Recent Progress for Computing Gröbner Bases

Shuhong Gao
Clemson University

Joint with
Frank Volny IV (National Security Agency)
Mingsheng Wang (Chinese Academy of Sciences)

Workshop on Computer Algebra and Polynomials
RICAM, Linz, Austria
November 25–29, 2013

New Criterion (G., Volny and Wang 2011)

$g_1, \ldots, g_m \in R = \mathbb{F}[x_1, \cdots, x_n]$: any given polynomials
$\mathbf{e}_1, \ldots, e_m \in R^m$: the unit vectors

Consider the R-submodule of $R^m \times R$:

$$\begin{aligned} M &= \langle (\mathbf{e}_1, g_1), \ldots, (\mathbf{e}_m, g_m) \rangle_R \\ &= \{(\mathbf{u}, v) \in R^m \times R : \mathbf{u}\mathbf{g}^t = v\} \end{aligned}$$

where $\mathbf{u}\mathbf{g}^t = u_1 g_1 + \cdots + u_m g_m$.

Theorem

Suppose G is a subset of M containing $(\mathbf{e}_1, g_1), \ldots, (\mathbf{e}_m, g_m)$. For any term order on R and any compatible term order on R^m, the following are equivalent:

(a) *G is a strong Gröbner basis for M,*

(b) $\cdots\cdots\cdots\cdots$

(c) *every J-pair of G is covered by G.*

Condition (c)

Let $G = \{(\mathbf{u}_1, v_1), (\mathbf{u}_2, v_2), \ldots, (\mathbf{u}_r, v_r)\} \subset R^m \times R$. We say

- a pair $p = (\mathbf{u}, v) \in R^m \times R$ with $v \neq 0$ is covered by G if there is a pair $p_i = (\mathbf{u}_i, v_i) \in G$ and a monomial $t \in R$ so that

$$\operatorname{lm}(\mathbf{u}) = t \operatorname{lm}(\mathbf{u}_i), \quad \text{and} \quad t \operatorname{lm}(v_i) \prec \operatorname{lm}(v).$$

  In this case, we say p_i covers p. Transitive relation

- a pair $(\mathbf{u}, 0) \in R^m \times R$ is covered by G if there is a pair $(\mathbf{u}_i, 0) \in G$ and a monomial $t \in R$ so that

$$\operatorname{lm}(\mathbf{u}) = t \operatorname{lm}(\mathbf{u}_i).$$

Remark. The condition (c) corresponds to F5 rewritten rules and is used in F5, Arri and Perry (2011) and in many recent papers.

Condition (c): Example

Let $R = \mathbb{F}[x, y, z]$ under the graded lex order with $x > y > z$. In $R^3 \times R$, suppose G contains the following pairs:

$$p_4 = (yz\mathbf{e}_1 + \cdots, 0), \; p_5 = (xz\mathbf{e}_2 + \cdots, 0), \; p_6 = (z\mathbf{e}_1 + \cdots, y + \cdots).$$

Then

$$\begin{array}{rcc}
(xz^2\mathbf{e}_2 + \cdots, 0) & \text{is covered by} & p_5, \\
(y^2z\mathbf{e}_1 + \cdots, z + \cdots) & \text{is covered by} & p_4, \\
(xz\mathbf{e}_1 + \cdots, x^2 + \cdots) & \text{is covered by} & p_6, \\
(xz\mathbf{e}_1 + \cdots, y^2 + \cdots) & \text{is not covered by} & p_6
\end{array}$$

as $xp_6 = (xz\mathbf{e}_1 + \cdots, xy + \cdots)$ and $y^2 \prec xy \prec x^2$. (In fact, the last pair is not covered by G.)

Recall Gröbner Bases

Definition

For any **term order** in $R = \mathbb{F}[x_1, \ldots, x_n]$, a subset $G = \{g_1, \ldots, g_r\}$ of an ideal $\mathbf{I} \subset R$ is called a **Gröbner basis** (GB) for $\mathbf{I}$ if every $f \in \mathbf{I}$ is **top-reducible** by G, that is, there exists some $g \in G$ such that $\mathrm{lm}(g)$ divides $\mathrm{lm}(f)$.

The corresponding reduction is

$$f := f - ctg$$

where $t = \mathrm{lm}(f)/\mathrm{lm}(g)$ is a monomial and $c = \mathrm{lc}(f)/\mathrm{lc}(g) \in \mathbb{F}$.

