Extending the GVW Algorithm to Local Ring

Fanghui Xiao

Key Laboratory of Mathematics Mechanization,
Academy of Mathematics and Systems Science, CAS

Joint work with Dong Lu, Dingkang Wang and Jie Zhou

July 16-19, 2018, City University of New York, USA

1. Problem
2. Previous Works
3. Proposed Algorithm
4. An Example
5. Implementation
6. Conclusion

Notations

- k : a field.
- $k[X]$: the polynomial ring in the variables $X = \{x_1, \ldots, x_n\}$.
- $R = \{f/(1+g) : f, g \in k[X], g(\mathbf{0}) = 0\}$: the local ring w.r.t. a local order $\succ$.
- $I = \langle f_1, \ldots, f_m \rangle$: an ideal.
- $\mathbf{e}_i$: the i-th unit vector of R^m.
- lm : leading monomial.

Definition 1 (Standard basis)

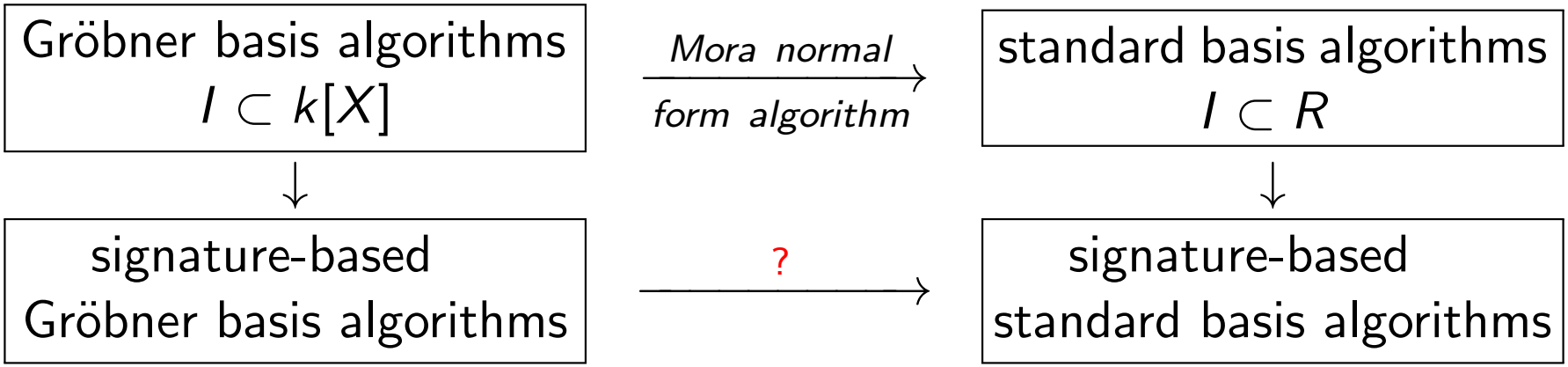
Let $\succ$ be a semigroup order, and I be an ideal in R or $k[X]$. A **standard basis** of I is a set $\{g_1, \ldots, g_s\}$ in I such that

$$\langle \mathrm{lm}(g_1), \ldots, \mathrm{lm}(g_s) \rangle = \langle \mathrm{lm}(I) \rangle.$$

$$I \subset k[X] \longleftrightarrow \text{Gröbner basis}$$
$$I \subset R \longleftrightarrow \text{standard basis}$$

Problem: How to find a new and efficient algorithm to compute the standard bases of ideals in a local ring?

Problem: How to find a new and efficient algorithm to compute the standard bases of ideals in a local ring?



