# Gb: une procédure de décision pour le système Coq

J. Creci[1] & L. Pottier[2]

*1: Saarland University, Saarbrucken, Germany*
creci@cs.uni-sb.de
*2: INRIA Sophia Antipolis,*
Loic.Pottier@sophia.inria.fr

**Résumé**

Dans cet article, nous proposons une tactique pour le système Coq qui, grâce à des outils algébriques tels que les bases de Gröbner et le théorème des zéros de Hilbert, et grâce à la tactique `Ring`, permet de montrer que des égalités dans un anneau commutatif en impliquent une autre.

## 1. Introduction

La tactique `Ring` [2], écrite par Samuel Boutin et Patrick Loiseleur, permet de prouver une égalité dans un anneau commutatif. Elle procède par mise sous forme normale des deux termes de l'égalité, et est implémentée en utilisant la technique de la réflexion, qui permet de remplacer une preuve par un calcul. Elle permet par exemple de montrer

$$\forall x, y, z \in \mathbb{R}, (x+y)z = zx + yz.$$

On propose ici une extension de cette tactique permettant d'utiliser des égalités en hypothèse. Par exemple, on pourra montrer:

$$\forall x, y, z \in \mathbb{R}, y = z \Rightarrow xy = xz.$$

ou bien

$$\forall x, y \in \mathbb{C}, x^2 + y^2 = 0 \Rightarrow xy = 0 \Rightarrow x + y = 0$$

Cette tactique, appelée `Gb`, est fondée sur le théorème des zéros de Hilbert (pour la théorie) et sur les notions de bases de Gröbner[1] et l'algorithme de Buchberger (pour l'implémentation).

Son principe est simple: dans un anneau intègre une égalité $g = d$ sera démontrable à partir d'égalités $g_1 = d_1, \ldots, g_r = d_r$ si une puissance de $g - d$ est dans l'idéal engendré par $g_1 - d_1, \ldots, g_r - d_r$.

Par exemple, on a bien $(x+y)^2 = (x^2+y^2) + 2(xy)$, d'où on déduit $\forall x, y \in \mathbb{C}, x^2 + y^2 = 0 \Rightarrow xy = 0 \Rightarrow x + y = 0$

La suite de cet article est organisée ainsi:

- dans la section 2, on présente la théorie: le *Nullstellensatz*, qui permet de réduire le problème de prouver une égalité à celui de tester l'appartenance d'une puissance d'un polynôme à un idéal.

[1] aussi appelées *bases standard* par Hironaka, indépendemment et au même moment où Buchberger définissait les *bases de Gröbner*.

- dans la section 3, on présente l'algorithmique qui résoud ce dernier problème, grâce à la notion de bases de Gröbner et à l'algorithme de Buchberger.
- dans la section 4, on présente l'implémentation de la tactique en ocaml et en Coq, des exemples et une discussion des résultats.
- la section 5 conclue cet article.

## 2. Le théorème des zéros de Hilbert.

Dans la suite $A$ est un anneau commutatif unitaire.

**Définition 1** *Un polynôme à n variables à coefficients dans $A$ est donné par une famille $(a_{\alpha_1,\ldots,\alpha_n})_{(\alpha_1,\ldots,\alpha_n)\in\mathbb{N}^n}$ d'éléments de $A$ telle que seul un nombre fini de $a_{\alpha_1,\ldots,\alpha_n}$ est non nul. On le note $P=\sum_{(\alpha_1,\ldots,\alpha_n)\in\mathbb{N}^n} a_{\alpha_1,\ldots,\alpha_n}X_1^{\alpha_1}...X_n^{\alpha_n}$. Ces polynômes forment un anneau, noté $A[X_1,...,X_n]$.*

**Définition 2** *Un idéal de $A$ est un sous-groupe additif de $A$ stable par multiplication par un élément de $A$.*

*L'idéal engendré par des éléments $g_1,\ldots,g_r$ de $A$ est l'ensemble des éléments $a$ de $A$ qui peuvent s'écrire $g=\sum_{i=1\ldots r} a_i g_i$, où les $a_i$ sont dans $A$. C'est aussi le plus petit idéal de $A$ contenant $\{g_1,\ldots,g_r\}$. On le note $(g_1,\ldots,g_r)$.*

Le théorème des zéros de Hilbert (*Nullstellensatz)* relie la géométrie et l'algèbre de la manière suivante:

**Théorème 1** *Soit $A$ un corps algébriquement clos. Soient $P,P_1,\ldots,P_r$ des polynômes de $A[X_1,...,X_n]$. Alors*

$\forall x_1,\ldots,x_n\in A, P_1(x_1,\ldots,x_n)=0,\ldots,P_r(x_1,\ldots,x_n)=0 \Rightarrow P(x_1,\ldots,x_n)=0$

*ssi*

$\exists N\in\mathbb{N}^*, P^N\in(P_1,\ldots,P_r)$

Il s'agit ici d'une des nombreuses versions de ce théorème (voir [4]).