S-polynomials

Definition

Let $f, g \in R$. The **S-polynomial** of f and g is defined to be

$$S(f,g) = t_1 f - c t_2 g$$

where $c = \mathrm{lc}(f)/\mathrm{lc}(g)$ and

$$t_1 = \frac{\mathrm{lcm}(\mathrm{lm}(f), \mathrm{lm}(g))}{\mathrm{lm}(f)}, \; t_2 = \frac{\mathrm{lcm}(\mathrm{lm}(f), \mathrm{lm}(g))}{\mathrm{lm}(g)}.$$

- For example, $f = 4x^3y^4 + \cdots$, and $g = 5x^4yz^2 + \cdots$,

$$S(f,g) = (5xz^2)f - (4y^3)g = xz^2(4x^3y^4 + \cdots) - \frac{4}{5}y^3(5x^4yz^2 + \cdots).$$

Buchberger's Criterion (1965)

Theorem

A subset $G = \{g_1, \ldots, g_r\}$ of an ideal $\mathbf{I} \subseteq R$ is a Gröbner basis for $\mathbf{I}$ iff every S-polynomial of G can be top-reduced to zero by G.

Detecting useless S-polynomials

- Buchberger (1979): If $\gcd(\text{lm}(g_i), \text{lm}(g_j)) = 1$ then $S(g_i, g_j)$ can be top-reduced to 0 by G.
- Lazard (1983), Möller, Mora and Traverso (1992):

$$\text{syzygies} \longleftrightarrow \text{"reduction to 0"}.$$

For $(g_1, \ldots, g_m) \in R^m$, its syzygy module is defined as

$$H = \{\mathbf{u} = (u_1, \ldots, u_m) \in R^m : u_1 g_1 + \cdots + u_m g_m = 0\}.$$

- Faugère (F5, 2002): Introduces signatures and uses principal syzygies to detect useless S-polynomials.

Recent papers

- Bardet (PhD Thesis, 2006), Stegers (2006), Gash (PhD thesis, 2008), Eder and Perry (2009), Sun and Wang (2009),
- Hashemi and Ars (2010), Sun and Wang (2010), G., Guan and Volny (2010), Zobnin (2010),
- G., Volny and Wang (2010/2011), Volny (PhD Thesis, 2011),
- Huang (2010), Eder and Perry (2010),
- Arri and Perry (2011), Eder and Perry (2011), Eder, Gash, Perry (2011), Sun and Wang (2011), Bigatti, Caboara and Robbiano (2011),
- Roune and Stillman (2012), Galkin (2012), Sun and Wang (2012),
- Eder (2013), Eder and Roune (2013), Gerdt and Hashime (2013), Pan, Hu and Wang (2013), Sun and Wang (2013),
- Simões (PhD thesis, 2013), Sun (2013).
- ....

Notations

Let $R = \mathbb{F}[x_1, \cdots, x_n]$. A monomial in R is written as

$$x^\alpha = x_1^{a_1} \cdot x_2^{a_2} \cdots x_n^{a_n}.$$

A term in R^m is of the form $x^\alpha \mathbf{e}_i$, $1 \leq i \leq m$.

Fix any term order $\prec_1$ on R and any term order $\prec_2$ on R^m. We say they are **compatible** if, for each $1 \leq i \leq m$,

$$x^\alpha \prec_1 x^\beta \text{ iff } x^\alpha \mathbf{e}_i \prec_2 x^\beta \mathbf{e}_i.$$

Signatures

Faugère (2002): For any polynomial $v \in I = \langle g_1, \ldots, g_m \rangle$, **the signature** of v is

$$\min\{\mathrm{lm}(\mathbf{u}) : \mathbf{u} = (u_1, \ldots u_m) \in R^m \text{ and } u_1 g_1 + \cdots + u_m g_m = v\}.$$

This definition is still used in Arri and Perry (2011) and many of the recent papers.

Signatures

Faugère (2002): For any polynomial $v \in I = \langle g_1, \ldots, g_m \rangle$, **the signature** of v is

$$\min\{\mathrm{lm}(\mathbf{u}) : \mathbf{u} = (u_1, \ldots u_m) \in R^m \text{ and } u_1 g_1 + \cdots + u_m g_m = v\}.$$

This definition is still used in Arri and Perry (2011) and many of the recent papers.

Definition

For any $(\mathbf{u}, v) \in R^m \times R$, we call $\mathrm{lm}(\mathbf{u})$ **the signature** of $(\mathbf{u}, v)$.

This is much easier to use in practice!

