Vérification formelle d'arithmétique réelle exacte

Nicolas Julien

Maître de stage : Yves Bertot
INRIA Sophia, projet Marelle

12 Juin 2006

Plan

Plan

Utilisation usuelle des réels

Nombres flottants (norme IEEE 754)

- Calculs efficaces
- Représentation compacte

Mais

- En fait un sous-ensemble fini de $\mathbb{Q}$
- On manipule souvent des approximations
- Addition non associative
- Accumulation d'arrondis parfois conséquente

Arithmétique réelle exacte

- Fournit des résultats sûrs avec une précision arbitraire
- Nécessite une représentation exacte des réels
- Calculs moins efficaces, plus de place en mémoire
- Notre approche pour garantir les résultats :

Preuve formelle des algorithmes de calcul

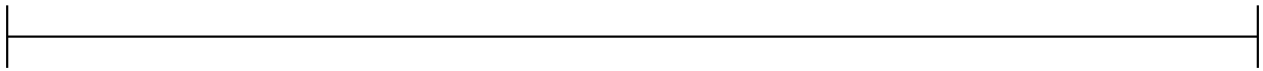
Plan

Représentation des réels

- Un réel r de $[-1, 1]$ en base β
- Une séquence infinie d_n de chiffres signés de β
- $$r = \sum_{i=1}^{\infty} \frac{d_i}{\beta^i}$$
- avec $-\beta < d_i < \beta$,
- En base 10, $\frac{1}{3}$: 33333333...

Représentation des réels

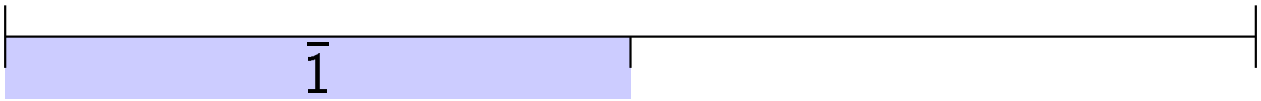
- On peut interpréter les d_i comme des fonctions qui transforment les intervalles
- Par ex pour la base 2



- Préfixe de taille k : approximation de taille $\frac{1}{\beta^k}$
- $d_1\, d_2\, d_3\, d_4\, d_5 \ldots \in [-1, 1]$

Représentation des réels

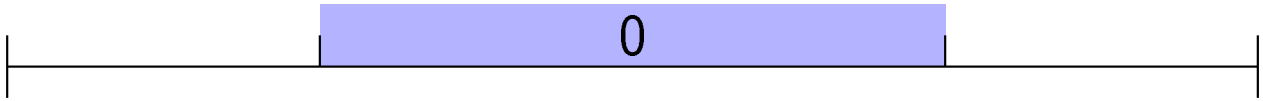
- On peut interpréter les d_i comme des fonctions qui transforment les intervalles
- Par ex pour la base 2



- Préfixe de taille k : approximation de taille $\frac{1}{\beta^k}$
- $d_1 d_2 d_3 d_4 d_5 \ldots \in [-1, 1]$

Représentation des réels

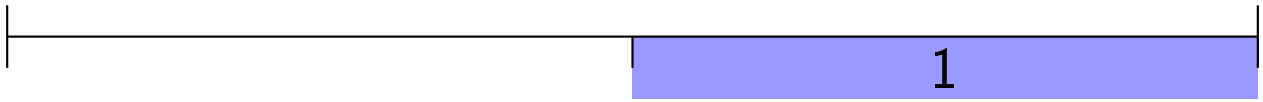
- On peut interpréter les d_i comme des fonctions qui transforment les intervalles
- Par ex pour la base 2



- Préfixe de taille k : approximation de taille $\frac{1}{\beta^k}$
- $d_1\, d_2\, d_3\, d_4\, d_5 \ldots \in [-1, 1]$

Représentation des réels

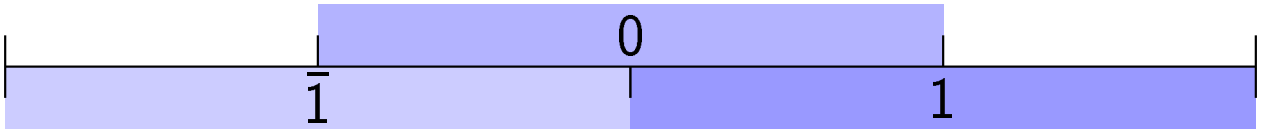
- On peut interpréter les d_i comme des fonctions qui transforment les intervalles
- Par ex pour la base 2