- **Original classical algorithm:**
  - H. Hironaka: Resolution of singularities of an algebraic variety over a field of characteristic zero, 1964. (standard basis)
  - B. Buchberger: Ein Algorithmus zum Auffinden der Basiselemente des Restklassenrings nach einem nulldimensionalen Polynomideal, 1965. (Buchberger's algorithm)
  - F. Mora: An algorithm to compute the equations of tangent cones, 1982. (Mora's algorithm)
  - D. Lazard: Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations, 1983. (Lazard's homogenization approach)

- **Signature-based Gröbner basis algorithms**
  - J.-C. Faugère: A new efficient algorithm for computing Gröbner bases without reduction to zero (F5), 2002. (F5 algorithm)
  - S.H. Gao, F. Volny IV, and M.S. Wang : A new framework for computing Gröbner bases, 2010. (GVW algorithm)

signature-based standard basis algorithms

Define a subset in $R^m \times R$:

$$M = \{(\mathbf{u}, v) \in R^m \times R : \mathbf{u} \cdot \mathbf{f} = v, \mathbf{u} \in R^m\}$$

where $\mathbf{f} = (f_1, \ldots, f_m) \in (k[X])^m$.

- M is a R-submodule in $R^m \times R$.
- M is generated by $(\mathbf{e}_1, f_1), \ldots, (\mathbf{e}_m, f_m)$.

Fix the local order $\prec_1$ in R, and the module order $\prec_2$ in R^m.

For convenience, denote by $\prec$ with no confusion.

signature: $p = (\mathbf{u}, v) \in M$, $s(p) = \mathrm{lm}(\mathbf{u})$.

Example 2

For local order $\prec$, $p = (\mathbf{u}, v) = ((x^2 + x^3, x^5 - 2x^7), x^4 + 2x^7)$

$\mathrm{lm}(v) = x^4, \quad s(p) = \mathrm{lm}(\mathbf{u}) = x^2\mathbf{e}_1 = (x^2, 0).$

signature-based Gröbner basis algorithms	$\xrightarrow{?}$	signature-based standard basis algorithms
global order($X^\alpha \succ 1$)	$\longrightarrow$	local order($X^\alpha \prec 1$)

signature-based Gröbner basis algorithms	$\xrightarrow{?}$	signature-based standard basis algorithms

global order($X^\alpha \succ 1$) $\longrightarrow$ local order($X^\alpha \prec 1$)

?: local orders are not well-orderings.

- 1. there may not be a minimal element in an infinite set; (correctness)
- 2. the top-reduction steps may not terminate in the local ring. (termination)

1. a minimal element problem related to correctness

For any $(\mathbf{u}_0, v_0) \in M$, we consider the set

$$L(\mathrm{lm}(v_0)) = \{\mathrm{lm}(\mathbf{u}) : (\mathbf{u}, v) \in M \quad \text{and} \quad \mathrm{lm}(v) = \mathrm{lm}(v_0)\}.$$

$L(\mathrm{lm}(v_0))$ is a nonempty set.

Question: Does $L(\mathrm{lm}(v_0))$ have a minimal element ?

Example 3

$R = k[x_1, x_2]_{\langle x_1, x_2\rangle}$, $\mathbf{f} = (x_1, x_2)$, $M = \{(\mathbf{u}, v) : \mathbf{u} \cdot \mathbf{f} = v\}$;
$\prec_1$: *an anti-graded lex order with* $x_2 \prec_1 x_1$ *in* R;
$\prec_2$: *a POT order with* $\mathbf{e}_2 \prec_2 \mathbf{e}_1$ *in* R^2;

$p_0 = (\mathbf{u}_0, v_0) = ((x_1, x_1 + 1),\ x_1^2 + x_1x_2 + x_2) \in M$;
$p_1 = (\mathbf{u}_1, v_1) = ((x_1^2, x_1 + 1),\ x_1^3 + x_1x_2 + x_2) \in M$;
.....
$p_i = (\mathbf{u}_i, v_i) = ((x_1^{1+i}, x_1 + 1),\ x_1^{2+i} + x_1x_2 + x_2) \in M$;
.....

$L(\mathrm{lm}(v_0)) = L(x_2) \supseteq \{x_1^i \mathbf{e}_1 : i \in \mathbb{Z}_{\geq 1}\}$ has not a minimal element.

