

*Les “vrais” nombres réels
en Calcul Formel ?*

1^{er} Colloque Franco-Maghrebin de Calcul Formel
Kerkenah. 24 mai 2008

H. Lombardi, Besançon
Henri.Lombardi@univ-fcomte.fr, <http://hlombardi.free.fr>
Pour imprimer ces transparents :

<http://hlombardi.free.fr/publis/KerkenahDoc.pdf>

Une version développée en anglais

<http://hlombardi.free.fr/publis/AlrecoProgram.pdf>

*Quelles sont les propriétés algébriques
des nombres réels*

**i.e., les propriétés
de $+$, $-$, $\times$, $>$, $\geq$**

Résumé :
Beaucoup de questions. Peu de réponses.

Pourquoi étudier l'algèbre réelle constructive ?

L'algèbre réelle constructive n'est pas bien comprise !

L'analyse constructive ($\simeq$ les méthodes certifiées en analyse numérique) est nettement mieux étudiée.

D'un point de vue constructif l'algèbre réelle est *assez éloignée* de la théorie usuelle classique des corps réels clos à la Artin, dans laquelle on suppose que l'on a un *test de signe*.

La plupart des algorithmes de l'algèbre classique échouent avec les nombres réels, parce qu'ils requièrent un test de signe.

Même en analyse constructive, on pourrait avoir des retombées intéressantes. Par exemple cela permettrait de mieux comprendre comment éviter le recours à l'axiome du choix dépendant.

Pourquoi étudier l'algèbre réelle constructive ?

La compréhension de l'algèbre réelle constructive peut être un premier pas pour une théorie constructive (et donc algorithmique) des *structures O-minimales*.

L'algèbre réelle peut être vue comme la plus simple des structures O-minimales. La théorie classique (non algorithmique) des structures O-minimales donne en effet des pseudo-algorithmes qui ne fonctionnent qu'avec un test de signe sur les réels.

Pourquoi étudier l'algèbre réelle constructive ?

En Calcul Formel, on cherche de plus en plus à profiter de la symbiose entre méthodes numériques et méthodes algébriques formelles.

J'ai le sentiment que l'on manque d'une théorie de cette symbiose, et qu'une bonne compréhension constructive des corps réels clos pourrait être une première approche de cette théorie.

Une courbe algébrique définie par un polynôme à coefficients réels ressemble plus à une courbe définie par un polynôme à coefficients réels flottants, qu'à une définie par un polynôme à coefficients rationnels.

— page 6 —

Qu'est-ce qu'un “vrai” nombre réel en Calcul Formel ?

Cela relève inévitablement de l'évaluation paresseuse.

Un peu comme la théorie de Galois sur un corps qui ne possède pas d'algorithme de factorisation pour les polynômes.

En entrée : un oracle (éventuellement un algorithme) qui donne le nombre réel sur un intervalle rationnel de longueur requise (requis par l'algorithme).

Instruction typique : $a \leftarrow x \pm 1/2^n$.

En sortie : un intervalle rationnel de longueur requise (requis par l'utilisateur).

Variante : écriture ambiguë en base 60 avec 64 chiffres.

— page 7 —

Un outil qui pourrait s'avérer utile : les racines virtuelles

Virtual roots of real polynomials.

Gonzalez-Vega L., L. H., Mahé L.

Journal of Pure et Applied Algebra **124**, (1998) 147–166.

<http://hlombardi.free.fr/publis/AVirtualRealRoots.html>

Generalized Budan-Fourier theorem et virtual roots.

Coste M., Lajous T., L. H., Roy M.-F.

Journal of Complexity **21** (2005), 479–486.

<http://hlombardi.free.fr/publis/BudanVirtual.pdf>

— page 8 —

les racines virtuelles

Lemme 1. *Une fonction continue f strictement croissante $[a, b] \subseteq \mathbb{R}$ ($a \leq b$) atteint son (unique) minimum valeur absolue.*

Corollaire 2. *On peut définir sur l'espace des polynômes réels de degré d , d fonctions “racines virtuelles” $\rho_{d,k}$ ($k = 1, \dots, d$) avec les propriétés caractéristiques suivantes,*

$$\begin{aligned} f(\rho_{1,1}(f)) &= 0 && \text{if } d = 1 \\ \rho_{d-1,k-1}(f') &\leq \rho_{d,k}(f) \leq \rho_{d-1,k}(f') && \text{if } d \geq 2 \\ |f(\rho_{d,k}(f))| &\leq |f(x)| && \text{if } \rho_{d-1,k-1}(f') \leq x \leq \rho_{d-1,k}(f') \end{aligned}$$

(avec la convention $f(\rho_{d,0}(f)) = \varepsilon(-1)^d \infty$, $f(\rho_{d,d+1}(f)) = \varepsilon \infty$, où $\varepsilon = \pm 1$ est le signe du coefficient dominant)

— page 9 —

les racines virtuelles, 2.