Top-reductions

Let $p_1 = (\mathbf{u}_1, v_1), p_2 = (\mathbf{u}_2, v_2) \in R^m \times R$ be any two pairs. When v_2 is nonzero, we say p_1 is top-reducible by p_2 if

(i) v_1 is nonzero and $\mathrm{lm}(v_2)$ divides $\mathrm{lm}(v_1)$; and

(ii) $\mathrm{lm}(t\mathbf{u}_2) \preceq \mathrm{lm}(\mathbf{u}_1)$ where $t = \mathrm{lm}(v_1)/\mathrm{lm}(v_2)$.

Top-reductions

Let $p_1 = (\mathbf{u}_1, v_1), p_2 = (\mathbf{u}_2, v_2) \in R^m \times R$ be any two pairs. When v_2 is nonzero, we say p_1 is top-reducible by p_2 if

(i) v_1 is nonzero and $\mathrm{lm}(v_2)$ divides $\mathrm{lm}(v_1)$; and

(ii) $\mathrm{lm}(t\mathbf{u}_2) \preceq \mathrm{lm}(\mathbf{u}_1)$ where $t = \mathrm{lm}(v_1)/\mathrm{lm}(v_2)$.

The corresponding **top-reduction** is then

$$p_1 - ctp_2 = (\mathbf{u}_1 - ct\mathbf{u}_2, v_1 - ctv_2), \tag{1}$$

where $c = \mathrm{lc}(v_1)/\mathrm{lc}(v_2)$.

Top-reductions

Let $p_1 = (\mathbf{u}_1, v_1), p_2 = (\mathbf{u}_2, v_2) \in R^m \times R$ be any two pairs.
When v_2 is nonzero, we say p_1 is top-reducible by p_2 if

(i) v_1 is nonzero and $\text{lm}(v_2)$ divides $\text{lm}(v_1)$; and

(ii) $\text{lm}(t\mathbf{u}_2) \preceq \text{lm}(\mathbf{u}_1)$ where $t = \text{lm}(v_1)/\text{lm}(v_2)$.

The corresponding **top-reduction** is then

$$p_1 - ctp_2 = (\mathbf{u}_1 - ct\mathbf{u}_2, v_1 - ctv_2), \tag{1}$$

where $c = \text{lc}(v_1)/\text{lc}(v_2)$.
Such a top-reduction is called **regular**, if

$$\text{lm}(\mathbf{u}_1 - ct\mathbf{u}_2) = \text{lm}(\mathbf{u}_1),$$

and **super** otherwise.

Top-reductions

When $v_2 = 0$, we say that p_1 is **top-reducible** by $(\mathbf{u}_2, 0)$ if $\mathbf{u}_1$ and $\mathbf{u}_2$ are both nonzero and $\mathrm{lm}(\mathbf{u}_2)$ divides $\mathrm{lm}(\mathbf{u}_1)$.

Top-reductions

When $v_2 = 0$, we say that p_1 is **top-reducible** by $(\mathbf{u}_2, 0)$ if $\mathbf{u}_1$ and $\mathbf{u}_2$ are both nonzero and $\mathrm{lm}(\mathbf{u}_2)$ divides $\mathrm{lm}(\mathbf{u}_1)$.

So the signature of p_1 remains the same under a regular top-reduction but becomes smaller under a super top-reduction.

Strong Gröbner basis

Recall that, for any $g_1, g_2, \ldots, g_m \in R = \mathbb{F}[x_1, \cdots, x_n]$,

$$\begin{aligned} M &= \langle (\mathbf{e}_1, g_1), \ldots, (\mathbf{e}_m, g_m) \rangle_R \\ &= \{ (u_1, \ldots, u_m, v) \in R^m \times R : v = u_1 g_1 + \cdots + u_m g_m \}. \end{aligned}$$

Definition

A subset G of M is called a **Strong Gröbner basis for** M if every pair in M is top-reducible by some pair in G.

Strong GB $\Longrightarrow$ GB for I and GB for syzygies

Suppose that $G = \{(\mathbf{u}_1, v_1), \ldots, (\mathbf{u}_k, v_k)\} \subset R^m \times R$ is a strong Gröbner basis for M. Then

1. a Gröbner basis for the syzygy module of $\mathbf{g} = (g_1, \ldots, g_m)$ is

$$\mathbf{G}_0 = \{\mathbf{u}_i : v_i = 0, 1 \leq i \leq k\},$$

2. and a Gröbner basis for $I = \langle g_1, \ldots, g_m \rangle$ is

$$G_1 = \{v_i : 1 \leq i \leq k\}.$$

J-pairs

Let $p_1 = (\mathbf{u}_1, v_1), p_2 = (\mathbf{u}_2, v_2) \in R^m \times R$ be any two pairs. We form a J-pair only if v_1 **and** v_2 **are both nonzero**.