But, at the following case:

Lemma 4

Let $\prec_1$ be an anti-graded order in R, and $\prec_2$ be a TOP order in R^m, where $\prec_2$ is compatible with $\prec_1$. Then for any $(\mathbf{u}_0, v_0) \in M$, $L(\mathrm{lm}(v_0))$ has a minimal element.

2. the reduction problem related to termination

the top-reduction steps may not terminate in the local ring.

2. the reduction problem related to termination

the top-reduction steps may not terminate in the local ring.

Example 5

Given the anti-graded order and $\mathbf{e}_2 \prec \mathbf{e}_1$;
$p_1 = (\mathbf{e}_1,\ x)$; $p_2 = (\mathbf{e}_2,\ x - x^2)$;

the top-reduction steps:

$$p_3 = Red(p_1, p_2) = p_1 - p_2 = (\mathbf{e}_1 - \mathbf{e}_2,\ x^2);$$
$$p_4 = Red(p_3, p_2) = p_3 - xp_2 = (\mathbf{e}_1 - (1+x)\mathbf{e}_2,\ x^3);$$
$$p_5 = Red(p_4, p_2) = p_4 - x^2p_2 = (\mathbf{e}_1 - (1+x+x^2)\mathbf{e}_2,\ x^4);$$
$$p_6 = Red(p_5, p_2) = p_5 - x^3p_2 = (\mathbf{e}_1 - (1+x+x^2+x^3)\mathbf{e}_2,\ x^5);$$
$$\cdots\cdots$$

Theorem 6

Let $G = \{p_1 = (\mathbf{u}_1, f_1), \ldots, p_s = (\mathbf{u}_s, f_s)\} \subset (k[X])^m \times k[X]$ *and* $p = (\mathbf{u}, f)$. *Then there is an algorithm for producing polynomials* $h, a_1, \ldots, a_s$ *in* $k[X]$ *and* $r = (\mathbf{w}, v)$ *in* $(k[X])^m \times k[X]$ *such that*

$$hp = a_1 p_1 + \cdots + a_s p_s + r,$$

where $\mathrm{lm}(h) = 1$, $\mathrm{lm}(a_i f_i) \preceq \mathrm{lm}(f)$, $\mathrm{lm}(a_i \mathbf{u}_i) \preceq \mathrm{lm}(\mathbf{u})$, $\mathrm{lm}(\mathbf{w}) = \mathrm{lm}(\mathbf{u})$, *and either* $v = 0$ *or* $\mathrm{lm}(f_i) \nmid \mathrm{lm}(v)$.

$r = \overline{p}^G$: **the remainder** of p regularly top-reduced by G

Definition 7 (Strong standard bases)

Let G be a finite subset of M. If for any nonzero $(\mathbf{u}, v) \in M$, it is top-reducible by some element in G, Then G is called a **strong standard basis** *for M.*

Definition 7 (Strong standard bases)

Let G be a finite subset of M. If for any nonzero $(\mathbf{u}, v) \in M$, it is top-reducible by some element in G, Then G is called a **strong standard basis** *for M.*

$$G \text{ is a strong standard basis for } M$$
$$\Downarrow$$
$$V = \{v : (\mathbf{u}, v) \in G\} \text{ is a standard basis for ideal } I \text{ in } R$$

J-pair: (similar to S-polynomial or S-pair) $\longrightarrow$ Jonit pair

$p_1 = (\mathbf{u}_1, v_1), p_2 = (\mathbf{u}_2, v_2) \in M$, and $v_1 v_2 \neq 0$.

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

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

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

If

$$\mathrm{lm}(t_1 \mathbf{u}_1 - c t_2 \mathbf{u}_2) = T, \qquad (\textit{regular})$$

then $t_1 p_1$ is called the **J-pair** of p_1 and p_2.

cover:

a pair $(\mathbf{u}, v) \in M$ is covered by $G \subset M$, if $\exists\ (\mathbf{u}_i, v_i) \in G$, s.t. $\mathrm{lm}(\mathbf{u}_i) \mid \mathrm{lm}(\mathbf{u})$, $t = \mathrm{lm}(\mathbf{u})/\mathrm{lm}(\mathbf{u}_i)$, and $t\mathrm{lm}(v_i) \prec_1 \mathrm{lm}(v)$

$$p = (\mathbf{u}, v)$$
$$tp_i = (t\mathbf{u}_i, tv_i)$$

Example 8

$p = (\mathbf{u}, v) = ((x_1^2 x_2,\ x_1^4 x_2),\ x_2^2)$;
$p_i = (u_i, v_i) = ((x_1 x_2,\ x_2^3),\ x_1^2 + x_2^3)$.

