Algorithms for computing syzygies over $\mathrm{V}[X_1, \ldots, X_n]$, V a valuation ring

Ihsen Yengui
Département de Mathématiques, Faculté des Sciences de Sfax, Tunisie

Besançon, october 15, 2011

Ideal membership Problem over the integers (Kronecker's Problem):

Given: An ideal $I = \langle f_1, \ldots, f_s \rangle \subseteq \mathbb{Z}[X_1, \ldots, X_n]$ and $f \in \mathbb{Z}[X_1, \ldots, X_n]$.

Decide: Whether $f \in I$. In case of positive answer, give $h_1, \ldots, h_s \in \mathbb{Z}[X_1, \ldots, X_n]$ such that $f = h_1 f_1 + \cdots + h_s f_s$.

Computing the syzygies module over $\mathbb{Z}$:

Given: $f_1, \ldots, f_s \in \mathbb{Z}[X_1, \ldots, X_n]$.

Compute a finite generating set for:

$$\mathrm{Syz}(f_1, \ldots, f_s) := \{(h_1, \ldots, h_s) \in \mathbb{Z}[X_1, \ldots, X_n]^s \mid$$

$$h_1 f_1 + \cdots + h_s f_s = 0\}.$$

Let $\mathbf{R}$ be a Dedekind domain $\mathbf{R}$ with field of fractions $\mathbf{F}$, and $f, f_1, \ldots, f_s \in \mathbf{R}[X_1, \ldots, X_n]$.

A necessary condition so that $f \in \langle f_1, \ldots, f_s \rangle$ in $\mathbf{R}[X_1, \ldots, X_n]$ is: $f \in \langle f_1, \ldots, f_s \rangle$ in $\mathbf{F}[X_1, \ldots, X_n]$.

Suppose that this condition is fulfilled, that is there exists $d \in \mathbf{R} \setminus \{0\}$ such that

$$d\, f \in \langle f_1, \ldots, f_s \rangle \text{ in } \mathbf{R}[X_1, \ldots, X_n] \quad (0).$$

Since the basic ring $\mathbf{R}$ is a Dedekind domain, we can write

$$\langle d \rangle = \prod_{i=1}^{\ell} \mathfrak{p}_i^{n_i},$$

where the $\mathfrak{p}_i$ are nonzero distinct prime ideals of $\mathbf{R}$.

Other necessary conditions so that $f \in \langle f_1, \ldots, f_s \rangle$ in $\mathbf{R}[X_1, \ldots, X_n]$ is: $f \in \langle f_1, \ldots, f_s \rangle$ in $\mathbf{R}_{p_i \mathbf{R}}[X_1, \ldots, X_n]$ for each $1 \leq i \leq \ell$. Here the polynomial ring is over the discrete valuation domain $\mathbf{R}_{\mathfrak{p}_i}$. Write:

$d_i\, f \in \langle f_1, \ldots, f_s \rangle$ in $\mathbf{R}[X_1, \ldots, X_n]$ for some $d_i \in \mathbf{R} \backslash \mathfrak{p}_i$.

Since $1 \in \langle d, d_1, \ldots, d_\ell \rangle$, we can glue all the equalities above and obtain that $f \in \langle f_1, \ldots, f_s \rangle$ in $\mathbf{R}[X_1, \ldots, X_n]$. Thus, the necessary conditions are sufficient and it suffices to treat the problem in case the basic ring is a valuation ring.

Definitions 1. Let $\mathbf{R}$ be a ring, $f = \sum_\alpha a_\alpha X^\alpha$ a nonzero polynomial in $\mathbf{R}[X_1, \ldots, X_n]$, E a non empty subset of $\mathbf{R}[X_1, \ldots, X_n]$, and $>$ a (global) monomial order.

(i) The X^α (resp. the $a_\alpha X^\alpha$) are called the monomials (resp. the terms) of f.

(ii) The multidegree of f is $\mathsf{mdeg}(f) := \max\{\alpha \in \mathbb{N}^n : a_\alpha \neq 0\}$.

(iii) The leading coefficient of f is $\mathsf{LC}(f) := a_{\mathsf{mdeg}(f)} \in \mathbf{R}$.

(iv) The leading monomial of f is $\mathsf{LM}(f) := X^{\mathsf{mdeg}(f)}$.

(v) The leading term of f is $\mathsf{LT}(f) := \mathsf{LC}(f)\,\mathsf{LM}(f)$.

(vi) $\mathsf{LT}(E) := \{\mathsf{LT}(g), g \in E\}$.

(vii) $\langle \mathsf{LT}(E) \rangle := \langle \mathsf{LT}(g), g \in E \rangle$.

