Recent Progress for Computing Gröbner Bases

Shuhong Gao

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

Simons Institute for the Theory of Computing
October 16, 2014

1. Gröbner bases and Buchberger's algorithm
2. General framework and new criterion
3. Comparisons and complexity issues

Gröbner Bases

Let $f_1, \ldots, f_m \in R = \mathbb{F}[x_1, \cdots, x_n]$ and define an **ideal** in R:

$$\mathbf{I} = \langle f_1, \ldots, f_m \rangle = \{u_1 f_1 + \cdots + u_m f_m : u_1, \ldots, u_m \in R\}.$$

Definition

For any **monomial order**, a subset $G = \{g_1, \ldots, g_m\} \subseteq \mathbf{I}$ is called a **Gröbner basis** (GB) for $\mathbf{I}$ if every $f \in \mathbf{I}$ is **reducible** by G, that is, there exists some $g \in G$ such that $\mathrm{lm}(g)$ divides $\mathrm{lm}(f)$.

Remarks

- When all f_i's are linear, then a Gröbner basis corresponds to "row Echelon form" or "triangular system".
- When all f_i's are univariate, then a Gröbner basis corresponds to $\gcd(f_1, \ldots, f_m)$.
- In general, a Gröbner basis for an ideal $\mathbf{I}$ consists of all the "smallest polynomials" in $\mathbf{I}$ under the given monomial order.
- For $R = \mathbb{F}[x_1, \cdots, x_n]$, the concept of Gröbner basis can also be defined for any R-submodule of R^t. We contend ourself to $t = 1$ in this talk.
- **Gröbner bases are extremely useful ....**

Monomial Orderings

Let $\mathbb{N} = \{0, 1, 2, 3, \cdots\}$. Each $\alpha = (a_1, a_2, \ldots, a_n) \in \mathbb{N}^n$ corresponds to a monomial

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

We say that $\prec$ is a **monomial order** or **term order** if

1. $\prec$ is a total ordering on all the monomials of R,
2. If $x^\alpha \prec x^\beta$, then $x^\alpha \cdot x^\gamma \prec x^\beta \cdot x^\gamma$ for each $\gamma \in \mathbb{N}^n$ (**compatible with multiplication**),
3. $\mathrm{lm}(f)$ and $\mathrm{lc}(f)$: leading monomial and leading coefficient.

Monomial Orderings

- **Lex order**: Under lex with $x > y > z$:

$$f = 10x - 7y^4 + 11y^3z, \qquad \mathrm{lm}(f) = x, \quad \mathrm{lc}(f) = 10.$$

- **Graded lex order**: Under graded lex order with $x > y > z$:

$$f = -7y^4 + 11y^3z + 10x, \qquad \mathrm{lm}(f) = y^4, \quad \mathrm{lc}(f) = -7.$$

Top reductions

$R = \mathbb{F}[x_1, \cdots, x_n]$
$f \in R$: any polynomial
$G \subseteq R$: any set of polynomials

Definition

f is called **reducible** by G if there is a polynomial $g \in G$ so 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, let

$$f = 4x^3y^4 + \cdots, \qquad g = 5x^4yz^2 + \cdots.$$

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

Buchberger's Criterion (1965)

Theorem

Suppose $G = \{g_1, \ldots, g_m\}$ *generate an ideal* $\mathbf{I} \subseteq R$. *Then* G *is a Gröbner basis for* $\mathbf{I}$ *iff, for every pair* $1 \leq i < j \leq m$, $S(g_i, g_j)$ *reduces to zero by* G.

Buchberger's Algorithm

- The criterion tells us exactly what must be done.
- Suppose $G = \{g_1, \ldots, g_m\}$ is any given list of polynomials.

Algorithm

(1) *For each pair g_i and g_j from G,*

(1a) *Reduce $S(g_i, g_j)$ by G until not reducible by G,*

(1b) *If the remainder is nonzero, add it to G.*

(2) *Repeat Step 1 until all S-polynomials of G reduce to 0.*

Buchberger's Algorithm

- The criterion tells us exactly what must be done.
- Suppose $G = \{g_1, \ldots, g_m\}$ is any given list of polynomials.

Algorithm

(1) *For each pair g_i and g_j from G,*

   (1a) *Reduce $S(g_i, g_j)$ by G until not reducible by G,*

   (1b) *If the remainder is nonzero, add it to G.*

(2) *Repeat Step 1 until all S-polynomials of G reduce to 0.*

- **Step (1a) is very expensive, and many S-polynomials reduce to 0!**
- **How to detect such S-polynomials without performing reductions?**

Detecting useless S-polynomials

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

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

  Lazard also pointed the relationship between Gröbner bases and Gauss elimination of the Sylvester matrix.

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

- 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).
- ....

General framework

Let $g_1, \ldots, g_m \in R = \mathbb{F}[x_1, \cdots, x_n]$. Define

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

called **the syzygy module** of $\mathbf{g} = (g_1, \ldots, g_m)$.

Problem

Given $g_1, \ldots, g_m \in R$, we wish to compute a Gröbner basis for the ideal $I = \langle g_1, \ldots, g_m \rangle$ and a Gröbner basis for the syzygy module H.

General framework

$R = \mathbb{F}[x_1, \cdots, x_n]$
A monomial in R:

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

A term in R^m is of the form $x^\alpha \mathbf{E}_i$ where

$$\mathbf{E}_i = (0, \ldots, 0, 1, 0, \ldots, 0) \in R^m$$

the i^{th} unit vector $1 \leq i \leq m$.

