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

Henri LOMBARDI -1990

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 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.

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 prédicatsintuitionniste : chaque prédicat n'est utilisé que précédé d'une double négation, les seuls connecteurs logiques utilisés sont ¬ et et le seul quantificateur utilisé est . 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 $\mathbf{CRD_i}$.
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 $\mathbf{T'(K)}$, (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 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.

---

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 autre que ludique”, nous ne commenterons pas leurs états d'âme.

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.

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 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, 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].

---

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 peut absolument pas être tranché à partir de l'algorithme donné dans l'hypothèse.

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]).

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 imposible 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 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 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 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 $\mathbf{K}$-isomorphisme unique près, de la clôture réelle d'un corps ordonné $\mathbf{K}$. Néanmoins, la preuve d'unicité donnée dans [VdW] utilise la factorisation d'un polynôme dans $\mathbf{K}[X]$ et n'est donc pas entièrement constructive.
En fait les théorèmes de Sturm et Sturm-Sylvester permettent de calculer dans la clôture réelle de $\mathbf{K}$ 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 $\mathbf{K}[X]$, $[\sigma_1, \sigma_2, \ldots, \sigma_n]$ une liste de signes stricts. Supposons que $\mathbf{K}$ possède une clôture réelle $\mathbf{R}$. On peut déterminer le nombre de

---

5 D'un point de vue constructif, l'infini est une notion purement négative. La comparaison entre N et 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 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 portant sur des entiers naturels. Ce serait le cas ici. De toute manière, quoique plus compliqué que N, l'infini R peut être traité de manière constructive comme l'a montré Bishop (cf. [BB]).

6 au moins si on admet qu'on peut décider le signe de tout élément

racines de P (dans $\mathbf{R}$) qui attribuent les signes $\sigma_1, \sigma_2, \ldots, \sigma_n$ aux polynômes $Q_1, Q_2, \ldots, Q_n$ 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 $\mathbf{K}$ 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 $\mathbf{K}$. Donc on sait calculer dans l'extension ordonnée $\mathbf{K}[\xi]$ de $\mathbf{K}$. En itérant le processus, on peut calculer dans la clôture réelle de $\mathbf{K}$. 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.
Cette généralisation du théorème de Sturm est basée sur une analyse détaillée de ce que compte 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 :
>
> $f_1(x_1, x_2, \ldots, x_n) = 0$, $f_2(x_1, x_2, \ldots, x_n) = 0$, ..., $f_s(x_1, x_2, \ldots, x_n) = 0$
>
> Dans le cas du corps 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 *relationpolynomiale* 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 $f : \mathbf{R}^n \to \mathbf{R}$, définie de telle manière qu'on ait un algorithme primitif récursif qui calcule, à partir d'une relation polynomiale arbitraire $A(y,t_1,t_2,\ldots,t_k)$ une autre relation polynomiale $B(x_1,x_2,\ldots,x_n,t_1,t_2,\ldots,t_k)$ telle qu'on ait l'équivalence dans $\mathbf{R}$:

$$A(f(x_1,x_2,\ldots,x_n),t_1,t_2,\ldots,t_k) \Leftrightarrow B(x_1,x_2,\ldots,x_n,t_1,t_2,\ldots,t_k)$$

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

En considérant la relation $y = t$ on voit que, entre autres choses, le graphe de f doit être semi-algébrique défini sur Q, et le but est en quelque sorte de montrer que toute fonction semi-algébrique définie sur Q est semi-algébrique effective. Cohen remarque que les fonctions semi-

---

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 Q.

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 , $P_d(c_0,c_1, \ldots,c_d , x) = P_d(\mathbf{c},x)$ (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 $\mathbf{R}$: $\text{signe}(P_d(\mathbf{c},f(\mathbf{x}))) = s \Leftrightarrow B(\mathbf{c},\mathbf{x},s)$

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 $A(x_1,x_2,\ldots,x_n)$ une autre relation polynomiale $B(x_2,\ldots,x_n)$ avec l'équivalence dans $\mathbf{R}$:
>
> $$x_1\ A(x_1,x_2,\ldots,x_n) \quad \Leftrightarrow \quad B(x_2,\ldots,x_n)$$

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 $x_2,\ldots,x_n$, 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 $A(x_1,x_2,\ldots,x_n)$ sera immédiate à tester. La "forme générale" de ce grand tableau dépendra de $x_2,\ldots,x_n$ 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 $\mathbf{K}$ 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,

---

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 inclue d dans les entrées de l'algorithme primitif récursif affirmé exister, mais la formulation serait plus lourde.