1. Si $f(T) = (T - a)(T - b)$ alors

$$\rho_{2,1}(f) = \inf(a, b), \rho_{2,2}(f) = \sup(a, b).$$

2. Si $\deg(f) = d$ et $f(x) = 0$ alors $\prod_{i=1}^d (x - \rho_{d,i}(f)) = 0$.

3. Version constructive de l'axiome des corps réels clos :

si $\deg(f) = d$, $a < b$ et $f(a)f(b) < 0$ alors

$$\prod_{i=1}^d f(\mu_{d,i}(f)) = 0,$$

où $\mu_{d,i}(f) = \inf(b, \sup(a, \rho_{d,i}(f)))$.

4. Chaque $\rho_{d,i}(f)$ est une fonction localement uniformément continue, et est un zéro du produit

$$f \cdot f' \dots f^{(k)} \dots f^{(d-1)}.$$

5. Les racines virtuelles sont comptées par la méthode de **Descartes-Budan-Fourier** (donc faciles à « calculer »).

page 10

les racines virtuelles, 3.

Un résultat à la Pierce-Birkhoff

Théorème 1.

Soit $f : \mathbb{R}^n \rightarrow \mathbb{R}$ une fonction semialgébrique continue définie sur $\mathbb{Q}$ entière sur l'anneau $\mathbb{Q}[X_1, \dots, X_n]$. Alors f est une combinaison de fonctions racines virtuelles et de polynômes à coefficients dans $\mathbb{Q}$.

Remarque. Dans le théorème précédent on peut remplacer $\mathbb{Q}$ par un sous-corps discret de $\mathbb{R}$.

Remarque. Est-il possible de remplacer $\mathbb{Q}$ par $\mathbb{R}$? (la signification exacte de l'hypothèse doit alors être éclaircie). Nous avons besoin d'une bonne définition de « $f : \mathbb{R}^n \rightarrow \mathbb{R}$ est une fonction semialgébrique continue. »!

page 11

Les corps de Heyting ... sans négation

$$(\mathbf{K}, =, 0, \neq, +, -, \times, 0, 1)$$

$$\text{— } x = y : x - y = 0$$

$$\text{— } x \neq y : x - y \neq 0$$

$$\text{— } x \neq 0 : x \text{ inversible}$$

Axiomes :

F1 $(\mathbf{K}, =, 0, +, -, \times, 0, 1)$ est un anneau commutatif. I.e., machinerie calculatoire des polynômes, plus 3 axiomes **directs** :

$$\vdash 0 = 0, \quad x = 0 \vdash xy = 0, \quad x = 0, y = 0 \vdash x + y = 0.$$

F2 $x^2 = 0 \vdash x = 0$ (**simplification**)

F3 $x + y \neq 0 \vdash x \neq 0 \vee y \neq 0$ (**dynamique**)

F4 $(x \neq 0 \Rightarrow 1 = 0) \vdash x = 0$ (**compliqué**)

page 12

Corps de Heyting

Autrement dit, un corps de Heyting est anneau local dont le radical de Jacobson est réduit à 0.

Exemples : $\mathbb{R}$, $\mathbb{C}$, $\mathbb{R}(t)$, $\mathbb{C}(t)$, nombres réels primitifs recursifs, ...

Remarque. L'axiome **F4**

$$\mathbf{F4} \quad (x \neq 0 \Rightarrow 1 = 0) \vdash x = 0$$

signifie que l'anneau local (axiome **F3**) a son radical de Jacobson égal à 0. Axiome très désagréable. Forme affaiblie de **DF** (discrete field) ; supposer qu'on a presque un test de signe :

$$\mathbf{DF} \quad x = 0 \vee x \neq 0$$

Remarquons que **F4** et **DF** sont des formulations sans négation : l'anneau trivial est autorisé.

Collapsus simultanés : corps de Heyting/anneaux commutatifs

Un anneau commutatif qui collapse (i.e, se réduit à l'anneau trivial) comme corps discret collapse comme anneau commutatif.

A fortiori un corps de Heyting (avec ou sans l'axiome désagréable **F4**) qui collapse comme corps discret, collapse comme corps de Heyting.