Recall the S-polynomial of v_1 and v_2 is $t_1 v_1 - c t_2 v_2$ where $c = \mathrm{lc}(v_1)/\mathrm{lc}(v_2)$, and

$$t = \mathrm{lcm}(\mathrm{lm}(v_1), \mathrm{lm}(v_2)), \quad t_1 = \frac{t}{\mathrm{lm}(v_1)}, \quad t_2 = \frac{t}{\mathrm{lm}(v_2)}.$$

J-pairs

For pairs, we have

$$t_1 p_1 - ct_2 p_2 = (t_1 \mathbf{u}_1 - ct_2 \mathbf{u}_2, t_1 v_1 - ct_2 v_2).$$

Suppose

$$T = \max(t_1 \mathrm{lm}(\mathbf{u}_1), t_2 \mathrm{lm}(\mathbf{u}_2)) = t_i \mathrm{lm}(\mathbf{u}_i)$$

where $i \in \{1, 2\}$.

Definition

If $\mathrm{lm}(t_1 \mathbf{u}_1 - ct_2 \mathbf{u}_2) = T$ then

- T is called the **J-signature** of p_1 and p_2, and
- $t_i p_i$ is called the **J-pair** of p_1 and p_2, denoted as $J(p_1, p_2)$.

Examples

$R = \mathbb{F}[x, y, z]$ under the graded lex order with $x \prec y \prec z$, $R^3 \times R$ with TOP (term over position) with $\mathbf{e}_3 \prec \mathbf{e}_2 \prec \mathbf{e}_1$.

$$p_1 = (\mathbf{e}_1, 5xy + \cdots), \qquad p_2 = (\mathbf{e}_2, 3yz + \cdots)$$
$$p_3 = (\mathbf{e}_3, 4xz + \cdots), \qquad p_4 = (x\mathbf{e}_2 + \cdots, x^2 + \cdots)$$

Some J-pairs:

$$\begin{aligned} (1,2): zp_1 &= (z\mathbf{e}_1, 5xyz + \cdots), & J(p_1, p_2) &= zp_1 \\ xp_2 &= (x\mathbf{e}_2, 3xyz + \cdots, & \text{as } x\mathbf{e}_2 &\prec z\mathbf{e}_1 \end{aligned}$$

$$\begin{aligned} (1,3): zp_1 &= (z\mathbf{e}_1, 5xyz + \cdots), & J(p_1, p_3) &= zp_1 \\ yp_3 &= (y\mathbf{e}_3, 4xyz + \cdots, & \text{as } y\mathbf{e}_3 &\prec z\mathbf{e}_1. \end{aligned}$$

New Criterion

Theorem (G, Volny and Wang)

Suppose G is a subset of M that contains $(\mathbf{e}_1, g_1), \ldots, (\mathbf{e}_m, g_m)$. Then the following are equivalent:

(a) *G is a strong Gröbner basis for M,*

(b) *every J-pair of G is eventually super top-reducible by G,*

(c) *every J-pair of G is covered by G.*

Useless pairs

Corollary

Any J-pair satisfying (c) should be discarded.

Special cases:

- Syzygy rule
- F5 rewritten rule

Useless pairs

Example. Let $R = \mathbb{F}[x, y, z]$ under the graded lex order with $x > y > z$. In $R^3 \times R$, suppose G contains the following pairs:

$$p_4 = (yz\mathbf{e}_1 + \cdots, 0),\ p_5 = (xz\mathbf{e}_2 + \cdots, 0),\ p_6 = (z\mathbf{e}_1 + \cdots, y + \cdots).$$

Then

$$\begin{array}{rcl}
(xz^2\mathbf{e}_2 + \cdots, 0) & \text{is covered by} & p_5,\ \text{syzygy rule} \\
(y^2z\mathbf{e}_1 + \cdots, z + \cdots) & \text{is covered by} & p_4,\ \text{syzygy rule} \\
(xz\mathbf{e}_1 + \cdots, x^2 + \cdots) & \text{is covered by} & p_6,\ \text{F5 Rewritten rule} \\
(xz\mathbf{e}_1 + \cdots, y^2 + \cdots) & \text{is not covered by} & p_6
\end{array}$$

as $xp_6 = (xz\mathbf{e}_1 + \cdots, xy + \cdots)$ and $y^2 \prec xy \prec x^2$. (In fact, the last pair is not covered by G.)

