightarrow \exists\, \mathbf{T}\ \mathbb{H}_2(\mathbf{X},\mathbf{T}))^*$ lu dans $\mathbf{K}$ et le même énoncé lu dans $\mathbf{L}$. En fait, une fois démonté le théorème des zéros réels, il est clair que les deux énoncés sont équivalents à l'énoncé $\forall\, \mathbf{x}\ (\mathbb{H}_1(\mathbf{x}) \Rightarrow \exists\, \mathbf{t}\ \mathbb{H}_2(\mathbf{x},\mathbf{t}))$ lu dans la clôture ordonnée de $\mathbf{K}$.

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 :

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

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

---

[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

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

Quelques règles de manipulation des énoncés d'existence potentielle

Des règles que nous allons énoncer, seule la règle de substitution n'est pas immédiate. Elles s'avèrent toutes bien utiles pour simplifier l'exposé.
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 $^*(H_1(X) \Rightarrow \exists\, T \;\; H_2(X,T))^*$ reste vraie si on affaiblit la conclusion, si on renforce l'hypothèse, ou si on supprime derrière $\exists$ des variables ne figurant pas dans $H_2(X,T)$.

Proposition 13 : (renforcement simultané de l'hypothèse et de la conclusion)
Si $^*(H_1(X) \Rightarrow \exists\, T \;\; H_2(X,T))^*$ **alors**
$$^*([\, H_1(X) , H_3(X) \,] \Rightarrow \exists\, T \, [\, H_2(X,T) , H_3(X) \,])^*$$
(rappel de l'hypothèse dans la conclusion)
Si $^*(H_1(X) \Rightarrow \exists\, T \;\; H_2(X,T))^*$ **alors** $^*(H_1(X) \Rightarrow \exists\, T \, [\, H_2(X,T) , H_1(X) \,])^*$

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

Proposition 14 : (existence potentielle comme généralisation de l'implication forte)
Supposons que les systèmes de csg H_1 et H_2 portent sur les seules variables X .
Alors $^*(H_1(X) \Rightarrow \exists\, T \;\; H_2(X))^*$ **si et seulement si** $^*(H_1(X) \Rightarrow H_2(X))^*$.

preuve> Voyons le seulement si: soit $Q\,\tau\,0$ une csg dans H_2 et soit $Q\,\tau'\,0$ la csg opposée. On a $^*([\, H_2(X), Q\,\tau'\,0 \,] \Rightarrow 1 = 0)^*$. Donc, par l'existence potentielle, on a également $^*([\, H_1(X), Q\,\tau'\,0 \,] \Rightarrow 1 = 0)^*$, c.-à-d. $^*(H_1(X) \Rightarrow Q\,\tau\,0)^*$.
Voyons l'implication dans l'autre sens. Soit $H(X,Y)$ un système de csg et supposons que $^*([\, H_2(X), H(X,Y) \,] \Rightarrow 1 = 0)^*$. D'après l'hypothèse, on a évidemment :
$^*([\, H_1(X), H(X,Y) \,] \Rightarrow [\, H_2(X), H(X,Y) \,])^*$. Il suffit d'appliquer la transitivité des implications fortes pour obtenir $^*([\, H_1(X) , H(X,Y) \,] \Rightarrow 1 = 0)^*$. ❑

Proposition 15 : (raisonnement cas par cas)
Soit Q un polynôme de $\mathbf{K}[X]$. Pour démontrer une existence potentielle $^*(H_1(X) \Rightarrow \exists\, T \;\; H_2(X,T))^*$ il suffit de démontrer chacune des existences potentielles $^*([\, H_1(X) , Q\,\sigma\,0 \,] \Rightarrow \exists\, T \;\; H_2(X,T))^*$ 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 $H_1(X)$, $H_2(X,T)$ et $H_3(X,T,U)$.
Si on a
$^*(H_1(X) \Rightarrow \exists\, T \;\; H_2(X,T))^*$ et $^*([\, H_1(X), H_2(X,T)] \Rightarrow \exists\, U \;\; H_3(X,T,U))^*$