Definitions 2. Let $\mathbf{R}$ be a $\mathbf{V}$ is coherent valuation ring, $f, g \in \mathbf{R}[X_1, \ldots, X_n] \setminus \{0\}$, $I = \langle f_1, \ldots, f_s \rangle$ a nonzero finitely generated ideal of $\mathbf{R}[X_1, \ldots, X_n]$, and $>$ a monomial order.

(i) If mdeg$(f) = \alpha$ and mdeg$(g) = \beta$ then let $\gamma = (\gamma_1, \ldots, \gamma_n)$, where $\gamma_i = \max(\alpha_i, \beta_i)$ for each i.

The S-polynomial of f and g is the combination:

$S(f,g) = \frac{X^\gamma}{\mathsf{LM}(f)} f - \frac{\mathsf{LC}(f)}{\mathsf{LC}(g)} \frac{X^\gamma}{\mathsf{LM}(g)} g$ if $\mathsf{LC}(g)$ divides $\mathsf{LC}(f)$.

$S(f,g) = \frac{\mathsf{LC}(g)}{\mathsf{LC}(f)} \frac{X^\gamma}{\mathsf{LM}(f)} f - \frac{X^\gamma}{\mathsf{LM}(g)} g$ if $\mathsf{LC}(f)$ divides $\mathsf{LC}(g)$ and $\mathsf{LC}(g)$ does not divide $\mathsf{LC}(f)$.

(ii) $S(f,f) := d\, f$, where d is a generator of the annihilator of $\mathsf{LC}(f)$ (it is defined up to a unit).

(iii) $G = \{f_1, \ldots, f_s\}$ is said to be a Gröbner basis for I if $\langle \mathsf{LT}(I) \rangle = \langle \mathsf{LT}(f_1), \ldots, \mathsf{LT}(f_s) \rangle$.

Theorem 2. *Let* $\mathbf{R}$ *be a coherent valuation ring,* $I = \langle g_1, \ldots, g_s \rangle$ *an ideal of* $\mathbf{R}[X_1, \ldots, X_n]$*, and fix a monomial order* $>$*. Then,* $G = \{g_1, \ldots, g_s\}$ *is a Gröbner basis for* I *if and only if for all pairs* $1 \leq i \leq j \leq s$*, the remainder on division of* $S(g_i, g_j)$ *by* G *is zero.*

Buchberger's Algorithm for Coherent valuation rings

Input: $g_1, \ldots, g_s \in \mathbf{V}[X_1, \ldots, X_n]$, $\mathbf{V}$ a valuation ring, $>$ a monomial order

Output: a Gröbner basis G for $\langle g_1, \ldots, g_s \rangle$ with

$\{g_1, \ldots, g_s\} \subseteq G$

$G := \{g_1, \ldots, g_s\}$ REPEAT
$G' := G$
For each pair f, g in G' DO
$S := \overline{S(f,g)}^{G'}$
If $S \neq 0$ THEN $G := G' \cup \{S\}$
UNTIL $G = G'$

Example: Let $\mathbf{V}[X] = (\mathbb{Z}/16\mathbb{Z})[X]$, and consider the ideal $I = \langle f_1 \rangle$, where $f_1 = 2+4X+8X^2$.

$S(f_1, f_1) = 2f_1 = 4 + 8X =: f_2$,

$S(f_1, f_2) = 2 =: f_3$,

$S(f_2, f_2) = 2f_2 = 8 \xrightarrow{f_3} 0$, $S(f_3, f_3) = 0$,

$f_2 \xrightarrow{f_3} 0$.

Thus, $\mathcal{G} = \{2\}$ is a Gröbner basis for I in $\mathbf{V}[X]$.

Question:

Does the generalized version of Buchberger's Algorithm for coherent valuation rings always terminate after a finite number of steps ?

Answer: NO

Of course if the base ring $\mathbf{V}$ is noetherian, it terminates.

An example

Let $\mathbf{V}$ be a valuation domain with valuation v and a non archimedian valuation group G.

$\exists\ a, b \in \mathbf{V}$ such that $v(a) > 0$, and $\forall\ n \in \mathbb{N}^*,\ v(b) > n\, v(a)$.

$I = \langle g_1 = aX + 1, g_2 = b \rangle$ in $\mathbf{V}[X]$

Buchberger's Algorithm for valuation rings does not terminate: $\Rightarrow\ \frac{b}{a} \Rightarrow\ \frac{b}{a^2} \Rightarrow \cdots$

We can prove that LT(I) is not finitely generated.

The Gröbner ring Conjecture.