Remarks on implementation

- **Store only the signature $\mathrm{lm}(\mathbf{u})$, not the whole vector $\mathbf{u}$.** This gives Gröbner basis for $\mathbf{I}$ and the minimal leading term of the syzygy module.
- **Use principal syzygies**. Any two pairs $p_1 = (\mathbf{u}_1, v_1)$ and $p_2 = (\mathbf{u}_2, v_2)$ give a principal syzygy:

$$v_2 p_1 - v_1 p_2 = (\mathbf{u}, 0).$$

- **Delete** every J-pair that is covered by a pair in G or H (recorded syzygies), or by another J-pair.
- The J-pairs can be processed in any order.

Finite termination

Theorem

The GVW algorithm terminates in finitely many steps if the term orders $\prec_1$ on R and $\prec_2$ on R^m are compatible.

- Huang (2010) proved the case when pairs are processed by increasing order. He also gives a nice example to show that the algorithm may not terminate if the signature order and the polynomial order are not compatible.
- There are several flawed proofs for F5: e.g. Hashemi and Ars (2010), Arri and Perry (2011).

Minimal Strong Gröbner bases

Theorem

If the J-pairs are processed in increasing order, then one gets a minimal strong Gröbner basis.

This means that the algorithm does not perform reduction to any extra J-pairs other than the ones in the minimal basis.

Specific Term Orders

Let $\prec$ be some term order on R. We extend $\prec$ to R^m as follows.

(POT) The first is called position over term ordering (POT). We say that $x^\alpha \mathbf{E}_i \prec x^\beta \mathbf{E}_j$ if $i < j$ or $i = j$ and $x^\alpha \prec x^\beta$.

(TOP) The second is the term over position ordering (TOP). We say that $x^\alpha \mathbf{E}_i \prec x^\beta \mathbf{E}_j$ if $x^\alpha \prec x^\beta$ or $x^\alpha = x^\beta$ and $i < j$.

(g1) Next is the **g**-weighted degree followed by TOP. We say that $x^{\alpha}\mathbf{E}_i \prec x^{\beta}\mathbf{E}_j$ if $\deg(x^{\alpha}g_i) < \deg(x^{\beta}g_j)$ or $\deg(x^{\alpha}g_i) = \deg(x^{\beta}g_j)$ and $x^{\alpha}\mathbf{E}_i \prec_{top} x^{\beta}\mathbf{E}_j$ where deg is for total degree.

(g2) Finally, we have **g**-weighted $\prec$ followed by POT. We say that $x^{\alpha}\mathbf{E}_i \prec x^{\beta}\mathbf{E}_j$ if $\mathrm{lm}(x^{\alpha}g_i) \prec \mathrm{lm}(x^{\beta}g_j)$ or $\mathrm{lm}(x^{\alpha}g_i) = \mathrm{lm}(x^{\beta}g_j)$ and $x^{\alpha}\mathbf{E}_i \prec_{pot} x^{\beta}\mathbf{E}_j$. Called Schreier oder.

Under the POT order, our algorithm corresponds with the G2V algorithm.

Under the ordering **g**1, our algorithm is related to the XL algorithm but much faster.

GVW algorithm under different term orders

Test Case (# gen)	POT (G2V)	TOP	g1	g2
Katsura5 (22)	4.32	0.91	1	0.65
Katsura6 (41)	14.21	5.76	6.29	3.75
Katsura7 (74)	169.63	33.1	34.66	19.9
Katsura8 (143)	1994.86	214.91	224.18	137.39
Schrans-Troost (128)	2106.48	81.86	85.2	95.62
F633 (76)	71.74	42.8	44.78	36.64
Cyclic 6 (99)	111.81	7539.49	7296.54	128.51
Cyclic 7 (443)	44078.6	-	-	24237.8

Table : Runtime in seconds using Singular 3110 on an Intel Core 2 Quad 2.66 GHz processor

Recent works and Open problems

- Yao Sun (August 2013): View GVW algorithm as **GB conversion** via the MMM algorithm of Marinari, Möller, and Mora (1992) or the FGLM algorithm of Faugére, Gianni, Lazard, and Mora (1993).
- Bruno Simões (PhD Thesis, April 2013): Use Hilbert functions.

Recent works and Open problems

- Yao Sun (August 2013): View GVW algorithm as **GB conversion** via the MMM algorithm of Marinari, Möller, and Mora (1992) or the FGLM algorithm of Faugére, Gianni, Lazard, and Mora (1993).
- Bruno Simões (PhD Thesis, April 2013): Use Hilbert functions.
- Improve on bounds for the degree D so that

$$\{u_1 g_1 + \cdots + u_m g_m : u_i \in \mathbb{F}[x_1, \ldots x_n], \deg(u_i) \leq D\}$$

  contains a Gröbner basis. This is closely related to the Castelnuovo-Mumford regularity (assuming g_i's are homogeneous).

Thank you!