- Préfixe de taille k : approximation de taille $\frac{1}{\beta^k}$
- $d_1\, d_2\, d_3\, d_4\, d_5 \ldots \in [-1, 1]$

Représentation des réels

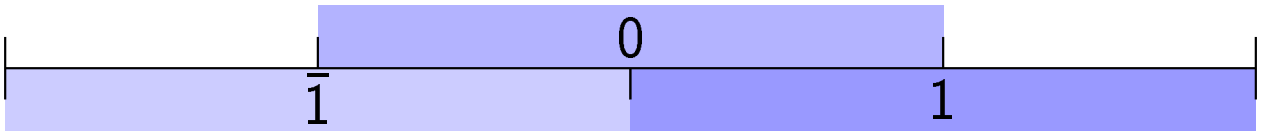
- On peut interpréter les d_i comme des fonctions qui transforment les intervalles
- Par ex pour la base 2



- Préfixe de taille k : approximation de taille $\frac{1}{\beta^k}$
- $d_1 d_2 d_3 d_4 d_5 \ldots \in [-1, 1]$

Représentation des réels

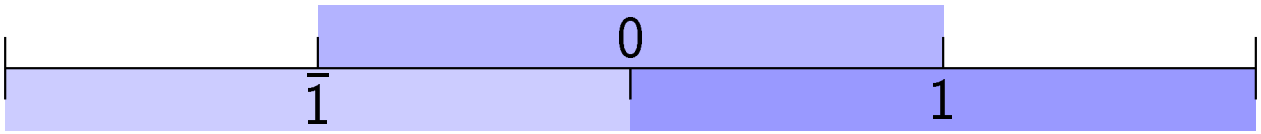
- On peut interpréter les d_i comme des fonctions qui transforment les intervalles
- Par ex pour la base 2



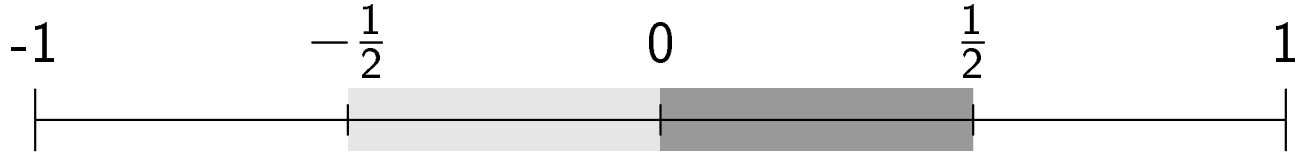
- Préfixe de taille k : approximation de taille $\frac{1}{\beta^k}$
- $0 d_2 d_3 d_4 d_5 \ldots \in [-\frac{1}{2}, \frac{1}{2}]$

Représentation des réels

- On peut interpréter les d_i comme des fonctions qui transforment les intervalles
- Par ex pour la base 2

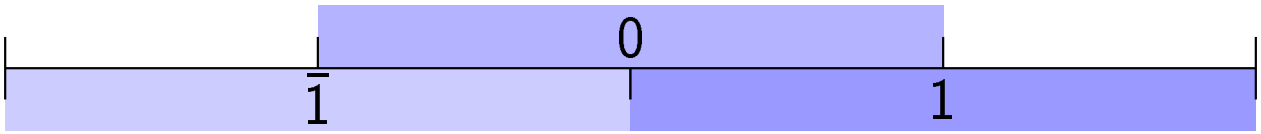


- Préfixe de taille k : approximation de taille $\frac{1}{\beta^k}$
- $01d_3d_4d_5\ldots \in [0, \frac{1}{2}]$

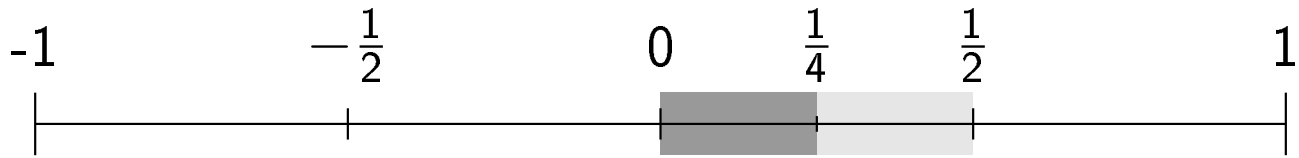


Représentation des réels

- On peut interpréter les d_i comme des fonctions qui transforment les intervalles
- Par ex pour la base 2