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

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

On veut construire

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

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 :

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

Par définition de l'existence potentielle on sait construire:

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

Par ailleurs :

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

Par transitivité (5) et (6) donnent :

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

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

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

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

Existences potentielles fondamentales

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

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

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

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

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

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

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

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

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

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

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

Ceci est exactement une implication forte du type voulu. ❑

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

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

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

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

L'hypothèse correspond à une équation :

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

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 :

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

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

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

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

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

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

preuve> $^*(U \geqslant 0 \Rightarrow \exists Z \quad U = Z^2)^*$ d'après le théorème 19 .

Par ailleurs $^*([U>0, U=Z^2] \Rightarrow Z \neq 0)^*$ donc par transitivité :

$^*(U>0 \Rightarrow \exists Z \quad [U=Z^2, Z \neq 0])^*$

Par ailleurs $^*(Z \neq 0 \Rightarrow \exists T \quad 1 = Z.T)^*$ d'après le théorème 20, donc

par transitivité : $^*(U>0 \Rightarrow \exists Z,T \quad [U=Z^2, Z \neq 0, \ 1=Z.T])^*$

Enfin $^*([U=Z^2, \ 1=Z.T] \Rightarrow 1 = U.T^2)^*$ donc par transitivité :

$^*(U>0 \Rightarrow \exists Z,T \quad [U=Z^2, Z \neq 0, \ 1=Z.T, 1=U.T^2])^*$

et a fortiori $^*(U>0 \Rightarrow \exists T \quad 1 = U.T^2)^*$ $\square$

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

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

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

$^*(U>0 \Rightarrow \exists T\ 1=U.T^2)^*$ 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) : $^*(P(U).P(V)\lessdot 0 \Rightarrow \exists Z\ P(Z)=0)^*$

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:

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

qui peut se relire :

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

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

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

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

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

On déduit par substitution:

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

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

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

Enfin, on a trivialement:

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

On conclut par transitivité des implications fortes.

Voyons maintenant le cas où P n'est pas unitaire.
Soit C(X) son coefficient dominant en Z .
Soit $R(X,Z) = P(X,Z) - C(X).Z^s$. (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 : $C(X)=0$

---

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

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

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

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

et par hypothèse de récurrence, on a:

$$^*(R(X,U).R(X,V) \leqslant 0 \Rightarrow \exists Z\ R(X,Z) = 0)^*$$

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

on conclut par transitivité.

2ème cas : $C(X) \neq 0$.

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

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

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

et donc:

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

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

$$^*(P_1(X,T,U).P_1(X,T,V) \leqslant 0 \Rightarrow \exists Z\ P_1(X,T,Z) = 0)^*$$

Par transitivité :

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

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

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(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:

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

Nous allons démontrer 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 $(Z - U).(Z - V) < 0$.

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

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

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

$$R(X,Z,T) := (P(X,T) - P(X,Z)) / (T - Z) \ .$$

Notons pour alléger R(T) pour R(**X**,Z,T) et P(T) pour P(**X**,T) .
Notons $\mathbb{H}_1(\mathbf{X},Z)$ pour $[\, P(U).P(V) < 0\ ,\ P(Z) = 0\ ,\ (Z-U).(Z-V) \geqslant 0\,]$.
(c'est l'hypothèse de l'existence potentielle que nous voulons démontrer)
On a facilement l'implication forte:

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

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

et donc aussi

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

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

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

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

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

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

1) $\mathcal{P}$ est finie.