Ce théorème permet de déduire la nullité d'un polynôme en les racines d'autres polynômes de l'appartenance d'une de ses puissances à un idéal. Ce qui pourra être effectué par l'agorithme de Buchberger, grâce à la notion de bases de Gröbner. On utilisera uniquement la condition suffisante, ce qui permet de travailler dans les anneaux intègres.

## 3. Bases de Gröbner

**Définition 3** *Étant donné un ordre admissible*[2] *sur les monômes de $A[X_1,...,X_n]$ - par exemple l'ordre lexicographique - on note in(P) le plus grand monôme d'un polynôme $P$ non nul. On note in($\mathcal{I}$) l'idéal engendré par les plus grand monômes des polynômes non nuls d'un idéal $\mathcal{I}$.*

**Définition 4** *Une base de Gröbner d'un idéal $\mathcal{I}$ de $A[X_1,...,X_n]$ est une famille $\mathcal{G}$ telle que in($\mathcal{G}$) engendre in($\mathcal{I}$).*

[2] i.e. stable par multiplication et tel que 1 est le plus petit monôme.

**Proposition 1** *Tout idéal admet une base de Gröbner, que l'on peut calculer avec l'algorithme de Buchberger.*

*Soit $\mathcal{I}$ un idéal de $A[X_1, ..., X_n]$ et $G_1, ..., G_s$ une base de Gröbner de $\mathcal{I}$. Alors, pour tout $P \in A[X_1, ..., X_n]$, il existe $A_1, ..., A_s \in A[X_1, ..., X_n]$ et un unique $R \in A[X_1, ..., X_n]$ satisfaisant $R \neq 0 \Rightarrow in(R) \not\in in(\mathcal{I})$ et:*

$$P = \sum_{i=1}^{s} A_i G_i + R$$

Pour plus de détails sur les bases de Gröbner on pourra consulter [3].

Les bases de Gröbner sont un outil précieux et quasi-inévitable dans les calculs algébriques.

En particulier, elles permettent de tester si une puissance d'un polynôme est dans un idéal:

**Théorème 2** [3] *Soit $A$ un corps. Soient $P, P_1, \ldots, P_r$ des polynômes de $A[X_1, ..., X_n]$.*

*Considérons de nouvelles variables $t, e, e_0, e_1, .., e_r$, et la famille de polynômes suivante:*

$$\mathcal{F} = \{t(1 - zP) - e_0, tP_1 - e_1, ..., tP_r - e_r\} \cup \{e_i e_j \mid 0 \leq i < j \leq n\} \cup \{te_i \mid 0 \leq i \leq n\}$$

*Alors $\exists N \in \mathbb{N}^*, P^N \in (P_1, \ldots, P_r)$*

*ssi la base de Gröber de l'idéal engendré par $\mathcal{F}$ pour l'ordre lexicographique tel que*

*$t > x_1 > .. > x_m > z > e_0 > .. > e_n$*

*contient un polynôme de la forme*

$$kt - Re_0 - R_1 e_1 \ldots - R_n e_n$$

*avec $k \in A$, $R, R_1, \ldots, R_n \in A[x_1, ..., x_m, z]$.*

*L'entier $N$ est alors le plus grand degré en $z$ des polynômes $R, R_1, \ldots, R_n$.*

*De plus si on pose*

$$\begin{aligned} Q_1 &= P^N R_1[z \leftarrow P^{-1}] \\ &\ldots \\ Q_n &= P^N R_n[z \leftarrow P^{-1}] \end{aligned}$$

*on a $P^N = Q_1 P_1 + \ldots + Q_r P_r$*

On a donc réduit la démonstration de la formule

$\forall x_1, \ldots, x_n \in A, P_1(x_1, \ldots, x_n) = 0, \ldots, P_r(x_1, \ldots, x_n) = 0 \Rightarrow P(x_1, \ldots, x_n) = 0$

à un calcul de bases de Gröbner.

