La Tactique Gb

Stage réalisé par

Jérôme Creci

encadré par

Loïc Pottier

INRIA Sophia-Antipolis

Plan

- Introduction
- Un peu d'algèbre
- La tactique Gb
- Exemples et Performances
- Conclusion

La tactique `Ring`

- Effectue de la réécriture sur tous les anneaux
- Procédure de décision pour les égalités sur les anneaux abéliens
- Tactique limitée: par exemple

$$\forall x,\ y,\ z\ \in\ \mathbb{R} \quad x = 0\ \rightarrow\ y = z\ \rightarrow\ x + y = z$$

ne peut être prouvé par `Ring`

$\Rightarrow$ `Ring` **n'utilise pas les hypothèses du but courant**

Anneaux de polynômes

- A un anneau commutatif

- Polynôme de n variables à coefficients dans A:
  suite $(a_{\alpha_1,\ldots,\alpha_n})_{(\alpha_1,\ldots,\alpha_n)\in\mathbb{N}^n}$ d'éléments de A telle que seul un nombre fini de $a_{\alpha_1,\ldots,\alpha_n}$ est non nul

Notations:

– $P = \sum_{(\alpha_1,\ldots,\alpha_n)\in\mathbb{N}^n} a_{\alpha_1,\ldots,\alpha_n} {X_1}^{\alpha_1} \ldots {X_n}^{\alpha_n}$

– $A[X_1, ..X_n]$ ensemble des suites de n variables à coefficients dans A

Motivation

Nouvelle tactique *étendant* `Ring`:

– en considérant les termes du but et des hypothèses comme des éléments d'un anneau de polynômes

– en utilisant des résultats d'algèbre sur les anneaux de polynômes (bases de Gröbner, théorème des zéros de Hilbert)

Un peu d'algèbre: idéaux et bases de Gröbner

– **Définition**: soit A un anneau, un idéal de A est un sous-ensemble I de A qui est un sous-groupe de A pour la loi additive et qui vérifie

$$\forall i \in I,\ \forall a \in A\ :\ a.i \in I$$

– **Définition**: soit I un idéal de $A[X_1, .., X_n]$. On appelle base de Gröbner de I toute famille finie $G_1,\ ..,G_s$ telle que les monômes de tête de $G_1,\ ..,G_s$ engendrent les monômes de tête des éléments de I.

– **Prop**: tout idéal I de $A[X_1, ..., X_n]$ admet une base de Gröbner.

Le théorème des zéros de Hilbert (nullstellensat

Théorème:
Soit $I = (P_1[X_1, ..., X_n], .., P_m[X_1, ..., X_n])$ un idéal de $A[X_1, ..., X_n]$. Alors pour tout P $\in$ $A[X_1, ..., X_n]$

$$P_1[X_1, ..., X_n] = 0 \ , \ .. \ , \ P_m[X_1, ..., X_n] = 0 \quad \Longrightarrow \quad P[X_1, ..., X_n] = 0$$

$$\Updownarrow$$

$$\exists l \ tel \ que \ (P[X_1, ..., X_n])^l \in I$$

Détails de la tactique (1)

Récupérer un ensemble de polynômes:

- hypothèses de la forme $a_i = b_i$

  $\Rightarrow p_i = a_i - b_i$

- but de la forme $a = b$

  $\Rightarrow p = a - b$

$$\Rightarrow \{p_1, p_2, ..., p\}$$

But à atteindre: trouver un l et écrire p^l en fonction des p_i

Remarque:
Anneau de polynômes considéré: $A[var.\ des\ hyp.\ et\ du\ but]$ avec A le type du but

Détails de la tactique (2)

Méthode de Rabinowitsch:

– introduction d'une nouvelle variable z

– Modification l'idéal $\{p_1, .., \ p_m, \ p\}$ en un nouvel idéal J de $A[x_1, .., x_n, z]$

– Calcul de la base de Gröbner G de J

– On récupére dans G un polynôme de la forme

$$a = q_1.p_1 + ... + q_m.p_m$$

avec a une constante et $q_i \in A[x_1, .., x_n, z]$

Détail de la tactique (3)

- Calcul de $l = \ max_i(deg \ \ q_i[z])$

- Subst $[q_i, \ z, \ 1/p]$ pour tous les q_i

- On multiplie l'égalité par p^l

Résultats du travail préliminaire

- liste de polynômes $q_i^{'}$ de $A[x_1, .., x_n]$
- un entier l (nullstellensatz)
- une constante a

tel que:

$$a.p^l = q_1^{'}.p_1 + ... + q_n^{'}.p_n$$

La tactique Gb

```
Coq <
```
1 subgoal
```
   x : A
  H1 : h1[x] = g1[x]
   .
   .
  Hn : hn[x] = gn[x]
  ============================
   b[x] = c[x]
```

où x $= \{x_1, .., x_n\}$

Remarque :
On peut évidemment avoir des hypothèses non *égalitairs*.

