ADT Coq

Bibliothèques en arithmétiques flottantes

Sylvie Boldo & Guillaume Melquiond

11 décembre 2008

INSTITUT NATIONAL
DE RECHERCHE
EN INFORMATIQUE
ET EN AUTOMATIQUE

INRIA

centre de recherche SACLAY - ÎLE-DE-FRANCE

Les flottants et leur formalisation (Daumas, Rideau, Théry)

Flottant = paire d'entiers signés (mantisse, exposant)

$$(n, e) \in \mathbb{Z}^2$$

Les flottants et leur formalisation (Daumas, Rideau, Théry)

Flottant = paire d'entiers signés (mantisse, exposant)
associé à une valeur réelle

$$(n, e) \in \mathbb{Z}^2 \quad \hookrightarrow \quad n \times \beta^e \in \mathbb{R}$$

Les flottants et leur formalisation (Daumas, Rideau, Théry)

Flottant = paire d'entiers signés (mantisse, exposant)
associé à une valeur réelle

$$(n, e) \in \mathbb{Z}^2 \hookrightarrow n \times \beta^e \in \mathbb{R}$$

1.00010_2 E 4	$\mapsto$	$(100010_2, -1)_2$	$\hookrightarrow$	17
IEEE-754		"significant" de la 754R		valeur réelle

$\Rightarrow$ flottant normal, subnormal, ~~overflow~~

La bibliothèque PFF/FP2

- Initiée en 2001 par l'ARC AOC (Arénaire, Lemme, Polka)
- Par Laurent Théry, Laurence Rideau (puis moi)
- Environ 60 000 lignes de Coq (dont 16 000 dans les contribs)
- Utilisée par la plateforme Why pour les OP Coq des programmes numériques

- Beaucoup de calculs sur $\mathbb{R}$
- Beaucoup de coercions $(\mathbb{N}, \mathbb{Z}, \mathbb{F}, \mathbb{R})$

Automatisations insuffisantes

- $\frac{1}{2} \leq 1$
- `Rle` et `Rge` ne sont pas égaux en termes d'automatisation. (Idem pour `Rlt` et `Rgt`).

Empilement de coercions

- `INR_IZR_INZ` pour prouver $n = n$.
- Je ne veux pas savoir le nom des coercions.

  Pourrait-on avoir des coercions affaiblies
  pour écrire `n%R` avec `n:nat` ?

Théorèmes manquants

- `Rmult_minus_distr_r` : $(a-b)*c = a*c - b*c$.
- `Rmult_le_compat_neg_r` : $a \leq 0 \Rightarrow b \leq c \Rightarrow c*a \leq b*a$
- `Rplus_le_reg_r` : $b+a \leq c+a \Rightarrow b \leq c$
- `Rmult_eq_reg_r` : $b \times a = c \times a \Rightarrow a \neq 0 \Rightarrow b = c$.
- `Rmult_eq_compat_r` : $b = c \Rightarrow b \times a = c \times a$.
- `Rmin_Rle` : $\min(b,c) \leq a \Leftrightarrow b \leq a \vee c \leq a$.
- `Rabs_def1_le` : $a \leq b \Rightarrow -b \leq a \Rightarrow |a| \leq b$.
- `Rabs_def2_le` : $|a| \leq b \Rightarrow -b \leq a \leq b$.

Théorèmes mal nommés

Erreurs de nommages :

- `Rplus_lt_reg_r` : $a + b < a + c \Rightarrow b < c$.
- `RRle_abs`
- `Rmult_ge_compat` et `Rmult_le_compat` sont identiques.

Théorèmes ambigus :

- $a < b \Rightarrow \mathrm{IZR}(a) < \mathrm{IZR}(b)$: `lt_IZR` ? `IZR_lt` ?

Définitions pénibles

- `Pcompare : positive -> positive -> comparison -> comparison`.
- `Rminus` et `Rdiv` ne sont pas des notations.

Réels entiers

`5%R` n'est convertible ni à `INR 5` ni à `IZR 5`.

- `INR 5` $\equiv$ `IZR 5` $\equiv$ `(2 + 1 + 1 + 1)%R`.

Exercice : prouver `(2 < 5)%R`.

Réels entiers

5%R n'est convertible ni à `INR 5` ni à `IZR 5`.

- `INR 5` ≡ `IZR 5` ≡ `(2 + 1 + 1 + 1)%R`.