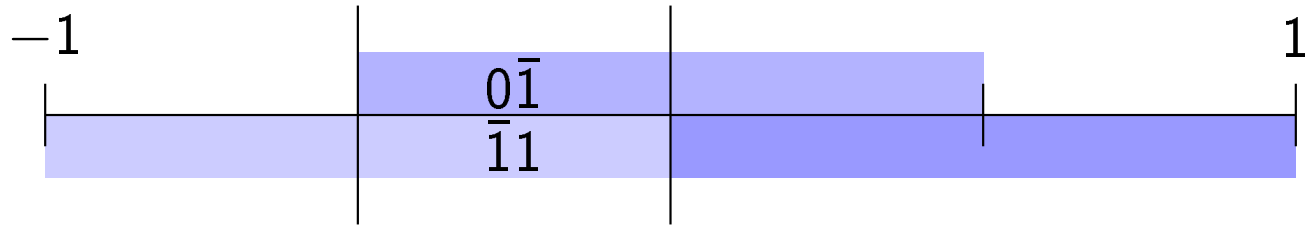


- Préfixe de taille k : approximation de taille $\frac{1}{\beta^k}$
- $01\bar{1}d_4d_5\ldots \in [0, \frac{1}{4}]$

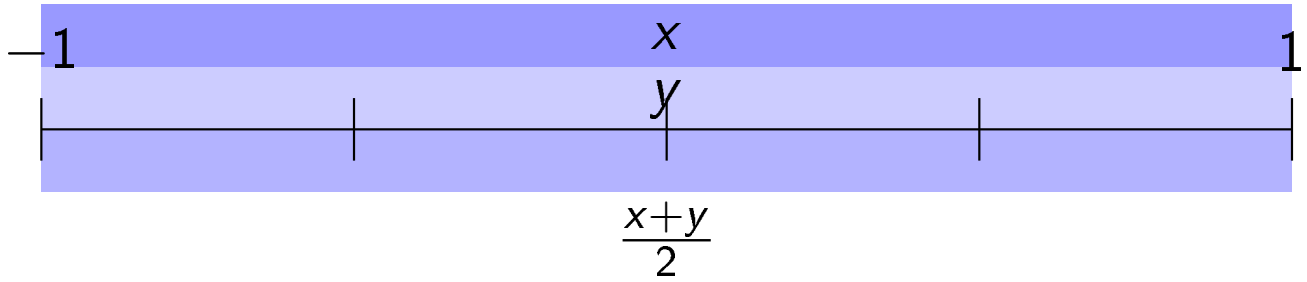


Méthode de calcul

- Représentation redondante



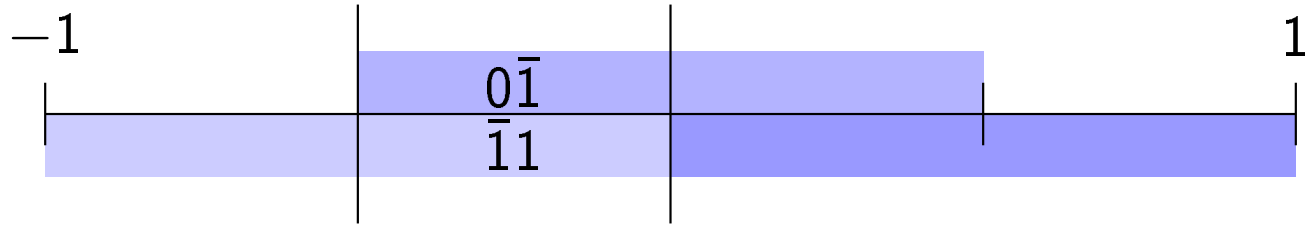
- Calculer un encadrement du résultat



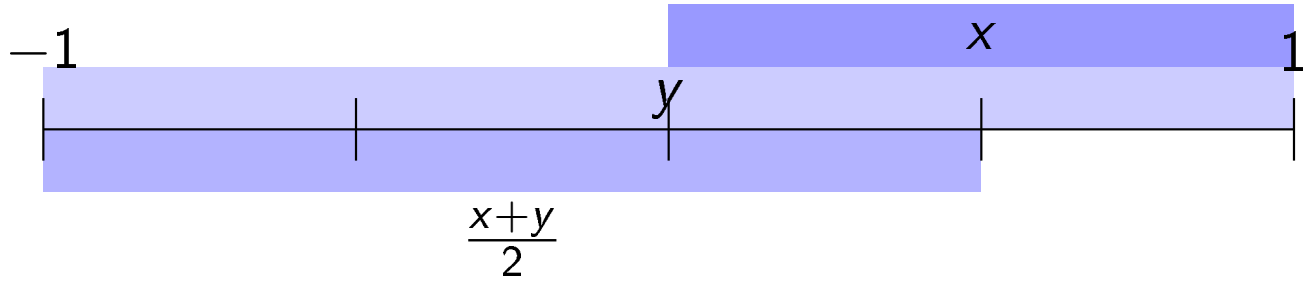
- $x \in [-1,1], y \in [-1,1] \Rightarrow \frac{x+y}{2} \in [-1,1]$