La tactique Gb

```
Lemma Th_minus_eq:(x,y:A) x - y = 0 -> x = y.
```

```
Coq < Apply Th_minus_eq.
```

1 subgoal

```
   x : A
  H1 : h1[x] = g1[x]
   .
   .
  Hn : hn[x] = gn[x]
  ============================
   p[x] = 0
```

La tactique Gb

```
Lemma Th_pow_l:(x:A)(l:nat)  x^l = 0 -> x = 0.

Coq < Apply Th_pow_l.
```

1 subgoal

```
   x : A
  H1 : h1[x] = g1[x]
   .
   .
  Hn : hn[x] = gn[x]
  ============================
   (p[x])^l = 0
```

La tactique Gb

```
Lemma Th_mult_cte:(x,a:A) a.x = 0 -> a <> 0 -> x = 0.

Coq < Apply Th_mult_cte.
2 subgoals
   x : A
  H1 : h1[x] = g1[x]
   .
   .
  Hn : hn[x] = gn[x]
  ============================
    a.(p[x])^1 = 0

 subgoal 2 is:
  a<>0
```

La tactique Gb

```
Lemma Th_trans:(x,y,z:A) x = y -> x = z -> y = z.

Coq < Apply Th_trans with
(h1[x]-g1[x])*q1[x]+..+(hn[x]-gn[x])*qn[x].
```

3 subgoals

```
   x : A
  H1 : h1[x] = g1[x]
   .
   .
  Hn : hn[x] = gn[x]
  ============================
    a.(p[x])^l = (h1[x]-g1[x])*q1[x]+..+(hn[x]-
```

```
gn[x])*qn[x]

 subgoal 2 is:
(h1[x]-g1[x])*q1[x]+..+(hn[x]-gn[x])*qn[x] = 0

 subgoal 3 is:
   a <> 0.
```

La tactique Gb

```
Coq < Simpl;Ring.
```

2 subgoals

```
   x : A
  H1 : h1[x] = g1[x]
   .
   .
  Hn : hn[x] = gn[x]
  ============================
(h1[x]-g1[x])*q1[x]+..+(hn[x]-gn[x])*qn[x] = 0


 subgoal 2 is:
   a <> 0.
```

La tactique Gb

```
Coq < Rewrite ...
```

2 subgoals

```
   x : A
  H1 : h1[x] = g1[x]
   .
   .
  Hn : hn[x] = gn[x]
  ============================
(g1[x]-g1[x])*q1[x]+..+(gn[x]-gn[x])*qn[x] = 0

 subgoal 2 is:
   a <> 0.
```

La tactique Gb

```
Coq < Ring.
1 subgoal
   x : A
  H1 : h1[x] = g1[x]
   .
   .
  Hn : hn[x] = gn[x]
  ============================
   a <> 0.
```

La tactique Gb

Suivant l'anneau A : `Omega` ou `Discr` ou ..

```
Coq < ....
Subtree proved!
```

La tactique Gb au 30/07/03

- environ **1000** lignes de code
- prouve des buts uniquement dans **R** ou **Z**
- possibilité d'avoir des fonctions puissances *réelles* dans le but courant

Quelques exemples

```
Coq < ...
1 subgoal
   x : R
   y : R
   H : ``x*x == -3*y*y``
  H0 : ``3*x*y == 0``
  ============================
   ``x+y == 0``

Coq < Time Gb.
Subtree proved!
Finished transaction in 3 secs.
```

Quelques exemples

```
Coq < ...
```

1 subgoal

```
   x : Z
   y : Z
   z : Z
   H : ‘x*x+y*y = 0‘
  H0 : ‘2*x*y+z*z = 0‘
  H1 : ‘2*x*z+2*y*z = 0‘
  ============================
   ‘x+y+z = 0‘

Coq < Time Gb.
Subtree proved!
Finished transaction in 6 secs.
```

Quelques exemples

```
Coq < ...
1 subgoal
   x : R
   y : R
   H : ``(pow x (S (S O)))+3*(powerRZ y (Zs (Zs ZERO)))==0``
  H0 : ``3*x*y==0``
  H1 : ``(pow y (S (S (S O))))==0``
  ============================
   ``x+y == 0``

Coq < Time Gb.
Subtree proved!
Finished transaction in 2 secs.
```

Conclusion

- **Point positif :**
  - économie de temps pour prouver de nombreux théorèmes (théorie des nombres réels, théorie des entiers relatifs)
- **Point négatif :**
  - certaine lenteur lorsque les coefficients des polynômes sont trop grands

Perspectives

- **Gb** pour tous les anneaux intègres (`Add Ring...`)

- Coefficients dans le type de l'anneau considéré (coefficients fractionnaires)