

Preuves formelles et arithmétique réelle exacte

Ioana Paşca

INRIA Sophia Antipolis – Equipe Projet Marelle

RAIM, Octobre 2009

Arithmétique réelle exacte dans les assistants à la preuve

Motivations :

les réels dans les assistants à la preuve

Implémentations et certification :

3 bibliothèques d'arithmétique réelle exacte

Méthodes numériques sur des réels exacts :

le cas de la méthode de Newton

Assistants à la preuve

- **formaliser** des concepts
- **prouver** des propriétés sur ces concepts

Assistants à la preuve et nombres réels

dans la bibliothèque standard de COQ on a des **réels abstraits**

- définis par des axiomes

$$r_1 + (r_2 + r_3) = (r_1 + r_2) + r_3$$

- définitions et preuves proches des “maths sur papier”
convergence, dérivabilité, théorème fondamental de l'analyse, etc.

Assistants à la preuve et nombres réels

dans la bibliothèque standard de COQ on a des **réels abstraits**

- définis par des axiomes

$$r_1 + (r_2 + r_3) = (r_1 + r_2) + r_3$$

- définitions et preuves proches des “maths sur papier”
convergence, dérivabilité, théorème fondamental de l'analyse, etc.
- mais sans la puissance du calcul

Assistants à la preuve et nombres réels

dans la bibliothèque standard de COQ on a des **réels abstraits**

- définis par des axiomes

$$r_1 + (r_2 + r_3) = (r_1 + r_2) + r_3$$

- définitions et preuves proches des “maths sur papier”
convergence, dérivabilité, théorème fondamental de l'analyse, etc.
- mais sans la puissance du calcul

situation analogue dans les autres assistants à la preuve

Assistants à la preuve et calcul

on veut :

calculer dans les assistants à la preuve

utiliser les calculs dans les preuves

Assistants à la preuve et calcul

on veut :

- calculer dans les assistants à la preuve
- utiliser les calculs dans les preuves

on peut :

- implémenter une bibliothèque d'arithmétique réelle exacte

pour avoir des **réels concrets**

Arithmétique réelle exacte certifiée

“What is the point in generating arbitrarily accurate answers to questions involving real arithmetic, if these answers cannot be relied upon?”

D. Lester

Implémentations

PVS et les suites rapides de Cauchy [Les08]

Algorithmes

le réel x est représenté par une fonction $c_x : \mathbb{N} \rightarrow \mathbb{Z}$

$$\forall n, \left| x - \frac{c_x(n)}{2^n} \right| < 2^{-n}$$

$$c_{\frac{1}{3}} = \left\lfloor \frac{2^n}{3} \right\rfloor \text{ ou } c_{\frac{1}{3}} = \left\lceil \frac{2^n}{3} \right\rceil$$

PVS et les suites rapides de Cauchy [Les08]

Algorithmes

le réel x est représenté par une fonction $c_x : \mathbb{N} \rightarrow \mathbb{Z}$

$$\forall n, \left| x - \frac{c_x(n)}{2^n} \right| < 2^{-n}$$

$$c_{\frac{1}{3}} = \left\lfloor \frac{2^n}{3} \right\rfloor \text{ ou } c_{\frac{1}{3}} = \left\lceil \frac{2^n}{3} \right\rceil$$

algorithmes : addition

$$(c_x \oplus c_y)(p) = \left\lfloor \frac{c_x(p+2) + c_y(p+2)}{4} \right\rfloor$$

PVS et les suites rapides de Cauchy [Les08]

Certification

$c_x, c_y : \text{cauchy_real}$

$x, y : \mathbb{R}$

$\text{cauchy_prop}(x, c_x) = \forall p \in \mathbb{N}, c_x(p) - 1 < x2^p < c_x(p) + 1$

PVS et les suites rapides de Cauchy [Les08]

Certification

$c_x, c_y : \text{cauchy_real}$

$x, y : \mathbb{R}$

$\text{cauchy_prop}(x, c_x) = \forall p \in \mathbb{N}, c_x(p) - 1 < x2^p < c_x(p) + 1$

add_correct: LEMMA

$\text{cauchy_prop}(x, c_x) \wedge \text{cauchy_prop}(y, c_y) \Rightarrow$
 $\text{cauchy_prop}(x + y, c_x \oplus c_y)$

PVS et les suites rapides de Cauchy [Les08]

Certification

$c_x, c_y : \text{cauchy_real}$

$x, y : \mathbb{R}$

$\text{cauchy_prop}(x, c_x) = \forall p \in \mathbb{N}, c_x(p) - 1 < x2^p < c_x(p) + 1$