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

preuve> 1) A priori, pour construire $\mathcal{P}$ on prend la liste L et on applique systématiquement l'opération "reste de tous les couples de polynômes 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 $\mathcal{P}_m$ la sous-famille de $\mathcal{P}$ 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 $\mathcal{T}_m$ 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 $\mathcal{P}_m$, 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 $\mathcal{P}$. Sur chacun des intervalles du tableau $\mathcal{T}_m$, le polynôme P est strictement monotone, d'après le théorème des accroissements finis. Chacun des points ξ du tableau $\mathcal{T}_m$ 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 $R = \mathbf{Rst}(P,Q)$, on a $P(\xi) = R(\xi)$. Le signe de $P(\xi)$ est donc connu dans tous les cas à partir des informations autorisées. On en déduit sur quels intervalles ouverts de $\mathcal{T}_m$ le polynôme P reste de signe constant, en quels points déjà introduits s'annule P et sur quels intervalles ouverts de $\mathcal{T}_m$ sont les racines de P dans $\mathbf{R}$ qui ne figuraient pas encore dans $\mathcal{T}_m$. Soit ζ

---

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

une racine de P sur l'un de ces intervalles ouverts $I =]\xi,\xi'[$. Si Q est un polynôme de numéro $\leq m$ dans $\mathcal{P}$, son signe sur I est connu donc aussi en ζ ,sur $]\xi,\zeta[$ et sur $]\zeta,\xi'[$. Quant à P , son signe sur $]\xi,\zeta[$ et celui sur $]\zeta,\xi'[$ sont également connus . On a donc construit le tableau complet des signes pour $\mathcal{P}_{m+1}$ à partir des informations autorisées et du tableau complet des signes pour $\mathcal{P}_m$. ❑

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 $P'(\xi)$, $P''(\xi)$, etc...

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

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

NB : Tout point de **R** peut être codé à la Thom dans **K** . Mais des intervalles ouverts de **R** peuvent ne pas être codables à la Thom dans **K** . L'important est que les intervalles ouverts minimaux des tableaux de 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 $\mathcal{P}$ une famille de polynômes de **K**[X] et $\mathbb{H}(X)$ un système de csg portant sur des éléments de $\mathcal{P}$. Alors :

ou bien $\mathbb{H}(x)$ est impossible dans **R** et alors $^*(\mathbb{H}(X) \Rightarrow 1 = 0)^*$ 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 $\mathcal{P}$ est stable par les opérations "reste" et "dérivation". (proposition 23).

L'impossibilité de $\mathbb{H}(x)$ dans **R** ou l'existence de x dans **R** vérifiant $\mathbb{H}(x)$ est directement lisible sur le tableau de 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] Pour chacun de ces signes est strict s'il est et le seul

Lorsque le corps K est réel clos

preuve du théorème dans ce cas > On a donc $\mathbf{R} = \mathbf{K}$. Soient $\upsilon_1, \upsilon_2, ..., \upsilon_k$ la liste ordonnée des points finis du tableau de Hörmander de la famille $\mathcal{P}$. On peut calculer υ_0 et υ_{k+1} dans $\mathbf{R}$ tels que l'évidence forte des signes de tous les $P \in \mathcal{P}$ soit facile à établir en $x \lessdot \upsilon_0$ et en $x \gtrdot \upsilon_{k+1}$.
La possibilité dans $\mathbf{R}$ pour un système de csg donné est immédiatement lisible et explicitable, soit en un υ_i , soit en un $x = (\upsilon_i + \upsilon_{i+1})/2$. Cela implique l'existence potentielle.
L'incompatibilité dans $\mathbf{R}$ pour une système $\mathbb{H}$ de csg est également lisible sur le tableau de 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 $\mathbf{R}$ (puisque $\upsilon_i \in \mathbf{R}$). Sur un intervalle $]\upsilon_i , \upsilon_{i+1}[$, les signes, constants et non nuls, des $P \in \mathcal{P}$ sont tous fortement évidents à partir des signes aux bords modulo une formule de Taylor mixte convenable (cf. théorème 10 (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 $\mathbf{K}$.
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 $\mathbf{K}$, au delà desquels les signes des polynômes de $\mathcal{P}$ sont fortement évidents. Ces 2 éléments de $\mathbf{K}$ remplaceront pour nous $-\infty$ et $+\infty$ dans le tableau de Hörmander.

