Gröbner Bases Over a "Dual Euclidean Domain".

Noncommutative rings an their applications
Lens 1-4 july 2013,

Djiby Sow
joint work with
André Saint Eudes Mialébama Bouesso
Université Cheick Anta Diop
Laboratoire d'Algèbre, de Cryptographie,
de Géométrie Algébrique et Applications (LACGAA)
Dakar Sénégal

Membership problem

Let A be a commutative ring and I an ideal of A. Let $a \in A$. How to answer to the question

$$"a \in I \quad ?"$$

We know that if $I = \langle b \rangle$, $b \neq 0$, then $a \in I \quad \Leftrightarrow \exists c \in I \ /a = bc \Leftrightarrow b/a$.

In this case, how to verify if the division b/a holds ?

If $A = K[X]$ is a principal ideal ring in one variable over a field K, then each ideal I is generated by a polynomial g : $I = \langle g \rangle$.

Let $f \in A = K[X]$, then by Euclidean division algorithm, there exists a unique pair $(q, r) \in K[X]^2$ such that $f = qg + r$.

Therefore $f \in I \Leftrightarrow r = 0$

Now, the problem is "how to generalize this result to the multivariate polynomials ring $K[X_1, \ldots, X_n]$?" This ring is factorial and noetherian but not principal.

This problem was solved independently by **Bruno Buchberger** and **Hironaka Heisuk**. But the main popular result is the problem of Buchberger because he provides an efficient algorithm.

B. Buchberger (1965), "An algorithm for finding a basis for the residue class ring of a zero-dimensional polynomial ideal", Ph.D. Thesis, Univ. of Innsbruck, Austria, Math., Inst.

Let I be an ideal in $K[X_1, \ldots, X_n]$ then $I = \langle F \rangle$ where $F = \{f_1, \ldots, f_t\}$ is a finite generating set.
Let $f \in K[X_1, \ldots, X_n]$. Is-it possible to divide f by F (**an ordered set**) ?
Yes, by defining first an admissible order on the set $\mathbb{M}$ of all monomials of $K[X_1, \ldots, X_n]$.
In this case, if the division yields $f = f_1g_1 + \ldots + f_tg_t + r$ with a suitable r, is-it true that

$$\text{"} f \in I \Leftrightarrow r = 0 \text{ ?"}$$

The answer is "false in general" because the result depends on the order on F. We denote

$$r = \overline{f}^{F,\mathrm{ord}}$$

Now, how to do ?
Bruno Buchberger, have proposed a wonderful result.
He proved that "it is always possible to transform the generating set F in a new generating set G such that

$$f \in I \Leftrightarrow \overline{f}^{G,\mathrm{ord}} = 0$$

and this result don't depend on the order on G. (Note that the construction of G depends on the admissible order on the set $\mathbb{M}$ of monomials).
This generating set G is called a **Gröbner basis**.
Moreover, Buchberger have proposed an algorithm which allow to compute, in a finite number of steps, a Gröbner basis G of an ideal I knowing a finite generating set F of I.

Introduction

In *"Introduction to Gröbner Bases" Talk at the Summer School Emerging Topics in Cryptographic Design and Cryptanalysis 30 April - 4 May, 2007, Samos, Greece* Bruno Buchberger makes the following remarks on the **motivation of Gröbner bases**

1. Dozens of (difficult) problems turned out to be reducible to the construction of Gröbner bases.
2. (1000 papers, 10 textbooks, 3000 citations in Research Index, extra entry 13P10 in AMS index).
3. This is based on the fact that Gröbner bases have many nice properties (e.g. canonicality property, elimination property, syzygy property).
4. For the construction of Gröbner bases we have (an) algorithm(s), [BB 1965, ...]
5. A "beautiful" theory : The notion of Gröbner bases and the algorithm is easy to explain, but correctness is based on a non-trivial theory.

Many researchers have generalized this work in different ways over rings. Here we present some results on Gröbner bases over rings.