$\text{add_correct} : \text{LEMMA}$

$\text{cauchy_prop}(x, c_x) \wedge \text{cauchy_prop}(y, c_y) \Rightarrow$
 $\text{cauchy_prop}(x + y, c_x \oplus c_y)$

bibliothèque : opérations de base, constantes de base, racine carrée, fonctions trigonométriques, logarithme, exponentielle

Coq et les fonctions régulières de rationnels [OCo08]

Algorithmes

le réel x est représenté par une fonction $r_x : \mathbb{Q}^+ \rightarrow \mathbb{Q}$

$$\forall \varepsilon_1 \varepsilon_2, |r_x(\varepsilon_1) - r_x(\varepsilon_2)| \leq \varepsilon_1 + \varepsilon_2$$

Coq et les fonctions régulières de rationnels [OCo08]

Algorithmes

le réel x est représenté par une fonction $r_x : \mathbb{Q}^+ \rightarrow \mathbb{Q}$

$$\forall \varepsilon_1 \varepsilon_2, |r_x(\varepsilon_1) - r_x(\varepsilon_2)| \leq \varepsilon_1 + \varepsilon_2$$

- avec ces fonctions régulières on construit \mathbb{R} comme la complétion de \mathbb{Q}
- la complétion est une monade
- les fonctions uniformément continues sur les rationnels sont remontées en fonctions sur les réels

Coq et les fonctions régulières de rationnels [OCo08]

Certification

isomorphes à une implémentation abstraite des réels :

Φ : réels abstraits \rightarrow réels concrets

$$\Phi(f_A(x)) = f_C(\Phi(x))$$

Coq et les fonctions régulières de rationnels [OCo08]

Certification

isomorphes à une implémentation abstraite des réels :

Φ : réels abstraits \rightarrow réels concrets

$$\Phi(f_A(x)) = f_C(\Phi(x))$$

bibliothèque : opérations de base, constantes de base, racine carrée, fonctions trigonométriques, logarithme, exponentielle

Coq et les suites infinies de chiffres [Jul08]

Représentation

le réel $x \in [-1, 1]$ représenté comme une suite infinie de chiffres signés en base β

$$\llbracket s_x \rrbracket_\beta = \llbracket c_1 :: c_2 :: c_3 :: \dots \rrbracket_\beta = \sum_{i=1}^{\infty} \frac{c_i}{\beta^i}; \quad -\beta < c_i < \beta$$

$$\llbracket c_1 :: \overline{s_x} \rrbracket_\beta = \frac{c_1 + \llbracket s_x \rrbracket_\beta}{\beta}$$

$$\frac{1}{3} = 0.333\dots = \llbracket 3 :: 3 :: 3 \dots \rrbracket_{10} = \llbracket 4 :: -7 :: 4 :: -7 \dots \rrbracket_{10}$$

Coq et les suites infinies de chiffres [Jul08]

Algorithmes : addition

contraintes :

- $x, y \in [-1, 1] \Rightarrow x + y \in [-2, 2]$
- algorithmes adaptés pour les suites infinies (co-récursifs)

Coq et les suites infinies de chiffres [Jul08]

Algorithmes : addition

contraintes :

- $x, y \in [-1, 1] \Rightarrow x + y \in [-2, 2]$
- algorithmes adaptés pour les suites infinies (co-récursifs)

idée : calculer $\frac{x+y+r}{\beta}$, $r \in \{-\beta + 2, \dots, \beta - 2\}$

Coq et les suites infinies de chiffres [Jul08]

Algorithmes : addition

contraintes :

- $x, y \in [-1, 1] \Rightarrow x + y \in [-2, 2]$
- algorithmes adaptés pour les suites infinies (co-récursifs)

idée : calculer $\frac{x+y+r}{\beta}$, $r \in \{-\beta + 2, \dots, \beta - 2\}$

- regarder le premier chiffre de x et de y

$$\frac{\frac{x_1+x'}{\beta} + \frac{y_1+y'}{\beta} + r}{\beta} = \frac{\frac{x_1+y_1}{\beta} + r + \frac{x'+y'}{\beta}}{\beta}$$

Coq et les suites infinies de chiffres [Jul08]

Algorithmes : addition

contraintes :

- $x, y \in [-1, 1] \Rightarrow x + y \in [-2, 2]$
- algorithmes adaptés pour les suites infinies (co-récursifs)

idée : calculer $\frac{x+y+r}{\beta}$, $r \in \{-\beta + 2, \dots, \beta - 2\}$

- regarder le premier chiffre de x et de y

$$\frac{\frac{x_1+x'}{\beta} + \frac{y_1+y'}{\beta} + r}{\beta} = \frac{\frac{x_1+y_1}{\beta} + r + \frac{x'+y'}{\beta}}{\beta}$$