Let $\mathbf{V}$ *be a valuation domain with corresponding valuation group* G, $n \in \mathbb{N}^*$, *and fix a monomial order* $>$ *in* $\mathbf{V}[X_1, \ldots, X_n]$. *Then the following assertions are equivalent:*

(i) It is always possible to compute a Gröbner basis for each finitely generated nonzero ideal of $\mathbf{V}[X_1, \ldots, X_n]$ *by the generalized version of Buchberger's Algorithm for valuation domains in a finite number of steps.*

(ii) G *is archimedian (*$\Leftrightarrow \dim \mathbf{V} \leq 1$*).*

(iii) For each finitely generated ideal I *of* $\mathbf{V}[X_1, \ldots, X_n]$, *the ideal* $\langle \mathsf{LT}(I) \rangle$ *is finitely generated.*

Solutions:

H. Lombardi, P. Schuster, I. Yengui, *The Gröbner ring conjecture in one variable*, Math. Zeitschrift (2011).

I. Yengui, *A solution to the Gröbner ring conjecture*. Preprint 2011.

The method of seeing what happens locally raised the following question:

How to avoid the expensive problem of factorizing a principal ideal in a Dedekind domain into a finite product of prime ideals ?

The use of gluing "local realizability" appeals to the use of dynamical methods and more precisely, as will be explained later in this course, the use of a new notion of Gröbner basis, namely the notion of "dynamical Gröbner basis". A key fact is that for any two nonzero elements a and b in a principal domain $\mathbf{R}$, writing $a = (a \wedge b)a'$, $b = (a \wedge b)b'$, with $a' \wedge b' = 1$, then a divides b in $\mathbf{R}_{a'}$ and b divides a in $\mathbf{R}_{b'}$, where the multiplicative subsets $\mathcal{M}(a')$ and $\mathcal{M}(b')$ are comaximal. This precious fact will enable us to go back from the leaves to the root of the evaluation tree produced by our dynamical method. In other words, this will make the gluing of "local realizability" possible.

Buchberger's Algorithm over coherent arithmetical rings

It works like Buchberger's Algorithm for coherent valuation rings. The only difference is when it has to handle two incomparable (under division) elements a, b in $\mathbf{R}$. In this situation, one should first compute $u, v, w \in \mathbf{R}$ such that

$$\begin{cases} ub = va \\ wb = (1-u)a. \end{cases}$$

Now, one opens two branches: the computations are pursued in $\mathbf{R}_u$ and $\mathbf{R}_{1-u\mathbf{R}}$.

At the end of the computation, one obtains a binary tree whose leaves corresponds to comaximal localizations $S_i^{-1}\mathbf{R}$ $(1 \leq i \leq s)$ of the base ring $\mathbf{R}$. If we denote by G_i the Gröbner basis obtained at the i^{th} leaf,

$$G := \{(G_1, S_1), \ldots, (G_s, S_s)\}$$

is called a **dynamical Gröbner basis**.

An example

1) Suppose that we want to construct a dynamical Gröbner basis for $I = \langle f_1 = 3XY + 1,\, f_2 = (4 + 2\theta)Y + 9 \rangle$ in $\mathbb{Z}[\theta][X, Y]$ where $\theta = \sqrt{-5}$.

Let fix the lexicographic order as monomial order with $X > Y$.

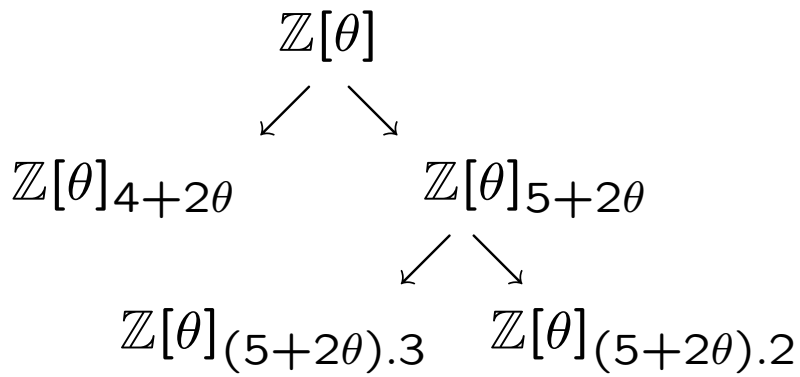
Since $x_1 := 3$ and $x_2 := 4 + 2\theta$ are incomparable under division, one has to compute $u, v, w \in \mathbb{Z}[\theta]$ such that:

$$\begin{cases} ux_2 = vx_1 \\ wx_2 = (1 - u)x_1. \end{cases}$$

Since $\mathbb{Z}[\theta]$ has a $\mathbb{Z}$-basis, finding u, v, w amounts to solve an under-determined linear system over the integers. The resolution can be done by any computer algebra system. One solution to this system is $u = 5 + 2\theta$, $v = 6\theta$, $w = -3$. Thus, one has to open two branches:

$$\begin{array}{ccc} & \mathbb{Z}[\theta] & \\ & \swarrow \quad \searrow & \\ \mathbb{Z}[\theta]_{4+2\theta} & & \mathbb{Z}[\theta]_{5+2\theta} \end{array}$$

