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

where V is a valuation ring

Ihsen Yengui

Department of Mathematics, University of Sfax, Tunisia

Graz, 07/07/2016

Plan

- Computing syzygies over $\mathbf{V}[X_1, \ldots, X_n]$ with Gröbner bases

- Computing syzygies over $\mathbf{V}[X_1, \ldots, X_n]$ via saturation, general case

$a_1, \ldots, a_n \in \mathbf{R}$. The **syzygy module** of $(a_1, \ldots, a_n)$ is

$$\mathrm{Syz}(a_1, \ldots, a_n)$$

$$:= \{(b_1, \ldots, b_n) \in \mathbf{R}^n \mid b_1 a_1 + \cdots + b_n a_n = 0\}.$$

A ring $\mathbf{V}$ is called a **valuation ring** if all its elements are comparable under division. A valuation ring is **coherent** if the annihilator $\mathrm{Ann}(x) = \mathrm{Syz}(x)$ of any element $x \in \mathbf{V}$ is finitely-generated.

Definitions 2. Let $\mathbf{V}$ be a coherent valuation ring, $f, g \in \mathbf{V}[X_1, \ldots, X_n] \setminus \{0\}$, $I = \langle f_1, \ldots, f_s \rangle$ a nonzero finitely generated ideal of $\mathbf{V}[X_1, \ldots, X_n]$, 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) The **auto-S-polynomial** of f is $S(f,f) := d\,f$, 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 $\mathbf{V}$ be a coherent valuation ring, $I = \langle g_1, \ldots, g_s \rangle$ an ideal of $\mathbf{V}[X_1, \ldots, X_n]$, 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 coherent 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 $\mathbf{V}[X]$.

Theorem. *Let* $\mathbf{V}$ *be a valuation ring. Then, one can construct Gröbner bases over* $\mathbf{V}$ *(for the lexicographic monomial order) if and only if* $\mathbf{V}$ *is both* **coherent** *and* **archimedean** *(i.e.,* $\forall\, a, b \in \mathrm{Rad}(\mathbf{V}) \setminus \{0\} \;\; \exists\, n \in \mathbb{N} \quad |\; a$ divides b^n*), or also, if and only if either*

- $\dim \mathbf{V} \leq 1$ *and* $\mathbf{V}$ *is without zero-divisors*

or

- $\dim \mathbf{V} = 0$ *and the annihilator of any element in* $\mathbf{V}$ *is finitely generated.*

References:

• Yengui I. *Dynamical Gröbner bases*. J. Algebra **301** (2006) 447–458.

• Hadj Kacem A., Yengui I. *Dynamical Gröbner bases over Dedekind rings.* J. Algebra **324** (2010) 12-24.

• Lombardi H., Schuster P., Yengui I. *The Gröbner ring conjecture in one variable*. Math. Z. **270** (2012) 1181-1185.

• Yengui I. *The Gröbner Ring Conjecture in the lexicographic order case*. Math. Z. **276** (2014) 261-265.

It is a folklore that if $\mathbf{V}$ is valuation domain then $\mathbf{V}[X_1, \ldots, X_n]$ is **coherent**, i.e., Syzygy modules over $\mathbf{V}[X_1, \ldots, X_n]$ are finitely generated. This follows from a deep and complicated paper: Gruson L., Raynaud M. Critères de platitude et de projectivité. Invent. Math. (1971).

Our goal is to find an algorithm for computing syzygies over $\mathbf{V}[X_1, \ldots, X_n]$, where V is a valuation domain of any Krull dimension.