Exercice : prouver `(2 < 5)%R`.

```
Fixpoint P2R (p : positive) :=
  match p with
  | xH => 1%R
  | xO xH => 2%R
  | xO t => (2 * P2R t)%R
  | xI xH => 3%R
  | xI t => (1 + 2 * P2R t)%R
  end.

Lemma Z2R_IZR :
  forall n, Z2R n = IZR n.
```

Comparaisons

Pour $\mathbb{R}$:

```
Parameter Rlt : R -> R -> Prop.
Axiom total_order_T : forall r1 r2:R,
  {r1 < r2} + {r1 = r2} + {r1 > r2}.
Axiom Rlt_asym : forall r1 r2:R,
  r1 < r2 -> ~ r2 < r1.
Definition Rle (r1 r2:R) : Prop :=
  (r1 < r2)%R \/ r1 = r2.
```

Comparaisons

Pour $\mathbb{R}$:

```
Parameter Rlt : R -> R -> Prop.
Axiom total_order_T : forall r1 r2:R,
  {r1 < r2} + {r1 = r2} + {r1 > r2}.
Axiom Rlt_asym : forall r1 r2:R,
  r1 < r2 -> ~ r2 < r1.
Definition Rle (r1 r2:R) : Prop :=
  (r1 < r2)%R \/ r1 = r2.
```

Pour $\mathbb{Z}$:

```
Definition Zcompare := ...
Definition Zlt (x y:Z) := (Zcompare x y) = Lt.
Definition Zle (x y:Z) := (Zcompare x y) <> Gt.
Lemma Zcompare_Eq_iff_eq : forall n m:Z,
  (n ?= m) = Eq <-> n = m.
Lemma Zcompare_Gt_Lt_antisym : forall n m:Z,
  (n ?= m) = Gt <-> (m ?= n) = Lt.
```

Comparaisons

Idéalement,

```
Parameter Rcompare : R -> R -> comparison.
Definition Rlt x y := (Rcompare x y) = Lt.
Definition Rle x y := (Rcompare x y) <> Gt.
Axiom Rcompare_Eq_iff_eq :
  forall x y, Rcompare x y = Eq <-> x = y.
Axiom Rcompare_Gt_Lt_antisym : forall x y,
  Rcompare x y = Gt <-> Rcompare y x = Lt.
Lemma total_order_T : forall x y,
  { Rlt x y } + { x = y } + { Rgt x y }.
Lemma Rlt_asym :
  forall x y, Rlt x y -> not (Rlt y x).
```

Comparaisons

Idéalement,

```
Parameter Rcompare : R -> R -> comparison.
Definition Rlt x y := (Rcompare x y) = Lt.
Definition Rle x y := (Rcompare x y) <> Gt.
Axiom Rcompare_Eq_iff_eq :
  forall x y, Rcompare x y = Eq <-> x = y.
Axiom Rcompare_Gt_Lt_antisym : forall x y,
  Rcompare x y = Gt <-> Rcompare y x = Lt.
Lemma total_order_T : forall x y,
  { Rlt x y } + { x = y } + { Rgt x y }.
Lemma Rlt_asym :
  forall x y, Rlt x y -> not (Rlt y x).
```

Bonus :

```
Lemma Zcompare_Rcompare : forall x y,
  Zcompare x y = Rcompare (IZR x) (IZR y).
```

Analyse

- Supprimer `derive_pt` et `D_in`.
- Ajouter arctan.
- Étendre quelques théorèmes :
  - tan est croissante, mais seulement sur $[-\frac{\pi}{4}, \frac{\pi}{4}]$,
  - $\sin(x + k2\pi) = \sin x$, mais seulement pour $k \geq 0$.
- Simplifier la manipulation des séries entières.

Comment j'énonce mes théorèmes

Propriétés locales : (introuvable dans Coq)

```
forall f x y,
(y < f x)%R ->
continuity_pt f x ->
locally_true x (fun u => (y < f u)%R).
```

Domaines connexes : (disponible seulement sur $\mathbb{R}$ entier)

```
forall f f' dom,
connected dom ->
( forall x, dom x ->
  derivable_pt_lim f x (f' x) /\
  (f' x <= 0)%R ) ->
forall u v, dom u -> dom v ->
(u <= v)%R -> (f v <= f u)%R.
```

Option $\mathbb{R}$

```
Definition Xinv x :=
  match x with
  | Xreal u =>
    if is_zero u then Xnan else Xreal (/ u)
  | _ => Xnan
  end.

Theorem Xderive_pt_inv :
  forall f x y',
  Xderive_pt f x y' ->
  Xderive_pt (fun x => Xinv (f x)) x
             (Xneg (Xdiv y' (Xsqr (f x)))).
```

Autrement dit : Si la dérivée de f en x vaut y',
la dérivée de $1/f$ en x vaut $-y'/y^2$ même si $y = f(x) = 0$.