At the end of computations, the dynamical evaluation of the problem of constructing a Gröbner basis for I produces the following evaluation tree:



The obtained dynamical Gröbner basis of I is

$$G = \{(\mathcal{M}(5+2\theta), G_1),\ (\mathcal{M}(4+2\theta), G_2)\}.$$

With $G_1 = \{3XY+1,\ -3X+\frac{2\theta}{5+2\theta},\ \frac{2\theta}{5+2\theta}Y+1\}$,

and $G_2 = \{3XY+1,\ -\frac{27}{4+2\theta}X+1,\ Y+\frac{9}{4+2\theta}\}$

2) Computing the syzygy module:

Denoting by $F = [f_1 \ f_2]$, we will compute a generating set for Syz(F).

Over $\mathbb{Z}[\theta]_{(5+2\theta).3}$:

$$\text{Syz}(F) = \langle \begin{pmatrix} 3X^2Y + \frac{4+2\theta}{3}X^2Y^2 \\ \frac{-1}{3}X^2Y - X^3Y^2 \end{pmatrix},$$

$$\begin{pmatrix} 27XY - 9 - (4+2\theta)Y + 3(4+2\theta)XY^2 \\ 1 - 9X^2Y^2 \end{pmatrix} \rangle.$$

Over $\mathbb{Z}[\theta]_{(5+2\theta).2}$:

$$\text{Syz}(F) = \langle \begin{pmatrix} \frac{9X^2Y(5+2\theta+2\theta Y)}{2\theta} \\ \frac{-(5+2\theta)(3X^3Y^2+X^2Y)}{2\theta} \end{pmatrix},$$

$$\begin{pmatrix} 27XY - 9 - (4+2\theta)Y + 3(4+2\theta)XY^2 \\ 1 - 9X^2Y^2 \end{pmatrix} \rangle.$$

Over $\mathbb{Z}[\theta]_{(4+2\theta)}$:

$$\mathrm{Syz}(F) = \langle \begin{pmatrix} -\frac{9}{4+2\theta} - Y \\ \frac{1}{4+2\theta} + \frac{3XY}{4+2\theta} \end{pmatrix} \rangle.$$

Finally, over $\mathbb{Z}[\theta]$, we have

$$\mathrm{Syz}(F) = \langle \begin{pmatrix} -(4+2\theta)Y - 9 \\ 3XY + 1 \end{pmatrix},$$

$$\begin{pmatrix} 27XY - 9 - (4+2\theta)Y + 3(4+2\theta)XY^2 \\ 1 - 9X^2Y^2 \end{pmatrix} \rangle$$

$$= \langle \begin{pmatrix} -(4+2\theta)Y - 9 \\ 3XY + 1 \end{pmatrix} \rangle.$$

On Polly Cracker over Valuation Rings (in collaboration with Jean-Marie Preira & Djiby Sow (Dakar)) :

Polly Cracker system is a public key cryptosystem in which the private key is a commutative Gröbner basis of a multivariate polynomials ideal over a finite field. Many attacks show that this system based on Gröbner bases over a field is not secure.

To design a secure Polly Cracker system, we propose to implement Polly Cracker over rings with enough zero divisors (provided that a concept of Gröbner basis exists), because the analysis of all known attacks like for example the linear algebra attack, shows that they use in some step, the solution of a linear system in the underlying field. Hence to avoid such attacks on Polly Cracker, it may be interresting to work over a ring for which linear systems are difficult to solve.

In order to obtain a such difficult linear system to solve, we propose a new version of Polly Cracker system that relies on Gröbner bases over a Dedekind ring with many zero-divisors.