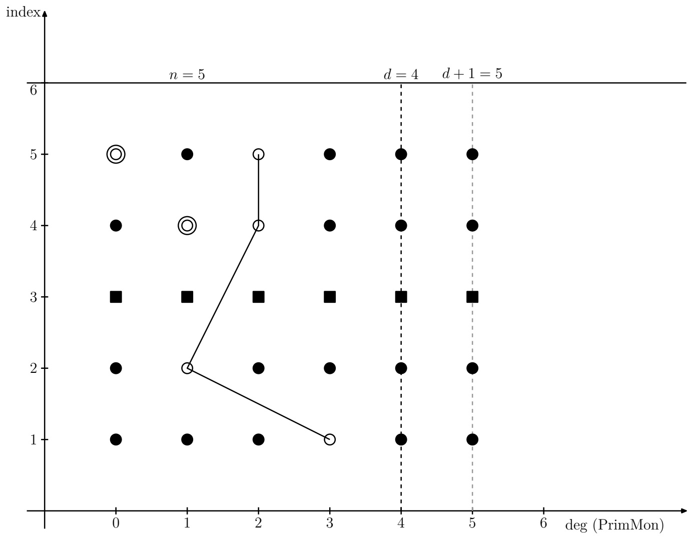
Let $p_1, \ldots, p_m \in \mathbf{V}[X_1, \ldots, X_k]$, and consider n vectors $s_1, \ldots, s_n \in \mathbf{V}[X_1, \ldots, X_k]^m$ generating the syzygy module of $p_1, \ldots, p_m$ over the quotient field $\mathbf{K}$ of $\mathbf{V}$ as a $\mathbf{V}[X_1, \ldots, X_k]$-module ($s_1, \ldots, s_n$ can be computed using Gröbner bases techniques). Then, the syzygy module $\mathcal{S}$ of $p_1, \ldots, p_m$ over $\mathbf{V}$ is nothing but the $\mathbf{V}$-saturation of $\mathcal{S}' = \langle s_1, \ldots, s_n \rangle$, i.e.,

$$\mathcal{S} := \{ s \in \mathbf{V}[X_1, \ldots, X_k]^m \mid \alpha\, s \in \mathcal{S}' \text{ for some }$$

$$\alpha \in \mathbf{V} \setminus \{0\} \} = (\mathcal{S}' \otimes_{\mathbf{R}} \mathbf{K}) \cap \mathbf{V}[X_1, \ldots, X_k]^m.$$

$$\mathbf{V} = \mathbb{Z}_{2\mathbb{Z}},$$

$$s_1 = ({\color{red}5},\, 4,\, -2X^2 - 6X + 12) \xrightarrow{\text{height}} (0, 1)$$



[defect=2]

$\mathbf{V} = \mathbb{Z}_{2\mathbb{Z}}$; $S := [s_1 = (5, 4, -2X^2 - 6X + 12), s_2 = (2X-1, 0, -2X^2 + 6X - 4)]$

$$\overset{\text{reduction}}{\Downarrow}$$

$S_0 = [(5, 4, -2X^2 - 6X + 12), (X, \frac{2}{5}, -\frac{6}{5}X^2 + \frac{12}{5}X - \frac{4}{5})]$; $\delta(S_0) = 1$

$$XS_0$$

$$\overset{\text{reduction}}{\Downarrow}$$

$S_1 = [(5X, 4X, -2X^3 - 6X^2 + 12X), (0, 2X-1, -X^3 + 2)]$; $\delta(S_1) = 0$

As a conclusion

$$\mathrm{Sat}(s_1, s_2)$$

$$= \langle (5, 4, -2X^2-6X+12), (X, \frac{2}{5}, -\frac{6}{5}X^2+\frac{12}{5}X-\frac{4}{5}),$$

$$(0, 2X-1, -X^3+2)\rangle.$$

Theorem: Let $S = [s_1, \dots, s_n]$ be a finite list of vectors in $\mathbf{V}[X]^m$ with degrees $\leq d$, where $\mathbf{V}$ is a valuation domain and $m \geq 1$. Then the "primitive triangulation algorithm" computes after $\min(n-1, m)d+1$ iterations a finite list G of vectors in $\mathbf{V}[X]^m$ of degrees $\leq (\min(n-1, m)+1)d$ generating $\mathrm{Sat}(\langle s_1, \dots, s_n \rangle)$ as a $\mathbf{V}[X]$-module.

