Le mystère de la structure du continu

Colloque « Des Nombres et des Mondes » La Rochelle. 27-29 juin 2011

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

http ://hlombardi.free.fr/publis/NombresLR2011Doc.pdf

L'invention de la droite réelle par Cantor et Dedekind

Il s'agit d'un coup de force étonnant.
Que sont et que doivent être les nombres réels ?, dit Dedekind.
Dedekind prétend être le premier à démontrer $\sqrt{2}.\sqrt{3} = \sqrt{6}$
Pourtant Archimède savait le démontrer.
Alors qu'est-ce qui a changé ?

L'appréciation de Poincaré

La Science et l'Hypothèse. Chapitre II.
La grandeur mathématique et l'expérience.

Avant d'aller plus loin, faisons une première remarque. Le continu ainsi conçu n'est plus qu'une collection d'individus rangés dans un certain ordre, en nombre infini, il est vrai, mais *extérieurs* les uns aux autres. Ce n'est pas là la conception ordinaire, où l'on suppose entre les éléments du continu une sorte de lien intime qui en fait un tout, où le point ne préexiste pas à la ligne, mais la ligne au point. De la célèbre formule, le continu est l'unité dans la multiplicité, la multiplicité seule subsiste, l'unité a disparu. Les analystes n'en ont pas moins raison de définir leur continu comme ils le font, puisque c'est toujours sur celui-là qu'ils raisonnent depuis qu'ils se piquent de rigueur. Mais c'est assez pour nous avertir que le véritable continu mathématique est tout autre chose que celui des physiciens et celui des métaphysiciens.

Des théorèmes au contenu étrange, difficile à cerner

Un théorème part d'une hypothèse pour arriver à une conclusion. Il est utile dans la mesure où il nous fait découvrir une propriété qui a le caractère d'une vraie nouveauté par rapport à l'hypothèse. Par exemple Cayley-Hamilton, ou un théorème qui décrit la répartition des nombres premiers, ou le théorème des accroissements finis.
En analyse il arrive pourtant fréquemment que l'on ne sache pas certifier l'hypothèse autrement que par la conclusion.
On part de quelque chose d'inconnu, pour arriver à quelque chose de concret. Mais la chose inconnue semble impossible à maitriser, sauf à avoir la conclusion.

L'analyse constructive : une solution ?

Un des mérites de Bishop est d'avoir clairement isolé un **principe d'omniscience**, **LPO : le petit principe d'omniscience**, qui gouverne ces théorèmes étranges, et d'ailleurs étrangers à l'analyse numérique.
Il contourne la difficulté en modifiant convenablement les définitions.
Néanmoins, chez lui, la droite réelle reste un ensemble de points, même s'ils ne sont plus aussi extérieurs les uns aux autres qu'ils ne le sont en mathématiques classiques.
Le recours à l'axiome du choix dénombrable jette en outre un certain trouble, car il permet des énoncés moins "uniformes" qu'on ne le souhaite avec notre intuition du continu : exemple du théorème fondamental de l'algèbre.

La topologie sans points : une solution ?

Certainement cela devrait ouvrir de belles perspectives.
Voir la manière dont on comprend le problème posé par "Heine-Borel" avec la topologie sans points !
Félicitations, messieurs !
Bon, mais il reste sans doute encore trop de points sur cette belle droite, élégante et minimaliste.

L'analyse constructive non standard : une solution ?

À creuser

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 (requise par l'algorithme).
Instruction typique : $a \leftarrow x \pm 1/2^n$.
Variante : écriture ambigüe en base 60 avec 64 chiffres.

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

Un programme typique : calculer $y = \exp(x)$
Questions posées par le programme : x avec la précision 1 ? la précision requise sur y ?
En fonction des réponses, nouvelle question : veuillez me donner x avec telle précision.
En sortie : un intervalle rationnel de longueur requise.

Un cas d'école à étudier : quelles sont les propriétés algébriques des nombres réels ?

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

En bref : qu'est-ce vraiment que l'algèbre réelle.

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-Tarski, 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.