General framework

$R = \mathbb{F}[x_1, \cdots, x_n]$
A monomial in R:

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

A term in R^m is of the form $x^\alpha \mathbf{E}_i$ where

$$\mathbf{E}_i = (0, \ldots, 0, 1, 0, \ldots, 0) \in R^m$$

the i^{th} unit vector $1 \leq i \leq m$.

Fix any term order $\prec_1$ on R and any term order $\prec_2$ on R^m (**compatible**), the latter is also called a **signature order**.
For any $v \in R$ and $\mathbf{u} \in R^m$, let

$$\mathrm{lm}(v) = \mathrm{lm}_{\prec_1}(v), \quad \mathrm{lm}(\mathbf{u}) = \mathrm{lm}_{\prec_2}(\mathbf{u}).$$

Signatures

Faugère (F5, 2002): For any polynomial $v \in I = \langle g_1, \ldots, g_m \rangle$, **the signature** of v is

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

Signatures

Faugère (F5, 2002): For any polynomial $v \in I = \langle g_1, \ldots, g_m \rangle$, **the signature** of v is

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

Definition

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

This allows us to deal with the ideal and the syzygy module at the same time.

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

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

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

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

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 $\mathrm{lm}(\mathbf{u}_1)$.

Remarks:

- So the signature of p_1 remains the same under a regular top-reduction but becomes smaller under a super top-reduction.
- In implementation, only regular top-reductions are performed!!!

Strong Gröbner basis

For any $g_1, g_2, \ldots, g_m \in R$, define the following R-submodule of $R^m \times R$:

$$M = \left\{(\mathbf{u}, v) \in R^m \times R : \mathbf{u}\mathbf{g}^t = u_1 g_1 + u_2 g_2 + \cdots + u_m g_m = v\right\}.$$

Then M is generated by

$$(\mathbf{E}_1, g_1), (\mathbf{E}_2, g_2), \ldots, (\mathbf{E}_m, g_m).$$

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 $\mathbf{I}$ 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
$$\mathbf{G}_0 = \{\mathbf{u}_i : v_i = 0, 1 \le i \le k\},$$
2. and a Gröbner basis for $I = \langle g_1, \ldots, g_m \rangle$ is
$$G_1 = \{v_i : 1 \le i \le k\}.$$

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

$$t_1 p_1 - c t_2 p_2 = (t_1 \mathbf{u}_1 - c t_2 \mathbf{u}_2, t_1 v_1 - c t_2 v_2).$$

Let

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

say $T = t_i \mathrm{lm}(\mathbf{u}_i)$ where $i \in \{1, 2\}$.

Definition

If $\mathrm{lm}(t_1 \mathbf{u}_1 - c t_2 \mathbf{u}_2) = T$ 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.

New Criterion

Theorem (G, Volny and Wang 2011)

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.
- 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

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

This is a transitive relation, useful in implementation.

Remarks on implementation

- The condition (c) can easily explain the F5 rewritten rules used in F5, Arri and Perry (2011) and in many recent papers.
- Store only the signature $\text{lm}(\mathbf{u})$, not the whole vector $\mathbf{u}$. This gives Gröbner basis for $\mathbf{I}$ and the minimal leading terms of the syzygy module.
- Use **trivial syzygies**. Any two pairs $p_1 = (\mathbf{u}_1, v_1)$ and $p_2 = (\mathbf{u}_2, v_2)$ give a trivial syzygy:

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

- **Finite Termination**: The criterion allows for a simple proof of finite termination of algorithms.

Specific Signature Orders

Let $\prec$ be some term order on R. We can 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 $i < j$.

Specific Signature Orders

(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 signature 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

Complexity Issues

- A minimal Gröbner basis with exponentially many polynomials:

$$\mathbf{I} = \langle f, x_1^2 - x_1, x_2^2 - x_2, x_n^2 - x_n \rangle \subset \mathbb{F}_2[x_1, x_2, \ldots, x_n],$$

  where f is **quadratic** (with rank $n/2$).
- #P complete:

$$\mathbf{I} = \langle f, x_1^2 - x_1, x_2^2 - x_2, x_n^2 - x_n \rangle \subset \mathbb{F}_2[x_1, x_2, \ldots, x_n],$$

  where f is **cubic**, as counting the number of $\mathbb{F}_2$-solutions of cubic polynomials is #P complete.

Complexity Issues

More generally, let $g_1, \ldots, g_m \in \mathbb{F}[x_1, \ldots x_n]$ with total degree $\leq d$. Define D be the smallest integer 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 number is closely related to the Castelnuovo-Mumford regularity (assuming g_i's are homogeneous).

Complexity Issues

- When the Gröbner basis contains 1 (so no solutions), Professor Krick talked about this on Tuesday:

$$(d-1)d^{n-1} \le D \le \max\{3, n\}^n$$

due to Masser and Phillipon, Kollar (1988), ...

- Mayr and Meyer (1982) give an example with D at least double exponential, and Dubé (1990) showed that

$$D \le 2\left(\frac{d^2}{2} + d\right)^{2^{n-1}}.$$

- (**Good news**) For zero dimensional homogeneous ideals, Lazard (1983) proved that,

$$D \le n(d-1),$$

after a generic linear change of variables and under graded reverse lex order.

Thank you!