In other terms, computing $\mathrm{Sat}(\langle s_1, \dots, s_n \rangle)$ amounts to performing gaussian elimination on a matrix of size $n(\min(n-1, m)d+1) \times m$ and with entries in $\mathbf{V}[X]$ of degrees $\leq (\min(n-1, m)+1)d$.

Proof. We denote by S_0 the list S put in an echelon form, and by induction $T_j = [S_0, \dots, S_j]$ where S_{j+1} denotes XS_j put in an echelon form with respect to T_j and then put in an echelon form, with the initialization $T_0 = S_0$.

Then the sequence $(\delta(S_j))_{j \geq 0}$ is non-increasing and becomes zero for $j \geq \min(n-1, m)d$.

Theorem: Let L be a finite list of vectors in $\mathbf{V}[X_1, \ldots, X_k]^m$, where $\mathbf{V}$ is a valuation domain of quotient field $\mathbf{K}$ and residue field $\mathbf{k}$. Then

- $\dim_{\mathbf{k}} L \leq \dim_{\mathbf{K}} L$,

- $\langle L \rangle_{\mathbf{V}}$ is $\mathbf{V}$-saturated if and only if $\dim_{\mathbf{K}} L = \dim_{\mathbf{k}} L$.

When a matrix over the integers is $\mathbb{Z}$-saturated ?

$A \in \mathbb{Z}^{m\times n}$; $\mathrm{rk}_0 A := \mathrm{rk}_{\mathbb{Q}} A$; $\mathrm{rk}_p A := \mathrm{rk}_{\mathbb{F}_p} A$;

$\mathbf{P}^* =$ the set of prime numbers; $\mathbf{P} := \mathbf{P}^* \cup \{0\}$.

Denoe by $p_1, \ldots, p_t$ the prime numbers dividing the denominators of the vectors obtained after putting the columns of A into an echelon form over $\mathbb{Q}$. Then the following assertions are equivalent:

(i) $\mathrm{Im}(A)$ is $\mathbb{Z}$-saturated.

(ii) $\mathrm{rk}_0 A = \mathrm{rk}_{p_1} A = \cdots = \mathrm{rk}_{p_t} A$.

(iii) The map $\mathrm{rk}(A) : \mathbf{P} \to \mathbb{N}$ defined by $\mathrm{rk}(A)(q) := \mathrm{rk}_q A$, is constant.

(iv) The map $\mathbf{P}^* \to \mathbb{N}$; $p \mapsto \mathrm{rk}_p A$, is constant.

Let $L = [u_1, \ldots, u_s]$ ($s \geq 1$) be a list of s polynomial vectors in $\mathbf{V}[X_1, \ldots, X_k]^m$, where $\mathbf{V}$ is a valuation domain of quotient field $\mathbf{K}$ and residue field $\mathbf{k}$. For $i \in \mathbb{N}$,

$$L_i := \langle M u_j;\ 1 \leq j \leq s,\ \mathrm{tdeg}(M) \leq i \rangle_{\mathbf{K}},$$

$$\bar{L}_i := \langle M \bar{u}_j;\ 1 \leq j \leq s,\ \mathrm{tdeg}(M) \leq i \rangle_{\mathbf{k}}.$$

$$h_{L,\mathbf{K}}(t) = \sum_{i \geq 0} (\dim_{\mathbf{K}} L_i)\, t^i,$$

$$h_{L,\mathbf{k}}(t) = \sum_{i \geq 0} (\dim_{\mathbf{k}} \bar{L}_i)\, t^i \leq h_{L,\mathbf{K}}(t),$$

$$\delta_L(t) := h_{L,\mathbf{K}}(t) - h_{L,\mathbf{k}}(t)$$

called the **saturation defect series** of the list L.