Lemme 26 : (évidence forte et existence potentielle pour les faits élémentaires lisibles sur un tableau de Hörmander)
Soit $\mathbf{K}$ un corps ordonné et $\mathbf{R}$ sa clôture réelle. Soit $\mathcal{P}$ une famille de polynômes de $\mathbf{K}[X]$ stable par les opérations "reste" et "dérivation", soit $\mathcal{T}$ son tableau de 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 $\mathcal{P}_m$ et le tableau $\mathcal{T}_m$, par récurrence sur m. En suivant pas à pas la preuve de la proposition 23. Le lemme est évident lorsque la famille $\mathcal{P}_m$ ne contient que des constantes.

Passons de m à m+1. Si λ est un point de $\mathcal{T}_m$, 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 $\mathbf{R}$ 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 $\mathcal{T}$, 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 $\mathcal{T}_m$ est fortement évident à partir du signe de $\mathbf{Rst}(P,Q_\lambda)(\lambda)$ et du fait que $Q_\lambda(\lambda)=0$; donc aussi, d'après l'hypothèse de récurrence (3), à partir de $\mathbb{H}_\lambda(\lambda)$. Soit ζ une racine de P située sur l'intervalle ouvert minimal $]\alpha,\beta[$ de $\mathcal{T}_m$. 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 $\lessdot$ ou $\gtrdot$ associé à τ_i.

On a les implications fortes:

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

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

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 $\mathcal{T}_{m+1}$ se déduit alors du point 2) pour $\mathcal{T}_m$: si par exemple $\lambda \in \mathcal{T}_m$ 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 $\mathcal{T}_m$ est fortement évident à partir du codage à la Thom de λ. Il reste à voir que le signe de $Q \in \mathcal{P}_m$ 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 :

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

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

on obtient le résultat voulu :

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

Voyons le point 4) Notons $\mathbb{H}_{\lambda,\mu}(X)$ le codage à la Thom d'un intervalle ouvert minimal de $\mathcal{T}_{m+1}$. 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 $\mathcal{P}_{m+1}$ 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 $\mathcal{P}$. Vu le lemme 26, nous pouvons recopier, avec les précautions d'usage, ce que nous avons fait dans le cas d'un corps réel clos. La disjonction des cas va pouvoir être pratiquée grâce à (2). L'évaluation du signe d'un polynôme en un point du tableau sera remplacée par l'évidence forte du signe de ce polynôme etc... ❑

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 $\mathbf{K}$. 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

---

[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 $\mathcal{T}_{n+1}$ respectent le théorème des accroissements finis sans faire appel à ce théorème, donc sans faire appel non plus à l'existence d'une clôture réelle de $\mathbf{K}$.

contenant les racines marquées dans le tableau, cela se déduit au contraire des formules de Taylor mixtes.

Sans supposer savoir déjà l'existence d'une clôture réelle de $\mathbf{K}$, les preuves données jusqu'ici montrent donc que :

Si P est un polynôme de $\mathbf{K}[X]$, 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 $\mathbf{K}$, ou bien on a l'existence potentielle d'un X vérifiant $\mathbb{H}$ (lue dans $\mathbf{K}$) .

Dans ce dernier cas, si Q est un polynôme de $\mathbf{K}[X]$, 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 $\mathbf{K}[X]$.

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 $\mathbf{K}$ 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 $\mathbf{K}$.

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 $\mathbf{K}$ 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 $\mathbf{K}$ 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 peut construire une famille finie $\mathcal{F}$ de polynômes de $\mathbf{K}[X_1, X_2, ..., X_n]$ telle que, pour tous $x_1, x_2, ..., x_n$ dans $\mathbf{R}$, 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 $S \in \mathcal{F}$.