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 $\mathbf{K}$ 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. 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 $17^{\text{ème}}$ problème de Hilbert. Nous rendons compte ici de l'article "Sums of

---

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 polynôme sur un intervalle.

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 :

" 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

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

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 :

($\mathbb{H}(\mathbf{c})$ $g_{n,d}(\mathbf{c},\mathbf{x})$ 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 : $\mathbb{C}'$: $\mathbf{x}$ z $g_{n,d}(\mathbf{c},\mathbf{x}) = z^2$.

---

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 pour tout $\mathbf{x}$ dans un corps réel clos contenant les coefficients.

16 portant sur des polynômes en les coefficients de f.

17 Les coefficients sont maintenant des éléments d'un corps réel clos.

Si nous examinons maintenant la preuve de ($\mathbb{H}'$ $\mathbb{C}'$) 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 : $\mathbb{A}_2$:
$u_1\ u_2 \ldots\ u_s\ \ 1+ u_1^2+ u_2^2 \ldots + u_s^2 \neq 0$ (un seul suffit)

– des axiomes existentiels : $\mathbb{A}_3$:
a) $u \neq 0\ \ z\ \ u.z = 1$,
b) $u\ \ z\ (u = z^2$ ou $u = -z^2)$, et des axiomes
c,r) $u_1\ \ u_2 \ldots\ u_{2r+1}\ \ z\ \ z^{2r+1} + u_1.z^{2r} + u_2.z^{2r-1} + \ldots + u_{2r+1} = 0$
(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 $\mathbb{A}_3$) $\mathbb{C}'$

Par ailleurs on a aussi une preuve pour :
($\mathbb{A}_1$ et $\neg\ \mathbb{A}_2$ et $\mathbb{A}_3$) $\mathbf{x}\ \ u_1\ \ u_2 \ldots\ u_s\ \ g_{n,d}(\mathbf{x}) = u_1^2+ u_2^2 \ldots + u_s^2$
(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 $\mathbb{A}_3$) $\mathbf{x}\ \ u_1\ \ u_2 \ldots\ u_s\ \ g_{n,d}(\mathbf{x}) = u_1^2+ u_2^2 \ldots + u_s^2$

Il faut maintenant arriver à faire façon des quantificateurs existentiels dans l'hypothèse. Pour cela on rajoute des symboles fonctionnels, le symbole ι (ι(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 ρ(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 : $u \neq 0\ \ u.u^{-1} = 1$). On appelle $\mathbb{A}_3'$ le nouveau système d'axiomes obtenu. D'où une preuve dans le calcul des prédicats classique pour :
($\mathbb{H}'(\mathbf{c},\mathbf{y})$ et $\mathbb{A}_1$ et $\mathbb{A}_3'$) $\mathbf{x}\ \ u_1\ \ u_2 \ldots\ u_s\ \ g_{n,d}(\mathbf{x}) = u_1^2+ u_2^2 \ldots + u_s^2$
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
($\mathbb{H}'(\mathbf{c},\mathbf{y})$ et $\mathbb{A}_1$ et $\mathbb{A}_3'$) $\bigvee_{i=1\ldots N}\ g_{n,d}(\mathbf{x}) = t_{i,1}^2+ t_{i,2}^2 \ldots + t_{i,s}^2$