Méthode de calcul

- Représentation redondante



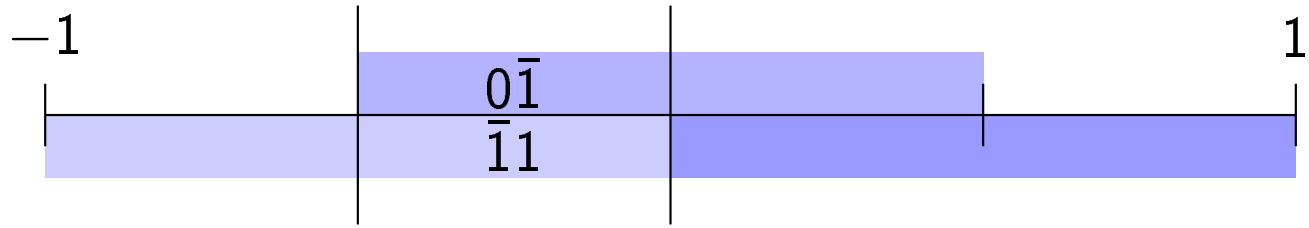
- Calculer un encadrement du résultat



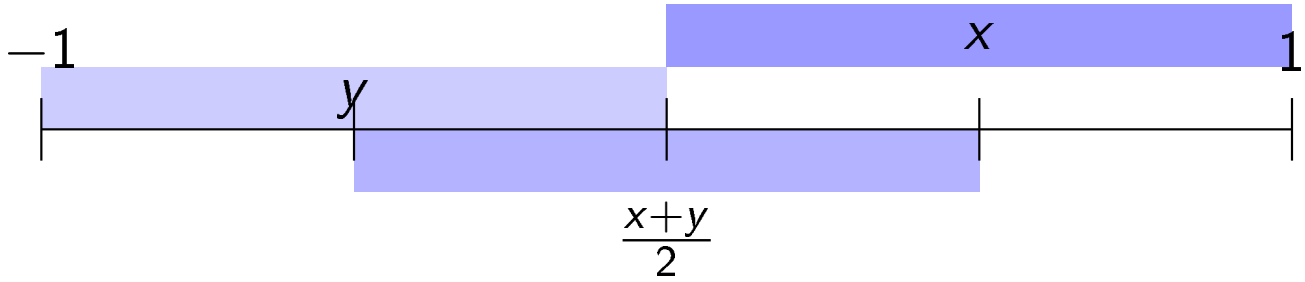
- $x \in [0,1], y \in [-1,1] \Rightarrow \frac{x+y}{2} \in [-1, \frac{1}{2}]$

Méthode de calcul

- Représentation redondante



- Calculer un encadrement du résultat



- $x \in [0,1], y \in [-1,0] \Rightarrow \frac{x+y}{2} \in [-\frac{1}{2}, \frac{1}{2}]$ mais $\frac{x+y}{2} \geq 0$???