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 $\mathcal{P}$ est "uniforme" à ceci près que le calcul d'un reste $\mathbf{Rst}(P,Q)$ 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 $\mathcal{F}$ tous les polynômes apparaissant au numérateur ou dénominateur d'un coefficient d'un polynôme de la famille $\mathcal{P}$, pour toutes les familles $\mathcal{P}$ possibles . ❑

Nous sommes maintenant en mesure de démontrer le :

Théorème 28 : (Tableau de 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 $\mathcal{F}$ 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 $\Sigma = (\sigma_S)_{S \in \mathcal{F}}$ de $\{-1 , 0 , +1\}^{\mathcal{F}}$. On note $\mathbb{H}_\Sigma(X_1,X_2,...,X_n)$ le système de conditions de signes $[S(X_1,X_2,...,X_n) \equiv \sigma_S ; S \in \mathcal{F}]$. 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 $\forall\, x_1,x_2,...,x_n \in \mathbf{R}$ $(\mathbb{H}_\Sigma(x_1,x_2,...,x_n) \Rightarrow \exists\, y \in \mathbf{R}\ \mathbb{H}(x_1,x_2,...,x_n,y))$
et alors : $^*(\mathbb{H}_\Sigma(X_1,X_2,...,X_n) \Rightarrow \exists\, Y\ \mathbb{H}(X_1,X_2,...,X_n,Y))^*$ (lu dans **K**)
ou bien $\forall\, x_1,x_2,...,x_n,y \in \mathbf{R}$ $(\mathbb{H}_\Sigma(x_1,x_2,...,x_n)$ et $\mathbb{H}(x_1,x_2,...,x_n,y)) \Rightarrow 1 = 0$
et alors : $^*([\mathbb{H}_\Sigma(X_1,X_2,...,X_n) , \mathbb{H}(X_1,X_2,...,X_n,Y)] \Rightarrow 1 = 0)^*$ (dans **K**)

preuve> Les conditions de signe $\mathbb{H}_\Sigma$ imposent les degrés des polynômes de la famille stable (par reste et dérivation) engendrée par L , ainsi que le tableau de 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 :

---

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 $\forall\, x_1,x_2,...,x_n \in \mathbf{R}$ $\mathbb{H}(x_1,x_2,...,x_n)$ est absurde,
alors : ${}^*(\mathbb{H}(X_1,X_2,...,X_n) \Rightarrow 1=0)^*$ (dans **K**).

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 $n+1^{\text{ème}}$ variable, on va utiliser le théorème 28. Pour construire l'implication forte demandée, on raisonne cas par cas, selon les signes que prennent les polynômes de la famille $\mathcal{F}$. Soit donc Σ un élément arbitraire de $\{-1,0,+1\}^{\mathcal{F}}$.
Nous voulons construire l'implication forte:

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

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 $\mathbf{K}[\mathbf{X},\mathbf{T}_1,T_2,...,T_m] = \mathbf{K}[\mathbf{X},\mathbf{T}]$. 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:

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

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

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

avec p_i positif dans $\mathbb{Q}$, R_i et T_j dans $\mathbb{Q}[X_1, X_2, ..., X_n]$. 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

---

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

récursif, avec une preuve directe et entièrement constructive (pour le cas des corps discrets[1]), 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.

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)

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

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. :

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

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 :

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

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 :

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.

$$^*([U>0, V>0] \Rightarrow [U+V>0, U.V>0])^*$$
$$^*([U+V\geqslant 0, U.V>0] \Rightarrow [U>0, V>0])^*$$ etc... (cf. p. 5)

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

$$^*(U=V \Rightarrow P(X,U)=P(X,V))^*$$

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 $\mathbf{K[X]}$, Q un élément de $\mathbf{K[X]}$.

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 : $^*(\mathbb{H} \Rightarrow Q>0)^*$ $\underset{cons}{\vdash}$ $^*(\mathbb{H} \Rightarrow Q\geqslant 0)^*$.