Dans le cas où la base de Gröbner contient bien un polynôme de la forme requise on a de plus l'équation $P^N = Q_1 P_1 + \ldots + Q_r P_r$, de laquelle il facile de produire une preuve de la formule de départ. C'est essentiellement ce que fait la tactique `Gb`.

## 4. La tactique Gb.

Supposons que l'on soit en train d'effectuer une preuve dans Coq. On a un contexte formé d'hypothèses et un but à prouver.

La tactique procède en plusieurs étapes:

[3] merci à Bernard Mourrain de nous l'avoir indiqué. La démonstration de ce théorème est assez technique, on ne la donnera pas ici.

1. détermination de l'anneau $A$ dans lequel se trouve les termes du but $g = d$,

   détermination des hypothèses $H_1, \ldots, H_r$ du contexte de la forme $g_i = d_i$, les termes $g_i$ et $d_i$ étant de type $A$. On en déduit les polynômes $P = g - d$, $P_i = g_i - d_i$.

2. calcul de $N$, $Q_1, \ldots, Q_r$ tels que $P^N = Q_1 P_1 + \ldots + Q_r P_r$.

3. construction de la preuve de $g_1 = d_1 \Rightarrow \ldots \Rightarrow g_r = d_r \Rightarrow g = d$, à partir de $H_1, \ldots, H_r$ et de l'égalité $(g - d)^N = Q_1(g_1 - d_1) + \ldots + Q_r(g_r - d_r)$.

Détaillons ces trois étapes.

## 4.1. Polynômes associés aux but et hypothèses.

L'anneau $A$ dans lequel les expressions vivent doit avoir été déclaré dans Coq comme un anneau. Les polynômes $P, P_1, \ldots, P_r$ sont obtenus en considérant toute expression qui n'est pas une somme, un produit, le zéro ou le un de $A$ comme une variable. On a alors des polynômes dont les coefficients sont dans $\mathbb{Z}$ (ou plus exactement dans son image dans $A$ par l'homomorphisme canonique). Ce qui fait que tous les calculs suivants vont se faire dans l'anneau intègre $\mathbb{Z}[X_1, \ldots, X_n]$. On peut étendre ce que l'on a dit dans les sections 2 et 3 aux anneaux intègres (il suffit de travailler dans leur corps de fractions et dans sa clôture algébrique).

Les calculs sur les polynômes de $\mathbb{Z}[X_1, \ldots, X_n]$ sont implémentés en ocaml, avec une représentation des entiers comme listes d'entiers machines de 16 bits (pour éviter les dépassements quand on multiplie deux entiers). On n'a pas utilisé la bibliothèque `nums` de `Ocaml` car pour cela il faut recompiler tout Coq... On a implémenté les algorithmes qu'on apprend à l'école primaire, ce qui est suffisant pour les problèmes que l'on aura à traiter: addition, multiplication, division.

## 4.2. Calculs de bases de Gröbner.

Pour déterminer $N$, $Q_1, \ldots, Q_r$ tels que $P^N = Q_1 P_1 + \ldots + Q_r P_r$, on calcule une base de Gröbner comme indiqué dans le thèorème 7. Pour cela on a utilisé le code extrait en `Ocaml` de la preuve de en Coq de l'algorithme de Buchberger faite par L.Théry [6].

## 4.3. Construction de la preuve.

On construit, à l'aide de tactiques élémentaires de Coq, une preuve de $g_1 = d_1 \Rightarrow \ldots \Rightarrow g_r = d_r \Rightarrow g = d$, à partir de $H_1, \ldots, H_r$ et de l'égalité $(g - d)^N = Q_1(g_1 - d_1) + \ldots + Q_r(g_r - d_r)$. Cette dernière égalité est prouvée en utilisant la tactique Ring.

Cette étape ne pose pas de difficulté particulière, si ce n'est que si l'entier $N$ est supérieur ou égal à 2, on a besoin de supposer que l'anneau $A$ est intègre (i.e. $\forall x, y \in A, xy = 0 \Rightarrow x = 0 \vee y = 0$) et que $1 \neq 0$ dans $A$. Dans ce cas la tactique produit un but qui est l'intégrité de $A$, et qui doit être prouvé par l'utilisateur (sauf si $A$ est $\mathbb{R}$ ou $\mathbb{Z}$).