1. In 1984, Buchberger proposed an algorithm and some technical developments for designing Gröbner basis over reduction rings.
2. In 1988, **D. Kapur and A. Kandri-rody** presented an algorithm for computing a commutative Gröbner basis over an Euclidean domain ;
3. In 1993, **Stifter** presented an algorithm for computing a commutative Gröbner basis in a module over reduction rings with zeros divisors ;
4. In 2000, **L. Bachmair and A. Tiwari** presented an algorithm for computing Gröbner basis over a commutative noetherian rings with additional conditions with zero divisors ;
5. In 2006, **I. Yengui** presented an algorithm for computing a dynamical commutative Gröbner basis (over a noetherian valuation ring and over a principal ideal ring).

Some results on Gröbner bases over rings

1. In 2007, **F. Pauer** presented a method for computing commutative Gröbner bases over rings of differential operators and polynomial rings over commutative noetherian rings with additional conditions ;
2. 2009, **D. Kapur and Y. Cai**, presented an algorithm for computing commutative Gröbner bases over $D - A$ rings with zero divisors.
3. In 2010, **A. Hadj Kacem and I. Yengui** proposed an algorithm for computing a dynamical commutative Gröbner bases over a Dedeking ring with zero divisors.
4. In 2012, **A. Mialébama and D. Sow** presented an algorithm for computing noncommutative Gröbner bases over some class of rings (To be published in "Communications in Algebra") ;

Unfortunately, there doesn't exist a general method for computing commutative Gröbner bases over an arbitrary ring with zero divisors. Each method depends on the properties of the ring. For instance all methods introduced above don't cover the rings of the form $A[\varepsilon] = \dfrac{A[X]}{\langle X^2 \rangle}$ where $\varepsilon = \overline{X}$, A is an arbitrary ring.

That's why we decide to study this case with different hypothesis on A.

Note that the particular case where $A = \mathbb{F}_2$ is used in coding theory in this workshop.

Previous works over $V[\varepsilon]$, with $\varepsilon^2 = 0$

1. In 2012, **André Mialébama** proposed a method for computing **commutative** Gröbner bases over $V[\varepsilon]$, with $\varepsilon^2 = 0$ where **V is a noetherian valuation domain** (To be published in international journal of algebra).
2. In 2013, **André Mialébama and Djiby Sow** proposed a method for computing **commutative** Gröbner bases over $V[\varepsilon]$, with $\varepsilon^2 = 0$ where **V is a noetherian valuation ring with zero divisors** : this method solve partially an open question left by Kapur and Cai in 2009).

This talk

1. In 1988, **D. Kapur and A. Kandri-rody** presented an algorithm for computing a **commutative** Gröbner basis over an **Euclidean domain by introducing an euclidean division on the coefficients in the basic ring**;
2. 2009, **D. Kapur and Y. Cai**, presented an algorithm for computing **commutative** Gröbner bases over $D - A$ rings with zero divisors **by introducing the possibility to compute GCD of the coefficients in the basic ring**.
3. In this work, **André Mialébama and Djiby Sow** propose a method for computing **commutative** Gröbner bases over $V[\varepsilon]$, with $\varepsilon^2 = 0$ where V **is an Euclidean domain by introducing a pseudo-euclidean division on the coefficients in the basic ring**. The technique is different from previous methods.

   This work can be seen as generalization in new kind of rings with zeros divisors.

PART I

Arithmetic in $A[\varepsilon]$

Arithmetic in $A[\varepsilon]$

Let A be an Euclidean domain, we mean by $A[\varepsilon]$ the ring whose elements are of the form $a+\varepsilon b$ satisfying to $\varepsilon^2 = 0$ where $a, b \in A$. This ring is called here, "**Dual Euclidean Domain**". If $z = a + \varepsilon b \in A[\varepsilon]$, then we denote by $\Re(z) = a$ the real part of z (respectively $\Im(z) = b$ the imaginary part of z).

Definition

1. $z = a + \varepsilon b \in A[\varepsilon]$ is invertible if and only if $Re(z) = a$ is invertible in A.
2. $z = a + \varepsilon b \in A[\varepsilon]$ is a zero divisor if and only if $Re(z) = 0$.

Arithmetic in $A[\varepsilon]$

Notation

We denote by $J_\varepsilon = \varepsilon \cdot A[\varepsilon] = \{z \in A[\varepsilon] /\ Re(z) = 0\}$ the set of zero divisors in $A[\varepsilon]$.