Proposition: If $\mathbf{R}$ is a local ring with n elements, denoting by $P_{(\mathbf{R})}$ (resp., $P_{(\mathbf{R}\times\mathbf{R})}$) the probability that an element in $\mathbf{R}$ (resp., in $\mathbf{R}\times\mathbf{R}$) is a zero-divisor (including zero), we have:

$$P_{(\mathbf{R})} \leq \frac{1}{2} \quad \& \quad P_{(\mathbf{R}\times\mathbf{R})} = 2P_{(\mathbf{R})} - P_{(\mathbf{R})}^2.$$

In Particular

$$P_{(\mathbf{R})} = \frac{1}{2} \text{ (that is maximal) } \Rightarrow P_{(\mathbf{R}\times\mathbf{R})} = 1 - \frac{1}{4} = 3/4.$$

More particularly,

$$P_{(\mathbb{Z}/p^\alpha\mathbb{Z})} = \frac{1}{p} \quad \& \quad P_{(\mathbb{Z}/p^\alpha\mathbb{Z}\times\mathbb{Z}/q^\beta\mathbb{Z})} = \frac{1}{p} + \frac{1}{q} - \frac{1}{pq},$$

$$P_{(\mathbb{Z}/2^\alpha\mathbb{Z})} = \frac{1}{2} \quad \& \quad P_{(\mathbb{Z}/2^\alpha\mathbb{Z})\times(\mathbb{Z}/2^\alpha\mathbb{Z})} = 3/4.$$

Example: Take $p = 2$ and $\alpha = 3$. Let

$$I = \langle f_1 = (2,1)X + (1,2)Y + (1,0),$$

$$f_2 = (1,2)X^2 + (1,1)\rangle \subseteq (\mathbb{Z}/8\mathbb{Z}) \times (\mathbb{Z}/8\mathbb{Z})[X,Y].$$

$$\begin{array}{ccc} (\mathbb{Z}/8\mathbb{Z}) \times (\mathbb{Z}/8\mathbb{Z}) & & \\ \swarrow & \searrow & \\ \mathbb{Z}/8\mathbb{Z} & & \mathbb{Z}/8\mathbb{Z} \end{array}$$

$$I_1 := \pi_1(I) = \langle g_1 = 2X + Y + 1,\, g_2 = X^2 + 1\rangle,$$

$$I_2 := \pi_2(I) = \langle h_1 = X + 2Y,\, h_2 = 2X^2 + 1\rangle.$$

We find $\mathcal{G}_1 = \{2X+Y+1,\, X^2+1,\, 4Y+4,\, XY+X-2,\, Y^2+6Y+1\}$ as a reduced Gröbner for I_1, and $\mathcal{G}_2 = \{1\}$ as a reduced Gröbner for I_2 according to $>_{\text{lex}}$.

As a conclusion, a reduced dynamical Gröbner basis for I in the ring $(\mathbb{Z}/8\mathbb{Z}) \times (\mathbb{Z}/8\mathbb{Z})[X,Y]$ is

$$\mathcal{G} = \{(\{(2,0)X+(1,0)Y+(1,0),\, (1,0)X^2+(1,0),$$

$$(4,0)Y+(4,0),\, (1,0)XY+(1,0)X-(2,0),$$

$$(1,0)Y^2+(6,0)Y+(1,0)\}, e^{\mathbb{N}}),\, (\{(0,1)\},\, (\mathbf{1}-e)^{\mathbb{N}})\},$$

where $e = (1,0)$ and $\mathbf{1} - e = (1,0)$

Recall that

$$\mathbb{Z}[t]/\langle p^\alpha, t^2 - t\rangle \overset{\varphi}{\cong} (\mathbb{Z}/p^\alpha\mathbb{Z}) \times (\mathbb{Z}/p^\alpha\mathbb{Z})$$

with $\varphi(\bar{f}) = (\overline{f(0)}, \overline{f(1)})$ for $f \in \mathbb{Z}[t]$

If coded in the ring $(\mathbb{Z}[t]/\langle 8, t^2 - t\rangle)[X, Y]$, a reduced dynamical Gröbner basis for $J = \varphi^{-1}(I)$ is

$$G = \{(\{2X + Y + 1,\ X^2 + 1,\ 4Y + 4,\ XY + X - 2,$$

$$Y^2 + 6Y + 1\}, (1 - t)^{\mathbb{N}}),\ (\{1\},\ t^{\mathbb{N}})\}.$$

Computing the syzygies module over a valuation domain with arbitrary Krull dimension:

1) Lombardi H., Quitté C., Yengui I. *Un algorithme pour le calcul des syzygies sur* $\mathbf{V}[X]$ *dans le cas où* $\mathbf{V}$ *est un domaine de valuation*, Preprint 2010. In this paper we prove a more general result: the $\mathbf{V}$-saturation of any finitely generated submodule of $\mathbf{V}[X]^n$ is finitely generated.

2) Generalization to many variables: work in progress in collaboration with Lionel Ducos, Henri Lombardi and Claude Quitté.

MERCI