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 $\mathbf{K[X]}$, Q un élément de $\mathbf{K[X]}$, alors:

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

De même :

$$[^*(\mathbb{H} \Rightarrow Q\leqslant 0)^* \text{ et } ^*(\mathbb{H} \Rightarrow Q\neq 0)^*] \underset{cons}{\vdash} ^*(\mathbb{H} \Rightarrow Q<0)^* \quad (b)$$
$$[^*(\mathbb{H} \Rightarrow Q=0)^* \text{ et } ^*(\mathbb{H} \Rightarrow Q\neq 0)^*] \underset{cons}{\vdash} ^*(\mathbb{H} \Rightarrow 1=0)^* \quad (c)$$
$$[^*(\mathbb{H} \Rightarrow Q\leqslant 0)^* \text{ et } ^*(\mathbb{H} \Rightarrow Q>0)^*] \underset{cons}{\vdash} ^*(\mathbb{H} \Rightarrow 1=0)^* \quad (d).$$

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 :

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

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

Nous posons :

$$\delta_6(d_1,d_2) = d_1.d_2 + \sup(d_1,d_2)$$ (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 $\leq d_1 + 2m.(d_2 - 1)$) 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 :

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

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 $\mathbf{K[X]}$.

Alors: $[\ ^*(\ \mathbb{H} \Rightarrow \mathbb{H}'\ )^*$ et $^*(\ [\ \mathbb{H}\ ,\ \mathbb{H}'\ ] \Rightarrow \mathbb{H}''\ )^*\ ]\ \underset{cons}{\vdash}\ ^*(\ \mathbb{H} \Rightarrow \mathbb{H}''\ )^*$

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 :

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

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* $\Phi : (\Delta^i)_{i=1,2,...} \longmapsto \Delta$, 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'hypothè

Proposition et majorations 13 :

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

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

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

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 X.

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

Si k est le nombre de csg dans $\mathbb{H}_2(X)$ et d_1 le degré de $^*(\mathbb{H}_1(X) \Rightarrow \mathbb{H}_2(X))^*$, une fonction Δ acceptable pour l'existence potentielle $^*(\mathbb{H}_1(X) \Rightarrow \exists\, T\ \mathbb{H}_2(X))^*$ 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 $^*(\mathbb{H}_1(X) \Rightarrow \mathbb{H}_2(X))^*$ admet Δ^1 pour fonction Δ et si δ majore le degré d'une csg ' $P\ \sigma\ 0$ ' dans $\mathbb{H}_2(X)$, alors on peut expliciter l'implication forte $^*(\mathbb{H}_1(X) \Rightarrow P\ \sigma\ 0)^*$ de manière que son degré soit majoré par $\Delta^1(\sup(1,2.\delta))$.

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

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

On peut alors éliminer une à une les k csg de $\mathbb{H}_2(X)$ en utilisant les k implications fortes élémentaires contenues dans $^*(\mathbb{H}_1(X) \Rightarrow \mathbb{H}_2(X))^*$, 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 $\exists\, T$ 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 :

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

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

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

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

$$\Delta = \Phi_{15,d}(\Delta^1,\Delta^2) \quad \text{où} \quad \Delta = \delta_{6,d} \circ (\Delta^1,\Delta^2)$$

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

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

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 $\Delta : d \longmapsto d.\delta'$.

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 $\Delta : d \longmapsto d + \delta$.

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 :

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

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 $\Delta : d \longmapsto 2d$.

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 $A^{2k} \leq 0$ $\square$

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 : $P^{(s)}(\mathbf{X},T) > 0$, $P^{(i)}(\mathbf{X},T) \geqslant 0$, i = 1, ..., s–1 .

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

On a alors les évidences fortes suivantes :

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

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

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

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

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

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

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 :

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

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 $\mathbf{X}$ 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 :

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

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 X et s le degré en U , l'existence potentielle accepte pour fonction Δ :

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

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 :

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

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 :

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

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 : $P(\mathbf{X},T.V) \equiv T^{s-1}\, Q(\mathbf{X},V) \quad (\mathrm{mod}\ 1 - C.T)$ (α)
Plus précisément $P(\mathbf{X},T.V) = T^{s-1}\, Q(\mathbf{X},V) + R(\mathbf{X},T,V).(1 - C.T)$ (β)
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 :

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

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 $d \geq \delta$) peut être calculée au moyen des formules récurrentes suivantes (qui font intervenir des fonctions auxiliaires):

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