Definition

$A[\varepsilon]$ is called pseudo-Euclidean if it comes together with a map

$$\varphi : A[\varepsilon] \longrightarrow \mathbb{N},\ z \mapsto \varphi(z)$$

called pseudo-norm satisfying the following properties :

1. $\varphi(z) \geq 0\ \forall z \in A[\varepsilon]$.
2. $\forall z \in A[\varepsilon],\ t \notin J_\varepsilon$ we have $\varphi(z) \leq \varphi(zt)$.
3. Let $z \in A[\varepsilon]$ and $t \notin J_\varepsilon$ then there exists a pair $(q, r) \in A[\varepsilon]^2$ such that $z = tq + r$ where $r = 0$ or $\varphi(r) < \varphi(t)$.

Definition

Let (B, ϕ) be an Euclidean ring.

- ϕ is said multiplicative if $\phi(a \cdot b) = \phi(a)\phi(b)\ \forall\ a, b \in B$.
- ϕ is said quasi-additive if $\phi(a \cdot b) = \phi(a) + \phi(b)\ \forall\ a, b \in B$.

.

Theorem : Main result 1

If (A, ϕ) is an Euclidean ring where ϕ is either multiplicative or quasi-additive, then $(A[\varepsilon], \varphi)$ is a pseudo-Euclidean ring, where $\varphi(z) = \phi(Re(z))\ \forall\ z \in A[\varepsilon]$.

Arithmetic in $A[\varepsilon]$

Algorithm of pseudo-division

Given two dual numbers $z \in A[\varepsilon]$ and $t \in A[\varepsilon] \setminus J_\varepsilon$ there exists $q, r \in A[\varepsilon]$ such that $z = t \cdot q + r$ where $r = 0$ or $\phi(Re(r)) < \phi(Re(t))$, where ϕ is a norm in A.

Input : $z \in A[\varepsilon]$ and $t \in A[\varepsilon] \setminus J_\varepsilon$.

Output : $(q, r) \in A[\varepsilon]^2$ such that $z = t \cdot q + r$.

Initialize : $a_1 := Re(z \cdot \bar{t}),\ a_2 := Im(z \cdot \bar{t})$ and $n := t \cdot \bar{t}$;

For i from 1 to 2, do

$a_i = q_i \cdot n + r_i$ where $\phi(r_i) < \phi(q_i)$.

end do ;

set $q = q_1 + \varepsilon q_2$ and $r = z - t \cdot q$.

Example

1. Set $A = \mathbb{Z}$ and let us divide in $\mathbb{Z}[\varepsilon]$, $z = 8 + 5\varepsilon$ by $t = 3 + 7\varepsilon$, we find $q = 2 - 4\varepsilon$ and $r = 2 + 3\varepsilon$.
2. Set $A = \mathbb{Q}[t]$ where and let us divide in $\mathbb{Q}[t][\varepsilon]$, $z = (3t^3 + 3t - t) + \varepsilon(6t^3 + 10t^2 + t)$ by $T = (t+1) + \varepsilon(2t+3)$. We have $\overline{T} = (t+1) - \varepsilon(2t+1)$, $z \cdot \overline{T} = (3t^4 + 6t^3 + 2t - t) + \varepsilon(t^3 + 4t^2 + 4t) = a_1 + \varepsilon a_2$ and $n = T \cdot \overline{T} = (t+1)^2$. By the Euclidean division in $\mathbb{Q}[t]$, we find $a_1 = (t+1)^2(3t^2 - 1) + (t+1)$ and $a_2 = (t+1)^2(t+2) + (-t-2)$. Set $q_1 = 3t^2 - 1$, $q_2 = t + 2$, $q = q_1 + \varepsilon q_2 = (3t^2 - 1) + \varepsilon(t+2)$ and $r = z - q \cdot T = 1 - 2\varepsilon$.

Arithmetic in $A[\varepsilon]$

Theorem

Let $z_1, z_2 \in A[\varepsilon]$, $t \in A[\varepsilon] \setminus J_\varepsilon$ such that $z_1 \equiv z_2 \mod t$. Then the pseudo-division algorithm outputs two remainder r_1 and r_2 such that $r_1 = r_2$

Proposition

Let $y \in A[\varepsilon]$ and $t \in A[\varepsilon] \setminus J_\varepsilon$ such that $\varphi(y) < \varphi(t)$ then all $z \equiv y \mod t$ are reduced to y.