Note that

$$h_{L,\mathbf{K}}(t) = \mathrm{HS}_{\mathrm{Syz}_{\mathbf{K}}(u_1,\ldots,u_s)}(t).$$

Example: Consider the list $U = [u_1 = 1 + 2X, u_2 = 1 + 2Y]$ with $u_i \in \mathbb{Z}_{2\mathbb{Z}}[X, Y]$. We have:

$$h_{U,\mathbb{Q}}(t) = \frac{1}{(1-t)^3} + \frac{1}{(1-t)^2},$$

$$h_{U,\mathbb{Z}/2\mathbb{Z}}(t) = \frac{1}{(1-t)^3},$$

and, thus, the defect series of U is

$$\delta_U(t) = \frac{1}{(1-t)^2}.$$

Theorem: Let L be a finite list of vectors in $\mathbf{V}[X_1, \ldots, X_k]^m$, where $\mathbf{V}$ is a valuation domain. If $\delta_L = 0$ then $\langle L \rangle_{\mathbf{V}[X_1,\ldots,X_k]}$ is $\mathbf{V}$-saturated.

Saturation algorithm in the multivariate case:

Input: A finite list $S = [s_1, \ldots, s_n]$ of vectors in $\mathbf{V}[X_1, \ldots, X_k]^m$, where $\mathbf{V}$ is a valuation domain and $m \geq 1$.

Output: A finite list G of vectors in $\mathbf{V}[X_1, \ldots, X_k]^m$ generating Sat$(\langle s_1, \ldots, s_n \rangle)$ as a $\mathbf{V}[X_1, \ldots, X_k]$-module.

We denote by S_0 the list S put in an echelon form, and by induction $T_j = [S_0, \ldots, S_j]$ where S_{j+1} denotes $[X_1 S_j, \ldots, X_k S_j]$ put in an echelon form with respect to T_j and then put in an echelon form, with the initialization $T_0 = S_0$.

We begin by putting S in an echelon form (it becomes S_0) and then compute its defect series $\delta_{S_0}(t)$. If $\delta_{S_0}(t) = 0$ then stop; else compute S_1. If $\delta_{S_1}(t) = 0$ then stop; else compute S_2, and so on.

Example: $U = [u_1 = 1 + 2X, u_2 = 1 + 2Y]$ with $u_i \in \mathbb{Z}_{2\mathbb{Z}}[X, Y]$. As $\delta_U(t) = \frac{1}{(1-t)^2} \neq 0$, one has to put U in an echelon form. This can be done as follows:

$$U = [u_1 = 1 + 2X, u_2 = 1 + 2Y] \rightarrow$$

$$U_0 := [u_1, \frac{1}{2}(u_2 - u_1)] = [1 + 2X, Y - X].$$

As $h_{U_0,\mathbb{Q}}(t) = h_{U_0,\mathbb{Z}/2\mathbb{Z}}(t) = \frac{1}{(1-t)^3} + \frac{1}{(1-t)^2}$, we have $\delta_{U_0}(t) = 0$. We conclude that

$$\mathrm{Sat}(\langle u_1, u_2 \rangle) = \langle 1 + 2X, Y - X \rangle.$$

References:

• 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*. Communications in Algebra **42:9** (2014) 3768–3781.

• Ducos L., Monceur S., Yengui I. *Computing the* $\mathbf{V}$*-saturation of finitely-generated submodules of* $\mathbf{V}[X]^m$ *where* $\mathbf{V}$ *is a valuation domain*. J. Symb. Comput., in press.

• Ducos L., Valibouze A., Yengui I. *Computing syzygies over* $\mathbf{V}[X_1, \ldots, X_k]$, $\mathbf{V}$ *a valuation domain*. J. Algebra **425** (2015) 133–145.

• Yengui I. *Constructive Commutative Algebra*. Lecture Notes in Mathematics, no 2138, Springer 2015.

DANKE