Plan

Présentation de Coq

- Vérification de preuves mathématiques
- Calcul des constructions inductives
- Langage fonctionnel typé
- Co-induction

Co-induction

- Définition de type d'objets infinis

```
CoInductive stream (A: Set) :=
  Cons :  A → stream A → stream A.
```

- Fonctions co-récursives pour construire les objets infinis

```
CoFixpoint zero : stream ℤ := Cons 0 zero
```

- Preuves infinies : preuves par co-induction
- Tactique `cofix`

Relation représentation $\longrightarrow$ nombres réels

- Principe
  - Si la séquence infinie s représente le réel r de $[-1, 1]$
  - Et si k est un chiffre de β
  - Alors la séquence constituée de k suivie de s représente $\frac{k+r}{\beta}$
- En Coq

```
CoInductive represents (b : ℤ): stream ℤ → ℝ → Prop :=
  | rep : ∀ (s : stream ℤ) (r : ℝ) (k : ℤ),
    represents b s r →
   -1 ≤ r ≤ 1 →
    -b < k < b →
    represents b (Cons k s) (k + r)/b.
```

- Formellement

$$\sum_{i=1}^{\infty} \frac{d_i}{\beta^i} = \frac{d_1 + \sum_{i=1}^{\infty} \frac{d_{i+1}}{\beta^i}}{\beta}$$

Preuve de correction

- Mettre en relation le résultat d'un algorithme avec celui de la fonction mathématique calculée

Notre représentation	s_1	s_2	$algo_f(s_1, s_2)$
	$\downarrow$	$\downarrow$	$\downarrow$
Objets mathématiques	r_1	r_2	$f(r_1, r_2)$

- Par exemple l'addition

```
Theorem add_correct :
  ∀ (b : ℤ) (s1 s2: stream ℤ) (r1 r2 : ℝ),
    represents b s1 r1 →
    represents b s2 r2 →
    -1<= r1 + r2 <= 1 →
    represents b (add b s1 s2) (r1 + r2).
```

État de l'art

- Avizienis 61 :
  - chiffres signés, parallélisation
  - preuves papiers
- Di Gianantonio 00 :
  - chiffres $\bar{1}$, 0 et 1, addition, multiplication,
  - preuves en Coq, co-induction
- Edalat 00 :
  - base arbitraire, fonctions mathématiques usuelles
  - preuves papiers
- Bertot 06 :
  - chiffres 0, $\frac{1}{2}$ et 1, technique calcul de séries entières
  - preuves en Coq, co-induction

Plan

Mes travaux

- Extension du travail existant sur $[0, 1]$
- Adaptation du travail à l'intervalle $[-1, 1]$
- Formalisation de la base

Extensions sur $[0, 1]$

- Algorithme de soustraction
- Preuve de sa correction en Coq
- Calcul de $arctan(\frac{1}{n})$
  29 théorèmes et 1300 lignes de preuves
- Définition de $\frac{\pi}{4} = arctan(\frac{1}{2}) + arctan(\frac{1}{3})$

Adaptation à l'intervalle $[-1, 1]$

- Définition des réels sur $[-1, 1]$
- Modifications des algorithmes de calculs et des preuves
  - Addition, soustraction, opposé
  - Représentation des rationnels
  - Multiplication
  - Calcul du nombre d'Euler
  - Calcul de $\frac{\pi}{4}$

Formalisation à une base quelconque

- Redéfinitions des algorithmes et des preuves
  - Addition, soustraction, opposé
  - Représentation des rationnels
  - Multiplication (preuve non terminée)
  - Calcul du nombre d'Euler

```
CoFixpoint half_sum (b : ℤ) (x y : ℤ) : stream ℤ :=
  match (x, y) with (k1 :: x', l1 :: y') ⇒
    if (Zmod (k1 + l1) 2) = 0 (* si k1 + l1 est pair *)
     then (k1+l1)/2 ::half_sum b x' y'
     else match x' with k2 :: x'' ⇒
       if k2 ≤ −1
         then (k1+l1−1)/2 ::half_sum b (k2 + 2b :: x'') y'
         else if 1 ≤ k2
           then (k1+l1+1)/2 ::half_sum b (k2 − 2b) :: x'' y'
           else match y' with l2 :: y'' ⇒
             if l2 ≤ −1
               then (k1+l1−1)/2 ::half_sum b x' (l2 + 2b) :: y''
               else (k1+l1+1)/2 ::half_sum b (k2 − b) :: x'' (l2 − b) :: y''
 end   end   end.
```

Plan

Perspectives

- Définir les séries formelles
- Définir l'inverse et la division
- Amélioration de la technique des séries entières
- Programmation paresseuse
- Combinaison induction co-induction