Both previous results guaranties that the algorithm of pseudo-division given above yields a unique smallest remainder relatively to our pseudo-norm.

Arithmetic in $A[\varepsilon]$

Definition

Let $u, v \in A$, we say that u and v are coprime, if whenever d divides u and v then d is a unit.

Lemma

An element $z = a + \varepsilon b = (1 + \varepsilon q)(a + \varepsilon r) \in A[\varepsilon]$ is irreducible if and only if a is irreducible or $a = c^n$ where c is irreducible in A and c and r are coprime.

PART II

Gröbner bases over $A[\varepsilon][X_1, \ldots X_n], \quad \varepsilon^2 = 0$

We denote by $R = A[\varepsilon][X_1, \ldots, X_m]$ the ring of multivariate polynomials with coefficients in $A[\varepsilon]$ and by $\mathbb{M}$ the set of all monomials in R.

Definition

A total order $<$ in $\mathbb{M}$, is said to be a monomial order if the following conditions hold :

- $<$ is a well ordering ;
- If $X^\alpha < X^\beta$ then $X^{\alpha+\gamma} < X^{\beta+\gamma}$ for $\alpha, \beta, \gamma \in \mathbb{N}^n$.

Definition

Lexicographic order : we say that $X^\alpha >_{\text{lex}} X^\beta$ if the first left non zero component of $\alpha - \beta$ is > 0.

Let $f = \sum_\alpha z_\alpha X^\alpha$ be a nonzero polynomial in $R = A[\varepsilon][X_1, \ldots, X_n]$.
Let $I = \langle f_1, \ldots, f_s \rangle$ be a finitely generated ideal of R and let fix a monomial order $<$, then :

Definition

1. The X^α (respectively the $z_\alpha X^\alpha$) are called the monomials (respectively the terms) of f.
2. The multidegree of f is $\mathrm{mdeg}(f) := \max\{\alpha / z_\alpha \neq 0\}$.
3. The leading coefficient of f is $Lc(f) := z_{\mathrm{mdeg}(f)}$.
4. The leading monomial of f is $Lm(f) := X^{\mathrm{mdeg}(f)}$.
5. The leading term of f is $Lt(f) := Lc(f) \cdot Lm(f)$.
6. $\langle Lt(I) \rangle := \langle Lt(g) / g \in I \setminus \{0\} \rangle$.

Theorem : Main result 2

Let $<$ be a monomial order and $f_1, \dots, f_s \in R \setminus \{0\}$. Then there exists $q_1, \dots, q_s, r \in R$ such that $f = \sum_{i=1}^{s} q_i f_i + r$ with $\mathrm{mdeg} f \geq \mathrm{mdeg}(q_i f_i)$ if $q_i f_i \neq 0$ and $r = 0$ or each monomial occurring in r is not dividable by any of $Lm(f_i)$ $\forall\ 1 \leq i \leq s$.

Division algorithm

Input : $f_1, \ldots, f_s, f$ and $<$.
Output : $Q_1, \ldots, Q_s, R$.
Initialization : $Q_1 := 0, \ldots, Q_s := 0$; $R := 0$ and $p := f$.
While $p \neq 0$ do :

$i := 1$
not divisionoccured
while $i \leq s$ and not divisionoccured do
If $Lm(f_i)$ divides $Lm(p)$ in $\mathbb{M}$, by pseudo-division do $Lc(p) = q_i Lc(f_i) + r_i \in A[\varepsilon]$ then, set

$$Q_i := Q_i + q_i \frac{Lm(p)}{Lm(f_i)}$$

$$p := Q_i - (q_i \frac{Lm(p)}{Lm(f_i)} + r_i) f_i$$

Else
$i := i + 1$
If not divisionoccured then
$r := r + Lt(p)$; $p := p - Lt(p)$

Example ($A = \mathbb{Z}$)

Let $R = \mathbb{Z}[\varepsilon][x, y]$ be a multivariate polynomials ring with respect to $x >_{\text{lex}} y$ and $f = 2x^2y - (3 - 2\varepsilon)y$, $f_1 = (2 + 3\varepsilon)x^2 + 3\varepsilon x$, $f_2 = (3 - \varepsilon)xy + (2 + 5\varepsilon)y^2$. Let us divide in $\mathbb{Z}[\varepsilon]$ f by $\{f_1, f_2\}$, we find
$f = [(1 - \varepsilon)y]f_1 - \varepsilon f_2 + [2\varepsilon y^2 + (-3 + 2\varepsilon)y]$.