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 $\rho(s)$". On se ramène au cas "somme de carrés de polynômes en $\rho(s)$" en utilisant "la quantité conjuguée". Par ailleurs, on se souvient que $\rho(s)$ 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 $\Sigma\, a_ib_i \neq 0$ on a $2\sqrt{s} = (\Sigma\, a_ib_i)^{-1}.(f - \Sigma\, a_i^2 - s\,\Sigma\, b_i^2)$ ce qui permet de faire disparaître $\sqrt{s}$ de la première expression. Si $\Sigma\, a_ib_i = 0$, on essaie avec la deuxième. Si $\Sigma\, a_ib_j = \Sigma\, c_jd_j = 0$, 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 $\imath$ (qui représente l'inverse d'un élément, avec $\imath(0) = 0$ par convention) : la réduction d'une écriture comportant comme seuls symboles fonctionnels $+$, $-$, $\times$, et $\imath$ à une forme "fraction rationnelle" pose en effet problème du fait que $u.\imath(v)$ n'est égal à $uw.\imath(vw)$ 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 $f_r(\mathbf{x}) = 0\,]$ $\quad g(\mathbf{x}) = 0$ dans la théorie formelle des anneaux intègres réels alors on peut construire un nullstellensatz, c.-à-d. une identité algébrique du type :
>
> $$\Sigma\, a_i(\mathbf{x}).f_i(\mathbf{x}) = m.g(\mathbf{x})^p + \Sigma\, b_j(\mathbf{x})^2 \quad (m \text{ et } p \text{ sont des entiers} \geq 1)$$

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.

---

[18] tous les axiomes de la théorie des anneaux intègres réels sont mis sous forme: dérivation d'une formule atomique à partir d'autres formules atomiques.

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 :

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

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 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 : $\mathbf{x} \quad \mathbf{R}^n \ (\ \mathbb{H}(\mathbf{x}) \qquad \mathbb{H}'(\mathbf{x})\ )$.
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 B et B C alors A 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 :

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

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 utilisé pour calculer dans la clôture réelle d'un corps ordonné $\mathbf{K}$.
Le deuxième est une preuve constructive du résultat suivant : si $\mathbf{K}$ est un corps réel, la théorie $\mathbf{CRCD_i}(\mathbf{K})$ 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. [Cos]).

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 :

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

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 $\neq$: $\neg (x \neq y) \Leftrightarrow x = y$
  $x \neq 0 \Leftrightarrow y \; x.y = 1 \Leftrightarrow x < 0$ ou $x > 0$
- axiomes pour $>$: $\neg (x > y) \Leftrightarrow x \leq y$
  $x > y \qquad x + z > y + z$
  $x > 0$ et $y > 0 \qquad x.y > 0$ et $x + y > 0$
  $x + y > 0 \qquad x > 0$ 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 R qui sera réel clos (notion qui reste à définir dans ce nouveau cadre) fera pour nous aussi bien l'affaire que 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 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 R .

Certains théorèmes classiques indémontrables constructivement pour des fonctions continues arbitraires sont néanmoins prouvables lorsque l'on se restreint aux fonctions polynômes, ou

---

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

20 Il est sans doute possible de considérer l'analyse classique comme intermédiaire entre l'analyse constructive habituelle et une analyse constructive non standard qui reste à ... construire.

semi-algébriques continues (ils sont en règle générale prouvables pour les fonctions semi algébriques définies sur 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 $x_0, x_1, \ldots, x_d$ 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. o

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. o
On voit que le deuxième théorème est démontrable à partir du premier dans la théorie $\mathbf{CO_i}$.

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 $x_1, x_2, \ldots, x_d$ les parties réelles des zéros de P' rangées en ordre croissant. Posons $y_0 = a$, $y_{d+1} = b$, et pour $i = 1, \ldots, d$: $y_i = f(x_i)$ 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 : $\inf \{P(x); a \leq x \leq b\} = \inf \{P(y_i); i = 0, 1, \ldots, d+1\}$

---

21 continuité des sorties en fonction des entrées

En effet : ce résultat est facile pour P à coefficients rationnels et se prolonge par continuité pour le cas de coefficients réels arbitraires. o

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 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 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 R.