Corps de Heyting ordonnés

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

- $x = y$ signifie $x - y = 0$
- $x > y$ signifie $x - y > 0$
- $x \leqslant y$ signifie $x - y \leqslant 0$
- $x \neq y$ signifie $(x - y)^2 > 0$

Axiomes directs

1. $(\mathbf{K}, = 0, +, -, \times, 0, 1)$ est un anneau commutatif :
   Machinerie calculatoire des polynômes et 3 axiomes directs

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

2. $\vdash\ 1 > 0$
3. $x = 0\ \vdash\ x \geqslant 0$
4. $x > 0\ \vdash\ x \geqslant 0$
5. $\vdash\ x^2 \geqslant 0$
6. $(x > 0,\ y \geqslant 0)\ \vdash\ x + y > 0$
7. $(x > 0,\ y > 0)\ \vdash\ xy > 0$
8. $(x \geqslant 0,\ y \geqslant 0)\ \vdash\ x + y \geqslant 0$
9. $(x \geqslant 0,\ y \geqslant 0)\ \vdash\ xy \geqslant 0$

Collapsus

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

Corps de Heyting ordonnés

Règles de simplification

11. $x^2 \leqslant 0 \ \vdash \ x = 0$
12. $(c \geqslant 0,\, cs > 0) \ \vdash \ s > 0$
13. $(s > 0,\, cs \geqslant 0) \ \vdash \ c \geqslant 0$
14. $(c \geqslant 0,\ x(x^2 + c) \geqslant 0) \ \vdash \ x \geqslant 0$

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
$\vdash \ x = 0 \vee x^2 > 0$

De Heyting : HOF
$(x \neq 0 \ \Rightarrow \ 1 = 0) \vdash \ x = 0$

Corps de Heyting ordonnés

Problème avec sup

La théorie formelle précédente **ne prouve pas** l'existence du sup de deux éléments, i.e., ceci n'est pas prouvable :

$$\forall x, y\ \exists z \quad (z - x)(z - y) = 0,\ z \geqslant x,\ z \geqslant y$$

Il faut ajouter le symbole de fonction sup avec les axiomes suivants.
Règles pour sup

18. $\vdash \ \sup(x, y) = \sup(y, x)$
19. $\vdash \ \sup(x, y) \geqslant x$
20. $\vdash \ (\sup(x, y) - x)\,(\sup(x, y) - y) = 0$

Corps de Heyting ordonnés

Propriétés de la fonction sup

On définit $\inf(a, b) = -\sup(-a, -b)$.

- $\sup(x + z, y + z) = \sup(x, y) + z$
- $\sup(x, y) + \inf(x, y) = x + y$
- $\sup(x, y) \inf(x, y) = xy$
- $\sup(x, y) > 0 \iff (\, x > 0 \vee y > 0\,)$
- $x = \sup(x, y) \iff x \geqslant y$
- $\sup(x, y) < 0 \iff (x < 0 \wedge y < 0)$
- $\sup(x, y) \leqslant 0 \iff (x \leqslant 0 \wedge y \leqslant 0)$

Remarque. Les deux ensembles $\{a, b\}$ et $\{\inf(a, b), \sup(a, b)\}$ ont la même adhérence, qui est l'ensemble des zéros de $(T - a)(T - b)$.
Choses similaires avec $(T - a_1) \cdots (T - a_n)$.

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

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/ABudanVirtual.pdf

les racines virtuelles

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

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

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

(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)

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 $\mathsf{deg}(f) = d$ 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 $\mathsf{deg}(f) = d$, $a < b$ 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
$$f \cdot f' \cdots f^{(k)} \cdots f^{(d-1)}.$$
5. Les racines virtuelles sont comptées par la méthode de **Descartes-Budan-Fourier** (donc faciles à « calculer »).

les racines virtuelles, 3.

Un résultat à la Pierce-Birkhoff

Théorème 1.
Soit $f : \mathbb{R}^n \to \mathbb{R}$ une fonction semialgébrique continue définie sur $\mathbb{Q}$ entière sur l'anneau $\mathbb{Q}[X_1, \ldots, X_n]$. 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 « $f : \mathbb{R}^n \to \mathbb{R}$ est une fonction semialgébrique continue. » !