Example ($A = \mathbb{Q}[t]$)

Let $R = \mathbb{Q}[t][\varepsilon][x, y]$ be a multivariate polynomials ring with respect to $x >_{\text{grlex}} y$ and $f = [2\varepsilon(t^2-1)(t+1)]x^2y^2 + [5t - 3\varepsilon(t+2)]xy$, $f_1 = [2(t+1)^2 + 3\varepsilon]x^2 - \varepsilon(t+1)y$, $f_2 = \varepsilon(t-1)y^2 + (2+\varepsilon t)x$. Let us divide f by $\{f_1, f_2\}$, we find

1. $f = \varepsilon(t-1)y^2 \cdot f_1 + [5t - 3\varepsilon(t+2)]xy$ if we start the division by f_1.
2. $f = -2t\varepsilon x \cdot f_1 + [2(t+1)^2 + 3\varepsilon]x^2 \cdot f_2 + 2\varepsilon(t+1)[xy - y]$ if we start the division by f_2.

Definition

A subset $G = \{g_1, \ldots, g_t\}$ of an ideal $I \subset R$ is called Gröbner basis for I with respect to a monomial order $<$ if $I = \langle G \rangle$ and $\langle Lt(I) \rangle = \langle Lt(G) \rangle$.

Definition

Let $f \neq g \in R = A[\varepsilon][X_1, \ldots, X_m]$ such that $Lc(f) = (a_1 + \varepsilon b_1)X^\alpha$ and $Lc(f) = (a_2 + \varepsilon b_2)X^\beta$, and consider a monomial order $>$. Let $\gamma \in \mathbb{N}^n$ with $X^\gamma = \mathrm{lcm}(X^\alpha, X^\beta)$, the S-polynomial of f and g is given by the combination :

1. If $f \neq g$

$$S(f,g) = \begin{cases} (a_2 + \varepsilon b_2)X^{\gamma-\alpha} f - (a_1 + \varepsilon b_1)X^{\gamma-\beta} g \text{ if } a_1 \text{or } a_2 \neq 0 \\ \dfrac{b_2}{\gcd(b_1, b_2)} X^{\gamma-\alpha} f - \dfrac{b_1}{\gcd(b_1, b_2)} X^{\gamma-\alpha} g \text{ if } a_1 = a_2 = 0. \end{cases}$$

2. If $f = g$ then

$$S(f,f) = \begin{cases} \varepsilon f \text{ if } Lc(f) \in J_\varepsilon \; i.e \; a_1 = 0 \\ 0 \text{ if not.} \end{cases}$$

Example

In $R = \mathbb{Z}[\varepsilon][x, y]$ with $x >_{lex} y$, we consider two polynomials $f_1 = 3\varepsilon x^2 + (2 - \varepsilon)xy$, $f_2 = (4 + 3\varepsilon)xy^2 - 5\varepsilon y^2$, then :
$S(f_1, f_1) = \varepsilon f_1 = 2\varepsilon xy$;
$S(f_1, f_2) = (4 + 3\varepsilon)y^2 f_1 - 3\varepsilon x f_2 = (8 + 2\varepsilon)xy^2$.
Let $f_3 = 6\varepsilon y^4 + (3 - 5\varepsilon)y^2$ we have
$S(f_1, f_3) = 2y^4 f_1 - x^2 f_3 = (3 - 5\varepsilon)x^2y^2 + 2(2 - \varepsilon)xy^5$.

Lemma

Let $<$ be a monomial order, and $f_1, \dots, f_s \in R = A[\varepsilon][X_1, \dots, X_m]$ such that $\mathrm{mdeg}(f_i) = \gamma \in \mathbb{N}^n$ for each $1 \leq i \leq s$. If $\mathrm{mdeg}(\sum_{i=1}^{s} z_i f_i) < \gamma$ for some $z_1, \dots, z_s \in A[\varepsilon]$, then there exists $t \in A[\varepsilon] \setminus J_\varepsilon$ such that $t \sum_{i=1}^{s} z_i f_i$ is a linear combination with coefficients in $A[\varepsilon]$ of the S-polynomials $S(f_i, f_j)$ for $1 \leq i \leq j \leq s$. Furthermore, each $S(f_i, f_j)$ has multidegree $< \gamma$.