Nous rendons compte maintenant de travaux qui cernent en partie la question du théorème des zéros réels dans 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 $\mathbf{K}$-semi-algébrique (c.-à-d. semi-algébrique défini par des équations et inéquations à coefficients dans $\mathbf{K}$ supposé discret) est réunion d'un nombre fini de fermés $\mathbf{K}$-semi-algébriques élémentaires (un fermé semi-algébrique est élémentaire s'il est défini par des inéquations du type $P(\mathbf{x}) \geq 0$). On trouve dans [Cos] 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 Q-semi-algébrique tel que dans tout corps réel clos discret $\mathbf{R}$ on ait l'équivalence :

$$\mathbf{c} \in \mathbf{R}^m \ (\ \mathbf{c} \in P_{n,d}(\mathbf{R})\ ^{22} \Leftrightarrow \mathbf{x} \in \mathbf{R}^n\ f_{n,d}(\mathbf{c},\mathbf{x}) \geq 0\ ) \qquad (1)$$

Delzell construit un entier s et des fonctions 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 :

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

---

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 Même remarque concernant la généricité de ces fonctions Q-semi-algébriques.

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 $\mathbf{x}$:

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

Les coefficients de chaque $t_h(\mathbf{c},\mathbf{x})$ (vue comme fraction rationnelle en $\mathbf{x}$) sont des fonctions 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 R^m et 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 $P_{n,d}(R) \times R^n$ 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 R, c.-à-d. à donner une preuve constructive de l'implication :

$$\mathbf{c} \quad R^m \quad [\,(\ \mathbf{x} \quad R^n \ f_{n,d}(\mathbf{c},\mathbf{x}) \geq 0\,) \qquad \mathbf{c} \quad P_{n,d}(R)\,]$$

Notons $Q_{n,d}(R)$ la partie de R^m définie par le premier membre de l'implication.
Il est clair que $Q_{n,d}(R)$ est un cône convexe fermé et que le point $\mathbf{c}$ correspondant à la forme $(\Sigma\, x_i^2)^{d/2}$ est intérieur à $Q_{n,d}(R)$. Donc $Q_{n,d}(R)$ est l'adhérence de son intérieur.
Enfin $Q_{n,d}(R)$ et $P_{n,d}(R)$ ont les mêmes points rationnels puisque l'équivalence (1) est valable pour les réels algébriques. Etant donné un point de $Q_{n,d}(R)$ on peut donc l'expliciter comme limite d'une suite de points rationnels de $P_{n,d}(R)$, et on conclut en remarquant que $P_{n,d}(R)$ 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 $P_{n,d}$", $\mathbf{c} \mapsto d(\mathbf{c},P_{n,d}(\mathbf{R}))$ (avec $\mathbf{R}$ corps des nombres réels algébriques) est une fonction semi-algébrique contractante qui se prolonge par continuité à R^m et cela montre que $P_{n,d}(R)$, adhérence de $P_{n,d}(\mathbf{R})$, est un fermé situé (la fonction distance est calculable).

Problème : Peut-on démontrer constructivement l'équivalence :

$$\mathbf{c} \quad R^m \quad (\ d(\mathbf{c},P_{n,d}(R)) > 0 \quad \Leftrightarrow \quad \mathbf{x} \quad R^n \ f_{n,d}(\mathbf{c},\mathbf{x}) < 0\,) \qquad (1') \qquad ?$$

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 $\mathbf{x} \quad \mathbf{R}^n \ (\ \mathbb{H}(\mathbf{c},\mathbf{x}) \qquad \mathbb{H}'(\mathbf{c},\mathbf{x})\,)$ à traduire en identité algébrique, est, par définition, vraie pour $\mathbf{c}$ dans une partie fermée.

Scowcroft : les problèmes du type 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 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 :

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

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

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

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 :

$$(\ \ p_{i,j}(\mathbf{x}) > 0 \qquad q_{i,k}(\mathbf{x}) > 0\ )$$

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 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 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

---

24 Nous ne présenterons pas ici le modèle de Scott, qui s'éloigne trop de notre propos.

25 Principes qui entrent en contradiction directe avec les mathématiques classiques, et ne sont pas admissibles du point de vue constructif minimal de Bishop.

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).

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

[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 17^{th} 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.