Passons maintenant à un exemple:

$\forall x, y \in \mathbb{R}, x^2 = -y^2 = 0 \Rightarrow xy = 0 \Rightarrow x = -y$

Supposons que nous ayons le but suivant:

```
1 subgoal
x : R
y : R
H : ``x*x == -y*y``
H0 : ``x*y == 0``
============================
``x == -y``
```

On a ici $P = x + y, P_1 = x^2 + y^2, P_2 = xy$. Avec le calcul de la base de Gröbner appropriée, on obtient $P^2 = P_1 + 2P_2$. La tactique construit alors la suite de déduction suivante:

```
H : ``x*x == -y*y``   H0 : ``x*y ==0``
donc H1 : ``x*x+y*y == 0`` par H
et ``(x*x+y*y)+2*(x*y) == 0`` par H0 et H
on a ``(x+y)*(x+y) == (x*x+y*y)+2*(x*y)`` par Ring
donc ``(x+y)*(x+y) == 0``
donc ``x+y == 0`` car R est intègre
et ``x == -y``
```

pour prouver ce but:

```
ex1 < Gb.
ex1 < Subtree proved!
```

Un deuxième exemple, où $A$ est un anneau intègre avec $1 \neq 0$:

```
Lemma ex2:(x,y,z,a,b,c,d:A)
  b==-a*(x+y+z)->c==a*(x*y+y*z+z*x)->d==-a*x*y*z -> a*x*x*x+b*x*x+c*x+d==0.
...
ex2 < Intros.

ex2 < 1 subgoal
...
H : b==-a*(x+y+z)
H0 : c==a*(x*y+(y*z)+(z*x))
H1 : d==-a*(x*(y*z))
============================
a*(x*(x*x))+(b*(x*x))+(c*x)+d==0

ex2 < Time Gb.

ex2 < Subtree proved!
Finished transaction in 6. secs (4.556u,0.01s)
```

Un dernier exemple, illustrant la possibilité d'avoir des expressions complexes dans les égalités:

```
x : R
y : R
```

```
H : ``(cos y)*(cos y) == 1-(sin y)*(sin y)``
H0 : ``(cos x) == 0``
H1 : ``1-(sin y)*(sin y) == 0``
H2 : ``(cos x)*(cos y) == 0``
============================
``(cos x) == -(cos y)``

ex2 < Time Gb.

ex2 < Subtree proved!
Finished transaction in 2. secs (1.282u,0.s)
```

## 5. Conclusion.

La tactique `Gb` permet une économie de temps précieux pour prouver de nombreux théorèmes, présents dans la théorie des nombres réels et dans la théorie des entiers relatifs. Elle permet aussi à un utilisateur, après avoir ajouté son propre anneau à l'aide de `Add Ring`, de faciliter les preuves de ces propres lemmes. A la différence des lemmes sur $\mathbb{R}$ ou $\mathbb{Z}$, il devra prouver à la fin l'intégrité de son anneau, ainsi que la non nullité d'un élément de son anneau (lemmes qui ne présenteront pas de difficultés particulières).

Après avoir effectué de nombreux tests nous nous sommes aperçus que pour certaines preuves la tactique `Gb` était assez lente lorsque les coefficients étaient très grands. Ceci s'explique par le fait que la tactique `Ring`, sur laquelle notre tactique est basée, développe les coefficients présents (par exemple 4 est réécrit sous la forme $1+1+1+1$) ce qui implique de prouver une égalité avec des termes parfois énormes.

Enfin, un point très important est que le travail de Laurent Thery [6] (certification de l'algorithme de Buchberger dans Coq [1] et son extraction) nous assure que le calcul des bases de Gröbner est correct et donc que la tactique `Gb` fonctionnera.

Dans un futur proche, nous pensons améliorer les performances de la tactique, en élargissant l'étendue des formes possibles des buts sur lesquels `Gb` travaille actuellement.

Nous souhaiterions en effet traiter des buts avec des polynômes à coefficients fractionnaires pour la théorie des nombres réels.

La tactique s'appuierait aussi sur la tactique `Field`.

## Bibliographie


[1] The Coq Proof Assistant Reference Manual Version 7.4. INRIA Rocquencourt, Année 2003

[2] The Coq Proof Assistant Reference Manual Version 7.4. Chapter 19 "The Ring tactic" INRIA Rocquencourt, Année 2003

[3] David A. Cox et al Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry

and Commutative Algebra, Undergraduate Texts in Mathematics, Springer ed.

[4] Lang S., Algebra - pp 374-376 Année 1984.

[5] The Objective Caml system release 3.06. INRIA Rocquencourt, Année 2002

[6] LAURENT THÉRY, A Machine-Checked Implementation of Buchberger's Algorithm, Journal of Automated Reasoning (2001) 26 pp 107-137.