Construction des nombres algébriques réels en Coq

Cyril Cohen

INRIA Saclay – Île-de-France
LIX École Polytechnique
INRIA Microsoft Research Joint Centre
cohen@crans.org

6 février 2012

Pourquoi les nombres algébriques réels ?

- Corps strictement compris entre $\mathbb{Q}$ et $\mathbb{R}$
- Instance de corps réel clos, dénombrable et avec comparaison décidable
- Utile dans la formalisation du théorème de Feit-Thompson (projet Mathematical Components)
- Objet intéressant pour faire de la géométrie algébrique réelle et du calcul formel

Définition usuelle des réels algébriques

Les nombres algébriques sont les racines de polynômes à coefficients dans $\mathbb{Q}$

Wishlist

- Un algorithme de comparaison (égalité + ordre)
- La procédure de décision de l'égalité reflète l'égalité de Leibniz
- Le type (ou le sétoïde) est dénombrable
- Des opérations arithmétiques + leurs propriétés
  Corps ordonné
- La propriété des valeurs intermédiaires pour les polynômes

L'approche "Top-down"

- On part de nombres réels
- On se restreint aux racines de polynômes à coefficients dans $\mathbb{Q}$

Les réels de Cauchy

Représentation :

- Une suite $(x_n)_{n \in \mathbb{N}}$
- Un module de convergence $m : \mathbb{Q} \to \mathbb{N}$
  tel que : $\forall \varepsilon\ i\ j,\ m(\varepsilon) < i, j \to |x_i - x_j| < \varepsilon$

La théorie des réels de Cauchy

- Une définition de l'égalité $\equiv$ (non décidable)

$$\bar{x} \equiv \bar{y} \quad \Longleftrightarrow \quad |x_n - y_n| \underset{n\infty}{\longrightarrow} 0$$

- Les réels de Cauchy forment un Setoide
- Les opérations arithmétiques sont des morphismes
- On a les propriétés de corps ordonné

L'inverse d'un réel de Cauchy

Pour produire l'inverse de $\bar{x}$, on doit savoir borner

$$\left|\frac{1}{x_n} - \frac{1}{x_m}\right|$$

grâce à un module de Cauchy. Or :

$$\left|\frac{1}{x_n} - \frac{1}{x_m}\right| = \left|\frac{x_m - x_n}{x_n x_m}\right|$$

$\Rightarrow$ Il suffit de minorer x_n.

$\Rightarrow$ Il suffit d'avoir une preuve de $\bar{x} \neq 0$

```
inv_creal :
  forall x : creal -> (x != 0) -> creal
```

Représentation “Top-down”

On définit le type `algcreal` des algébriques réels de Cauchy :

- Un réel de Cauchy $\bar{x}$
- Un polynôme $P \in \mathbb{Q}[X]$ tel que $P(\bar{x}) \equiv 0$

Propriétés des algébriques réels de Cauchy

- La comparaison devient décidable (grâce au polynôme)
- On transfère toutes les opérations depuis les réels de Cauchy

$\rightarrow$ Il faut reconstruire le polynôme pour chaque opération (grâce à un calcul de résultant)

L'inverse d'un réel **algébrique** de Cauchy

Il n'est plus nécessaire de fournir la preuve d'inégalité pour faire l'inverse.

```
Definition inv_algcreal
  (x : algcreal) : algcreal :=
match eq_algcreal_dec x (cst_algcreal 0)
   with
  | left x_eq0 => cst_algcreal 0
  | right x_neq0 => @AlgCReal
     (@inv_creal _ x_neq0) _
     (@monic_annul_creal _)
     (@root_inv_algcreal _ x_neq0)
end.
```

Wishlist

- Un algorithme de comparaison (égalité + ordre)
- La procédure de décision de l'égalité reflète l'égalité de Leibniz
- Le type (ou le sétoïde) est dénombrable
- Des opérations arithmétiques + leurs propriétés
  Corps ordonné
- La propriété des valeurs intermédiaires pour les polynômes

Wishlist

- Un algorithme de comparaison (égalité + ordre)
- La procédure de décision de l'égalité reflète l'égalité de Leibniz
- Le type (ou le sétoïde) est dénombrable
- Des opérations arithmétiques + leurs propriétés
  Corps ordonné
- La propriété des valeurs intermédiaires pour les polynômes

Approche “Bottom-up”

On représente un algébriques grâce à :

- Un polynômes de $\mathbb{Q}[X]$
- La sélection d'une racine (intervalle, approximation, ...)

