Predicting zero reductions in Gröbner Basis computations

Christian Eder

SNC 2014, Shanghai, China

July 30, 2014

How to detect zero reductions in advance?

Let $I = \langle g_1, g_2 \rangle \in \mathbb{Q}[x, y, z]$ and let $<$ denote DRL. Let

$$\mathbf{g_1 = xy - z^2}, \quad \mathbf{g_2 = y^2 - z^2}$$

How to detect zero reductions in advance?

Let $I = \langle g_1, g_2 \rangle \in \mathbb{Q}[x, y, z]$ and let $<$ denote DRL. Let

$$\mathbf{g_1} = \mathbf{xy} - \mathbf{z^2}, \quad \mathbf{g_2} = \mathbf{y^2} - \mathbf{z^2}$$

$$\begin{aligned} \mathrm{spol}(g_2, g_1) &= xg_2 - yg_1 = \mathbf{xy^2} - xz^2 - \mathbf{xy^2} + yz^2 \\ &= -xz^2 + yz^2. \end{aligned}$$

$$\Longrightarrow \mathbf{g_3} = \mathbf{xz^2} - \mathbf{yz^2}.$$

How to detect zero reductions in advance?

Let $I = \langle g_1, g_2 \rangle \in \mathbb{Q}[x, y, z]$ and let $<$ denote DRL. Let

$$\mathbf{g_1} = \mathbf{xy} - \mathbf{z^2}, \quad \mathbf{g_2} = \mathbf{y^2} - \mathbf{z^2}$$

$$\begin{aligned} \mathrm{spol}(g_2, g_1) &= xg_2 - yg_1 = \mathbf{xy^2} - xz^2 - \mathbf{xy^2} + yz^2 \\ &= -xz^2 + yz^2. \end{aligned}$$

$$\Longrightarrow \mathbf{g_3} = \mathbf{xz^2} - \mathbf{yz^2}.$$

$$\mathrm{spol}(g_3, g_1) = \mathbf{xyz^2} - y^2z^2 - \mathbf{xyz^2} + z^4 = -y^2z^2 + z^4.$$

How to detect zero reductions in advance?

Let $I = \langle g_1, g_2 \rangle \in \mathbb{Q}[x,y,z]$ and let $<$ denote DRL. Let

$$\mathbf{g_1 = xy - z^2}, \quad \mathbf{g_2 = y^2 - z^2}$$

$$\begin{aligned} \mathrm{spol}(g_2, g_1) &= xg_2 - yg_1 = \mathbf{xy^2} - xz^2 - \mathbf{xy^2} + yz^2 \\ &= -xz^2 + yz^2. \end{aligned}$$

$$\Longrightarrow \mathbf{g_3 = xz^2 - yz^2}.$$

$$\mathrm{spol}(g_3, g_1) = \mathbf{xyz^2} - y^2z^2 - \mathbf{xyz^2} + z^4 = -y^2z^2 + z^4.$$

We can reduce further using $z^2 g_2$:

$$\boxed{-y^2z^2 + z^4 + y^2z^2 - z^4 = 0.}$$

Buchberger's criteria

Product criterion [1, 2]

If $\operatorname{lcm}(\operatorname{lt}(f), \operatorname{lt}(g)) = \operatorname{lt}(f)\operatorname{lt}(g)$ then $\operatorname{spol}(f,g) \xrightarrow{\{f,g\}} 0$.

Buchberger's criteria

Product criterion [1, 2]

If $\operatorname{lcm}(\operatorname{lt}(f), \operatorname{lt}(g)) = \operatorname{lt}(f)\operatorname{lt}(g)$ then $\operatorname{spol}(f, g) \xrightarrow{\{f,g\}} 0$.

Couldn't we remove $\operatorname{spol}(g_3, g_2)$ in a different way?

Buchberger's criteria

Product criterion [1, 2]

If $\mathrm{lcm}\left(\mathrm{lt}\left(f\right), \mathrm{lt}\left(g\right)\right) = \mathrm{lt}\left(f\right)\mathrm{lt}\left(g\right)$ then $\mathrm{spol}\left(f, g\right) \xrightarrow{\{f,g\}} 0$.