$x_1 p_i = (u_i, v_i) = ((x_1^2 x_2,\ x_1 x_2^3),\ x_1^3 + x_1 x_2^3)$ and $x_1^3 \prec x_2^2$.

main theorem

Theorem 9 (Cover Theorem)

Let $G \subset (k[X])^m \times k[X]$ be a finite subset of M such that, for any term $T \in R^m$, there is a pair $(\mathbf{u}, v) \in G$ and a monomial t such that $T = t\,\mathrm{lm}(\mathbf{u})$. Then the following are equivalent:

1. *G is a strong standard basis for M; (the corresponding v part is a standard basis)*
2. *every J-pair of G is covered by G.*

Priori criterion with "Signature"

Cover Criterion:

Any J-pair that is covered by G can be discarded without performing any reductions

Cover Criterion includes:

Syzygy Criterion, Signature Criterion and Rewrite Criterion

▶ GVW algorithm in local ring

Input: $F = \{f_1, \ldots, f_m\} \subset k[X]$
Output: V — a standard basis for $\langle f_1, \ldots, f_m \rangle \subset R$

1 $G := \{(\mathbf{e}_1, f_1), \ldots, (\mathbf{e}_m, f_m)\}$; $H := \{\mathrm{lm}(f_i\mathbf{e}_j - f_j\mathbf{e}_i)\}$; $JP := \{\text{J-pairs of } G\}$;
2 **while** $JP \neq \emptyset$ **do**
3 choose $(T, v) \in JP$, and $JP := JP \setminus \{(T, v)\}$;
4 **if** (T, v) is covered by G or H **then** next; $\longrightarrow$Cover Criterion
5 **else**
6 $(T_0, v_0) := \overline{(T, v)}^G$;
7 **if** $v_0 = 0$ **then** $H := H \cup \{T_0\}$;
8 **else**
9 $JP := JP \cup \{\text{J-pairs between } (T_0, v_0) \text{ and } G\}$; $\longrightarrow$Cover Criterion
$H := H \cup \{\mathrm{lm}(v_0 T_j - v_j T_0)\}$;
$G := G \cup \{(T_0, v_0)\}$;
10 **end if**
11 **end while**
12 **return** $V := \{v \mid (T, v) \in G\}$

An Example

Example 10

Given $\prec_1$ be the anti-graded reverse lex order, and $\prec_2$ is a TOP order in R^3 and compatible with $\prec_1$,

$x_1 \succ x_2 \succ x_3, \quad \mathbf{e}_1 \succ \mathbf{e}_2 \succ \mathbf{e}_3$

$R = \mathbb{C}[x_1, x_2, x_3]_{\langle x_1, x_2, x_3\rangle}$, $I = \langle f_1, f_2, f_3\rangle \subset R$,

$f_1 = x_1^2 - 5x_2x_3 - 2x_2^2x_3, f_2 = 2x_1x_2 + 2x_2^3 - x_3^3, f_3 = -x_1x_2 + x_2x_3^2.$

Compute a standard basis for I.