Méthode de sélection choisie

On définit le type `algdom` du "domaine des algébriques réels" par :

- Un polynôme $P \in \mathbb{Q}[X]$
- Un intervalle $[c - r, c + r]$ tel que

  P change de signe et soit monotone

Méthode de sélection choisie

On définit le type `algdom` du "domaine des algébriques réels" par :

- Un polynôme $P \in \mathbb{Q}[X]$
- Un intervalle $[c - r, c + r]$ tel que P change de signe

et construit tel que P soit monotone

Encodage des algébriques de Cauchy

On construit des fonctions d'encodage et de décodage :

- `to_algdom: algcreal -> algdom`
- `to_algcreal: algdom -> algcreal`

C'est-à-dire qui vérifient :

```
forall x, to_algcreal (to_algdom x) == x
```

Transfert de la comparaison et des opérations

On déduit trivialement les opérations de `algdom` depuis celles de `algcreal` :

```
eq_algdom x y := (eq_algcreal
    (to_algcreal x)(to_algcreal y))

add_algdom x y := to_algdom (add_algcreal
    (to_algcreal x)(to_algcreal y))
```

Wishlist

- Un algorithme de comparaison (égalité + ordre)
- La procédure de décision de l'égalité reflète l'égalité de Leibniz
- Le type (ou le sétoïde) est dénombrable
- Des opérations arithmétiques + leurs propriétés
  Corps ordonné
- La propriété des valeurs intermédiaires pour les polynômes

Wishlist

- Un algorithme de comparaison (égalité + ordre)
- La procédure de décision de l'égalité reflète l'égalité de Leibniz
- Le type (ou le sétoïde) est dénombrable
- Des opérations arithmétiques + leurs propriétés
  Corps ordonné
- La propriété des valeurs intermédiaires pour les polynômes

Quotient de algdom

`eq_algdom` (noté à nouveau ==) est une relation d'équivalence décidable sur un type dénombrable

Quotient de `algdom`

`eq_algdom` (noté à nouveau ==) est une relation d'équivalence décidable sur un type dénombrable

$\Rightarrow$ On peut prendre le quotient effectif de `algdom` par cette équivalence.

Quotient de `algdom`

`eq_algdom` (noté à nouveau ==) est une relation d'équivalence décidable sur un type dénombrable

$\Rightarrow$ On peut prendre le quotient effectif de `algdom` par cette équivalence.

$\Rightarrow$ Cela donne le type `realalg` des nombres algébriques réels exacts.

À propos du choix

Si `T` est dénombrable et `P : T -> Prop` est décidable, il existe une fonction de **choix unique** :

```
xchoose : (exists x : T, P x) -> T
```

Construction “inlinée” de realalg

Choix d'un élément canonique :

```
((P y):= (fun x => y == x))
```

```
Lemma exists_eq (y : algdom) :
    exists x : algdom, y == x
Definition canon (y : algdom) =
    xchoose (exists_eq y)
```

Definition des algébriques :

```
Definition realalg :=
    {x : algdom | canon x == x}
```

Structure de `realalg`

- On transfère la comparaison et les opérations arithmétiques de `algdom` vers `realalg`
  - On sait déjà qu'elle sont un morphisme pour le sétoïde `algdom`
  - Le transfert de la procédure de décision de l'égalité donne une procédure qui reflète l'égalité de Leibniz
- On transfère les propriétés des opérations (vérifiées dans `algcreal`)

Structure de `realalg`

- On transfère la comparaison et les opérations arithmétiques de `algdom` vers `realalg`
  - On sait déjà qu'elle sont un morphisme pour le sétoïde `algdom`
  - Le transfert de la procédure de décision de l'égalité donne une procédure qui reflète l'égalité de Leibniz
- On transfère les propriétés des opérations (vérifiées dans `algcreal`)

$\Rightarrow$ `realalg` possède une structure de corps réel clos avec comparaison décidable

Wishlist

- Un algorithme de comparaison (égalité + ordre)
- La procédure de décision de l'égalité reflète l'égalité de Leibniz
- Le type (ou le sétoïde) est dénombrable
- Des opérations arithmétiques + leurs propriétés
  Corps ordonné
- La propriété des valeurs intermédiaires pour les polynômes

Wishlist

- Un algorithme de comparaison (égalité + ordre)
- La procédure de décision de l'égalité reflète l'égalité de Leibniz
- Le type (ou le sétoïde) est dénombrable
- Des opérations arithmétiques + leurs propriétés
  Corps ordonné
- La propriété des valeurs intermédiaires pour les polynômes

Utilisation pratique

- Pas approprié pour faire des calculs efficaces (Algorithmes naïf sur des structures naïves)
- Le but est de faire des preuves constructives :
  - en implémentant l'interface de corps réel clos
  - pour des preuves ne demandant que les réels qui sont algébriques
  - pour aider la formalisation d'une implémentation plus efficace de réels algébriques.

Conclusion

On a trois représentations :

- Une représentation pour écrire les algorithmes : `algcreal`
- Un encodage intermédiaire : `algdom`
- Une représentation pour travailler : `realalg`

Travaux futurs :

- Les algébriques complexes (extension par i)
- Une implémentation efficace `realalg_eff` à mettre en relation avec `realalg`

The End

Merci de votre attention

Des questions ?