Couldn't we remove $\mathrm{spol}\left(g_3, g_2\right)$ in a different way?

$$\mathrm{lt}\left(g_1\right) = xy \mid xy^2z^2 = \mathrm{lcm}\left(\mathrm{lt}\left(g_3\right), \mathrm{lt}\left(g_2\right)\right)$$

Product criterion [1, 2]

If $\mathrm{lcm}(\mathrm{lt}(f), \mathrm{lt}(g)) = \mathrm{lt}(f)\,\mathrm{lt}(g)$ then $\mathrm{spol}(f,g) \xrightarrow{\{f,g\}} 0$.

Couldn't we remove $\mathrm{spol}(g_3, g_2)$ in a different way?

$$\mathrm{lt}(g_1) = xy \mid xy^2z^2 = \mathrm{lcm}(\mathrm{lt}(g_3), \mathrm{lt}(g_2))$$

$\Longrightarrow$ We can rewrite $\mathrm{spol}(g_3, g_2)$:

$$\mathrm{spol}(g_3, g_2) = y\,\underbrace{\mathrm{spol}(g_3, g_1)}_{\xrightarrow{G} 0} - z^2\,\underbrace{\mathrm{spol}(g_2, g_1)}_{\xrightarrow{G} -g_3}$$

Buchberger's criteria

Product criterion [1, 2]

If $\operatorname{lcm}(\operatorname{lt}(f), \operatorname{lt}(g)) = \operatorname{lt}(f)\operatorname{lt}(g)$ then $\operatorname{spol}(f, g) \xrightarrow{\{f,g\}} 0$.

Couldn't we remove $\operatorname{spol}(g_3, g_2)$ in a different way?

$$\operatorname{lt}(g_1) = xy \mid xy^2z^2 = \operatorname{lcm}(\operatorname{lt}(g_3), \operatorname{lt}(g_2))$$

$\Longrightarrow$ We can rewrite $\operatorname{spol}(g_3, g_2)$:

$$\operatorname{spol}(g_3, g_2) = y\underbrace{\operatorname{spol}(g_3, g_1)}_{\xrightarrow{G} 0} - z^2\underbrace{\operatorname{spol}(g_2, g_1)}_{\xrightarrow{G} -g_3}$$

Standard representations of $\operatorname{spol}(g_2, g_1)$ and $\operatorname{spol}(g_3, g_1)$
$\Longrightarrow$ Standard representation of $\operatorname{spol}(g_3, g_2)$.

Chain criterion [3]

Let $f, g, h \in \mathscr{R}$, $G \subset \mathscr{R}$ finite. If

1. $\mathrm{lt}(h) \mid \mathrm{lcm}(\mathrm{lt}(f), \mathrm{lt}(g))$, and
2. $\mathrm{spol}(f, h)$ and $\mathrm{spol}(h, g)$ have a standard representation w.r.t. G respectively,

then $\mathrm{spol}(f, g)$ has a standard representation w.r.t. G.

Chain criterion [3]

Let $f, g, h \in \mathscr{R}$, $G \subset \mathscr{R}$ finite. If

1. $\operatorname{lt}(h) \mid \operatorname{lcm}(\operatorname{lt}(f), \operatorname{lt}(g))$, and
2. $\operatorname{spol}(f, h)$ and $\operatorname{spol}(h, g)$ have a standard representation w.r.t. G respectively,

then $\operatorname{spol}(f, g)$ has a standard representation w.r.t. G.

Combined implementation of Product and Chain criterion:
Gebauer-Möller Installation [10]

Signatures

Let $I = \langle f_1, \ldots, f_m \rangle$.

Idea: Give each $f \in I$ a bit more structure:

Signatures

Let $I = \langle f_1, \ldots, f_m \rangle$.
Idea: Give each $f \in I$ a bit more structure:

- Let $\mathscr{R}^m$ be generated by $e_1, \ldots, e_m$ and let $\prec$ be a compatible monomial order on the monomials of $\mathscr{R}^m$.