An Example

Initial:

$G_0 := \{(\mathbf{e}_1, f_1), (\mathbf{e}_2, f_2), (\mathbf{e}_3, f_3)\}$;

$H_0 := \{x_1^2\mathbf{e}_2, x_1^2\mathbf{e}_3, x_1x_2\mathbf{e}_2\}$; the signature of principle syzygies

$JP_0 := \{(T_1, v_1), (T_2, v_2), (T_3, v_3)\}$

$= \{(x_1\mathbf{e}_3, x_1f_3), (x_1\mathbf{e}_2, x_1f_2), (\mathbf{e}_2, f_2)\}$; the J-pairs set of G_0

An Example

First cycle:

- Select the J-pair $(T_1, v_1) = (x_1\mathbf{e}_3, x_1 f_3)$ from JP_0;
- (T_1, v_1) is not covered by G_0 or H_0;
- $p_4 = (T_1, \widetilde{v_1}) = \overline{(T_1, v_1)}^{G_0} = (x_1\mathbf{e}_3, -5x_2^2x_3 + x_1x_2x_3^2 - 2x_2^3x_3)$;
- $JP_1 := \{(T_2, v_2), (T_3, v_3)\}$
  $= \{(x_1\mathbf{e}_3, x_1 f_3), (x_1\mathbf{e}_2, x_1 f_2), (\mathbf{e}_2, f_2)\}$ Cover Criterion
  $H_1 := H_0 = \{x_1^2\mathbf{e}_2, x_1^2\mathbf{e}_3, x_1x_2\mathbf{e}_2\}$ Cover Criterion
  $G_1 := G_0 \cup \{p_4\}$.

An Example

Sixth cycle:

$$JP_5 := \{(T_7, v_7), (T_5, v_5)\} = \{(x_1x_3\mathbf{e}_2, x_1\tilde{v}_4), (x_1\mathbf{e}_2, x_1\tilde{v}_3)\}$$
$$G_5 := G_4 \cup \{p_8\} = \{(\mathbf{e}_1, f_1), (\mathbf{e}_2, f_2), (\mathbf{e}_3, f_3), p_4, p_5, p_6, p_7, p_8\}$$

- Select $(T_7, v_7) = (x_1x_3\mathbf{e}_2, 2x_1x_2x_3^3 + *)$ from JP_5 ;
- (T_7, v_7) is covered by $p_5 = (x_1\mathbf{e}_2, -x_1x_3^3 + *)$; Cover Criterion

$$(T_7, v_7) = (x_1x_3\mathbf{e}_2, 2x_1x_2x_3^3 + *)$$
$$x_3p_5 = (x_1x_3\mathbf{e}_2, -x_1x_3^4 + *)$$

Discard (T_7, v_7) , and reselect another J-pair to continue the cycle.

An Example

Continue: $\cdots$

Discard: 23 J-pairs by using Cover Criterion (including: Syzygy Criterion, Signature Criterion and Rewrite Criterion)

Do: 5 regular top-reductions

the standard basis of I in $R = \{f_1, f_2, f_3, \tilde{v}_1, \tilde{v}_2, \tilde{v}_3, \tilde{v}_4, \tilde{v}_5\}$.

Implementation

Table: examples

ideal	signature-based method(our)			classical method		
	J-pairs	discard	discard/J-pairs	S-polys	discard	discard/S-polys
I_1	21	14	67%	28	6	21%
I_2	21	14	67%	21	9	43%
I_3	15	12	80%	15	8	53%
I_4	20	16	80%	21	10	48%
I_5	15	9	60%	15	4	27%
I_6	20	16	80%	21	6	29%
I_7	14	11	79%	15	4	27%
I_8	35	29	83%	28	9	32%
I_9	10	7	70%	15	6	40%
I_{10}	21	17	81%	66	28	43%

- We implement the two algorithms in *Maple*, and the codes and examples are available on the web:
  `http://www.mmrc.iss.ac.cn/~dwang/software.html`.

Conclusion

- Propose an efficient algorithm to compute the standard bases in local ring. (signature-based algorithm)
- Solve two key problems:
  - an infinite set may have not a minimal element in local ring. $\longrightarrow$ the signature set $L(\mathrm{lm}(v_0))$ w.r.t. v_0 has a minimal element (anti-graded order and TOP order)
  - the general division algorithm may not terminate in local ring. $\longrightarrow$ extend Mora normal form algorithm to do regular top-reduction (signature-based case)

Thanks for your attention!