Pour les collapsus simultanés voir :

<http://hlombardi.free.fr/publis/NullstellensatzDynamic.pdf>

(*Dynamical method in algebra : Effective Nullstellensätze*. Coste M., L. H., Roy M.-F. Annals of Pure et Applied Logic **111**, (2001) 203-256)

Corps de Heyting ordonnés

$$(\mathbf{K}, =, 0, \neq 0, > 0, \geq 0, +, -, \times, \sup, 0, 1)$$

$$\text{— } x = y \text{ means } x - y = 0$$

$$\text{— } x \neq y \text{ means } x - y \neq 0$$

$$\text{— } x > y \text{ means } x - y > 0$$

$$\text{— } x \leq y \text{ means } x - y \leq 0$$

Axiomes directs

$$1. (\mathbf{K}, =, 0, +, -, \times, 0, 1) \\ \text{anneau commutatif.}$$

$$6. (x > 0, y \geq 0) \vdash x + y > 0$$

$$2. \vdash 1 > 0$$

$$7. (x > 0, y > 0) \vdash xy > 0$$

$$3. x = 0 \vdash x \geq 0$$

$$8. (x \geq 0, y \geq 0) \vdash x + y \geq 0$$

$$4. x > 0 \vdash x \geq 0$$

$$9. (x \geq 0, y \geq 0) \vdash xy \geq 0$$

$$5. \vdash x^2 \geq 0$$

Collapsus

$$10. 0 > 0 \vdash 1 = 0$$

Corps de Heyting ordonnés

Règles de simplification

$$11. \quad x^2 \leq 0 \vdash x = 0$$

$$12. \quad (c \geq 0, cs > 0) \vdash s > 0$$

13. $(s > 0, cs \geq 0) \vdash c \geq 0$
14. $(c \geq 0, x(x^2 + c) \geq 0) \vdash x \geq 0$

Règles dynamiques

15. $x + y > 0 \vdash x > 0 \vee y > 0$
16. $xy > 0 \vdash x > 0 \vee -y > 0$
17. $x^2 > 0 \vdash \exists y xy = 1$

Discrets

DOF $\vdash x \geq 0 \vee -x > 0$

De Heyting

HOF $(x > 0 \Rightarrow 1 = 0) \vdash x \leq 0$

— page 16 —

Collapsus simultanés et faits prouvables

Théorème 2. Soit **A** un anneau commutatif. Soient Z, P, S trois sous-ensembles. On considère l' "anneau préordonné dynamique" défini par ces données (i.e., let $x = 0$ for $x \in Z$, $x \geq 0$ pour $x \in P$, $x > 0$ pour $x \in S$). Alors on a les collapsus simultanés suivants :

- a) Utiliser uniquement les axiomes directs.
- b) Utiliser aussi les règles de simplification.
- c) Utiliser les axiomes directs, les règles dynamiques et **DOF** (les règles de simplification s'ensuivent).
- d) Ajouter aussi les axiomes de clôture réelle : un polynôme unitaire qui change de signe entre a et b a un zéro sur $]a, b[$.

En outre les structures dynamiques b), c) et d) prouvent les mêmes faits.

— page 17 —

Collapsus simultanés et faits prouvables, 2.

Ainsi ajouter **DOF** comme un axiome dans un corps ordonné de Heyting ne change pas les faits, et ne produit pas de collapsus (dans la ligne du programme de Hilbert).

Même chose avec les axiomes de clôture réelle

On peut donc utiliser librement le « tiers exclu limité » **DOF** et les axiomes de clôture réelle si on veut seulement prouver des faits.

— page 18 —

Propriétés de clôture réelle

Dans le cas d'un corps discret.

RCF1 : Un polynôme P tel que $P(a) < 0$, $P(b) > 0$, $a < b$ admet un zéro sur (a, b) .

L'axiome **RCF1** n'est pas valable pour les nombres réels sans recours à l'axiome du choix dépendant. L'axiome suivant est par contre toujours constructivement valide :

RCF2 : Un polynôme P tel que $P(a) < 0$, $P(b) > 0$, $a < b$ et $P' > 0$ sur (a, b) admet un zéro sur (a, b) .

— page 19 —

Une définition plausible

Définition 3. Un corps réel clos est un corps de Heyting ordonné avec des fonctions racines virtuelles en tout degré qui satisfont les propriétés caractéristiques données dans le cas du corps des nombres réels.

Exemples de sous corps non discrets de $\mathbb{R}$ réels clos en ce sens.

- Les nombres réels primitifs rékursifs.
- Les nombres réels calculables en temps polynomial.
- Les nombres réels Turing-calculables.

— page 20 —

*Questions connexes
en suspens*

**Construction de la clôture réelle d'un corps
ordonné (non discret)**

Autres propriétés de clôture

Le théorème de projection semialgébrique

Positivstellensätze constructifs