Signatures

Let $I = \langle f_1, \ldots, f_m \rangle$.
Idea: Give each $f \in I$ a bit more structure:

- Let $\mathscr{R}^m$ be generated by $e_1, \ldots, e_m$ and let $\prec$ be a compatible monomial order on the monomials of $\mathscr{R}^m$.
- Let $\alpha \mapsto \overline{\alpha} : \mathscr{R}^m \to \mathscr{R}$ such that $\overline{e}_i = f_i$ for all i.

Signatures

Let $I = \langle f_1, \ldots, f_m \rangle$.
Idea: Give each $f \in I$ a bit more structure:

- Let $\mathscr{R}^m$ be generated by $e_1, \ldots, e_m$ and let $\prec$ be a compatible monomial order on the monomials of $\mathscr{R}^m$.
- Let $\alpha \mapsto \overline{\alpha} : \mathscr{R}^m \to \mathscr{R}$ such that $\overline{e}_i = f_i$ for all i.
- Each $f \in I$ can be represented via some $\alpha \in \mathscr{R}^m$: $f = \overline{\alpha}$

Signatures

Let $I = \langle f_1, \dots, f_m \rangle$.
Idea: Give each $f \in I$ a bit more structure:

- Let $\mathscr{R}^m$ be generated by $e_1, \dots, e_m$ and let $\prec$ be a compatible monomial order on the monomials of $\mathscr{R}^m$.
- Let $\alpha \mapsto \overline{\alpha} : \mathscr{R}^m \to \mathscr{R}$ such that $\overline{e}_i = f_i$ for all i.
- Each $f \in I$ can be represented via some $\alpha \in \mathscr{R}^m$: $f = \overline{\alpha}$
- **A signature** of f is given by $\mathfrak{s}(f) = \mathrm{lt}_{\prec}(\alpha)$ where $f = \overline{\alpha}$.

Signatures

Let $I = \langle f_1, \ldots, f_m \rangle$.
Idea: Give each $f \in I$ a bit more structure:

- Let $\mathscr{R}^m$ be generated by $e_1, \ldots, e_m$ and let $\prec$ be a compatible monomial order on the monomials of $\mathscr{R}^m$.
- Let $\alpha \mapsto \overline{\alpha} : \mathscr{R}^m \to \mathscr{R}$ such that $\overline{e}_i = f_i$ for all i.
- Each $f \in I$ can be represented via some $\alpha \in \mathscr{R}^m$: $f = \overline{\alpha}$
- **A signature** of f is given by $\mathfrak{s}(f) = \mathrm{lt}_\prec(\alpha)$ where $f = \overline{\alpha}$.
- An element $\alpha \in \mathscr{R}^m$ with $\overline{\alpha} = 0$ is called **a syzygy**.

Our example again – with signatures and $\prec_{\text{pot}}$

$$g_1 = xy - z^2,\ \mathfrak{s}(g_1) = e_1,$$
$$g_2 = y^2 - z^2,\ \mathfrak{s}(g_2) = e_2.$$

Our example again – with signatures and $\prec_{\textbf{pot}}$

$$g_1 = xy - z^2,\ \mathfrak{s}(g_1) = e_1,$$
$$g_2 = y^2 - z^2,\ \mathfrak{s}(g_2) = e_2.$$

$$g_3 = \operatorname{spol}(g_2, g_1) = xg_2 - yg_1$$
$$\Rightarrow \mathfrak{s}(g_3) = x\,\mathfrak{s}(g_2) = xe_2.$$

Our example again – with signatures and $\prec_{\text{pot}}$

$$g_1 = xy - z^2,\ \mathfrak{s}(g_1) = e_1,$$
$$g_2 = y^2 - z^2,\ \mathfrak{s}(g_2) = e_2.$$

$$g_3 = \operatorname{spol}(g_2, g_1) = xg_2 - yg_1$$
$$\Rightarrow \mathfrak{s}(g_3) = x\,\mathfrak{s}(g_2) = xe_2.$$

$$\operatorname{spol}(g_3, g_1) = yg_3 - z^2 g_1$$
$$\Rightarrow \mathfrak{s}(\operatorname{spol}(g_3, g_1)) = y\,\mathfrak{s}(g_3) = xye_2.$$