This lemma is the key to prove the following theorem.

Theorem : Main result 3

Let $<$ be a monomial order and $G = \{g_1, \ldots, g_s\}$ be a finite set of polynomials of $R = A[\varepsilon][X_1, \ldots, X_m]$. Let $I = \langle G \rangle$ be an ideal of R, then G is a Gröbner basis for I if and only if $\overline{S(g_i, g_j)}^G = 0$, for $1 \leq i \leq j \leq s$.

Since $A[\varepsilon]$ is noetherian, then $R = A[\varepsilon][X_1, \ldots, X_m]$ is also noetherian therefore this theorem allows to compute a Gröbner basis for an ideal of R in finite number of steps).

(Buchberger's algorithm)

Input : $g_1, \dots, g_s \in T$ and $<$ a monomial order.
Output : a Gröbner basis G for $I = \langle g_1, \dots, g_s \rangle$ with $\{g_1, \dots, g_s\} \subseteq G$

$G := \{g_1, \dots, g_s\}$
REPEAT
$G' := G$
For each pair g_i, g_j in G' do
$S := \overline{S(g_i, g_j)}^{G'}$
If $S \neq 0$ THEN $G := G' \cup \{S\}$
UNTIL $G = G'$

Example

$R = \mathbb{Z}[\varepsilon][x,y]$, $I = \langle f_1 = 3\varepsilon x^2 + (2-\varepsilon)xy, f_2 = (4+3\varepsilon)xy^2 - 5\varepsilon y^2 \rangle$.
Let us construct a Gröbner basis for I w.r.t $x >_{\text{lex}} y$.
Set $g_1 := f_1, g_2 := f_2$ and $G := \{g_1, g_2\}$. We have :

- $S(g_1, g_1) = \varepsilon g_1 = 2\varepsilon xy$ and $\overline{S(g_1, g_1)}^G = 2\varepsilon xy = g_3$, put $G := \{g_1, g_2, g_3\}$;
- $S(g_1, g_3) = 2yf_1 - 3xf_3 = (4-2\varepsilon)xy^2$ and $\overline{S(g_1, g_3)}^G = -\varepsilon xy^2 = g_4$, put $G := \{g_1, g_2, g_3, g_4\}$;
- $S(g_1, g_4) = (4-2\varepsilon)y^2 g_1 - 3\varepsilon x g_4 = 8xy^3$ and $\overline{S(g_1, g_4)}^G = 0$;
- $S(g_1, g_2) = 4(1-\varepsilon)yg_1 - 3\varepsilon x g_7 = 4(2-3\varepsilon)xy^3$ and $\overline{S(g_1, g_2)}^G = 0$;
- $\overline{S(g_2, g_3)}^G = \overline{S(g_3, g_4)}^G = \overline{S(g_3, g_3)}^G = \overline{S(g_4, g_4)}^G = 0$

Thus $G = \{3\varepsilon x^2 + (2-\varepsilon)xy, (4+3\varepsilon)xy^2 - 5\varepsilon y^2, 2\varepsilon xy, -\varepsilon xy^2\}$ is a Gröbner basis for I w.r.t $x >_{\text{lex}} y$.

Open problem

Open problem by Kapur and Cai in 2009

Consider the ring $A = \frac{\mathbb{F}_2[X,Y]}{\langle X^2-X, Y^2-Y\rangle}$.
Let $Z = XY + X + Y + 1$, then X and Y belong to the annihilator of Z. The $\gcd(X,Y) \neq 1$? may not be defined (or it may not be possible to define division of one parameter by another parameter).

Therefore how to generalize Buchberger's algorithm for such quotient rings ?.

This an open problem of Kapur and Cai in :

*Deepak Kapur and Yongyang Cai "**An Algorithm for Computing a Gröbner Basis of a Polynomial Ideal over a Ring with Zero Divisors**" Math.comput.sci. 2 (2009), 601-634 (2009) Birkhauser Verlag Basel Switzerland 1661-8270/040601-34, published online December 7, 2009 DOI 10.1007/s11786-009-0072-z*

Thank you for your attention !