- calculer $q \in \{-1, 0, 1\}$, $r' \in \{-\beta + 2, \dots, \beta - 2\}$

$$x_1 + y_1 = q \times \beta + r'$$

Coq et les suites infinies de chiffres [Jul08]

Algorithmes : addition

contraintes :

- $x, y \in [-1, 1] \Rightarrow x + y \in [-2, 2]$
- algorithmes adaptés pour les suites infinies (co-récursifs)

idée : calculer $\frac{x+y+r}{\beta}$, $r \in \{-\beta + 2, \dots, \beta - 2\}$

- regarder le premier chiffre de x et de y

$$\frac{\frac{x_1+x'}{\beta} + \frac{y_1+y'}{\beta} + r}{\beta} = \frac{\frac{x_1+y_1}{\beta} + r + \frac{x'+y'}{\beta}}{\beta}$$

- calculer $q \in \{-1, 0, 1\}$, $r' \in \{-\beta + 2, \dots, \beta - 2\}$

$$x_1 + y_1 = q \times \beta + r'$$

- retourner $(r + q) :: \frac{x'+y'+r'}{\beta}$

Coq et les suites infinies de chiffres [Jul08]

Certification

$$\llbracket c_1 :: \overline{s_x} \rrbracket_\beta = \frac{c_1 + \llbracket s_x \rrbracket_\beta}{\beta}$$

represents (s_x, x) :=

$\forall s_x x c_1, -\beta < c_1 < \beta, -1 \leq x \leq 1, \text{ represents } s_x x \Rightarrow$
 $\Rightarrow \text{ represents } (c_1 :: s_x) \frac{c_1+x}{\beta}.$

Theorem Sadd_correct: $\forall s_x s_y x y,$
 $\text{ represents } s_x x \rightarrow \text{ represents } s_y y \rightarrow$
 $\text{ represents } (s_x \oplus s_y) (x + y).$

Coq et les suites infinies de chiffres [Jul08]

Certification

$$\llbracket c_1 :: \overline{s_x} \rrbracket_\beta = \frac{c_1 + \llbracket \overline{s_x} \rrbracket_\beta}{\beta}$$

represents (s_x, x) :=

$\forall s_x x c_1, -\beta < c_1 < \beta, -1 \leq x \leq 1, \text{represents } s_x x \Rightarrow$
 $\Rightarrow \text{represents } (c_1 :: s_x) \frac{c_1 + x}{\beta}.$

Theorem Sadd_correct: $\forall s_x s_y x y,$
 $\text{represents } s_x x \rightarrow \text{represents } s_y y \rightarrow$
 $\text{represents } (s_x \oplus s_y) (x + y).$

bibliothèque : opérations de base, constantes de base, racine carrée, sinus, cosinus

Recette

- prendre des algorithmes pas trop compliqués pour les calculs
- relier les algorithmes à une implémentation abstraite des réels
- faire des calculs
 - pas trop rapides
 - bénéficiant de propriétés prouvées sur les réels abstraits

Méthodes numériques

La méthode de Newton

Définition :

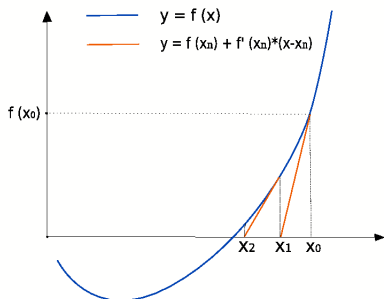
- $x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$

Propriétés :

- convergence vers la racine de la fonction f
- vitesse de convergence
- unicité locale de la racine
- stabilité locale

Dans un assistant à la preuve:

- exprimer ces propriétés
- implémenter des calculs efficaces



Newton dans un assistant à la preuve

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$$

- jolies **propriétés** prouvées sur les **réels abstraits**
- **calculs** sur les **réels concrets**
- relier les algorithmes

represents $\text{Newton}_C(f_C, x_C, n)$ $\text{Newton}_A(f_A, x_A, n)$

- récupérer les **propriétés** sur les **réels concrets** calculés

Conclusions

Que peuvent apporter les bibliothèques de calcul exact aux assistants à la preuve ?

- puissance de calcul
- preuve par calcul
- étude des méthodes numériques

Que peuvent apporter les assistants à la preuve aux bibliothèques de calcul exact ?

- certification du calcul

Références

- Les08** Lester, David. *Real Number Calculations and Theorem Proving*. TPHOLs 2008, Springer
- OC08** O'Connor, Russel. *Certified Exact Transcendental Real Number Computation in Coq*. TPHOLs 2008, Springer
- Jul08** Julien, Nicolas. *Certified Exact Real Arithmetic Using Co-induction in Arbitrary Integer Base*. FLOPS 2008, Springer