Our example again – with signatures and $\prec_{\text{pot}}$

$$g_1 = xy - z^2,\ \mathfrak{s}(g_1) = e_1,$$
$$g_2 = y^2 - z^2,\ \mathfrak{s}(g_2) = e_2.$$

$$g_3 = \operatorname{spol}(g_2, g_1) = xg_2 - yg_1$$
$$\Rightarrow \mathfrak{s}(g_3) = x\,\mathfrak{s}(g_2) = xe_2.$$

$$\operatorname{spol}(g_3, g_1) = yg_3 - z^2 g_1$$
$$\Rightarrow \mathfrak{s}\left(\operatorname{spol}(g_3, g_1)\right) = y\,\mathfrak{s}(g_3) = xye_2.$$

Note that $\mathfrak{s}\left(\operatorname{spol}(g_3, g_1)\right) = xy\,e_2$ and $\operatorname{lm}(g_1) = xy$.

Think in the module

$\alpha \in \mathscr{R}^m \implies$ polynomial $\overline{\alpha}$ with $\mathrm{lt}(\overline{\alpha})$, signature $\mathfrak{s}(\alpha) = \mathrm{lt}(\alpha)$

Think in the module

$\alpha \in \mathscr{R}^m \implies$ polynomial $\overline{\alpha}$ with $\operatorname{lt}(\overline{\alpha})$, signature $\mathfrak{s}(\alpha) = \operatorname{lt}(\alpha)$

S-pairs/S-polynomials:

$$\operatorname{spol}\left(\overline{\alpha}, \overline{\beta}\right) = a\overline{\alpha} - b\overline{\beta} \implies \operatorname{spair}(\alpha, \beta) = a\alpha - b\beta$$

Think in the module

$\alpha \in \mathscr{R}^m \implies$ polynomial $\overline{\alpha}$ with $\mathrm{lt}\left(\overline{\alpha}\right)$, signature $\mathfrak{s}(\alpha) = \mathrm{lt}\left(\alpha\right)$

S-pairs/S-polynomials:

$$\mathrm{spol}\left(\overline{\alpha}, \overline{\beta}\right) = a\overline{\alpha} - b\overline{\beta} \implies \mathrm{spair}\left(\alpha, \beta\right) = a\alpha - b\beta$$

$\mathfrak{s}$-reductions:

$$\overline{\gamma} - d\overline{\delta} \implies \gamma - d\delta$$

Think in the module

$$\alpha \in \mathscr{R}^m \implies \text{polynomial } \overline{\alpha} \text{ with } \operatorname{lt}(\overline{\alpha}), \text{ signature } \mathfrak{s}(\alpha) = \operatorname{lt}(\alpha)$$

S-pairs/S-polynomials:

$$\operatorname{spol}\left(\overline{\alpha}, \overline{\beta}\right) = a\overline{\alpha} - b\overline{\beta} \implies \operatorname{spair}(\alpha, \beta) = a\alpha - b\beta$$

$\mathfrak{s}$-reductions:

$$\overline{\gamma} - d\overline{\delta} \implies \gamma - d\delta$$

Remark

In the following we need one detail from signature-based Gröbner Basis computations:

We pick from P by increasing signature.

Signature-based criteria

$\mathfrak{s}(\alpha) = \mathfrak{s}(\beta) \implies$ Compute 1, remove 1.

Signature-based criteria

$$\mathfrak{s}(\alpha) = \mathfrak{s}(\beta) \implies \text{Compute 1, remove 1.}$$

Sketch of proof

1. $\mathfrak{s}(\alpha - \beta) \prec \mathfrak{s}(\alpha), \mathfrak{s}(\beta)$.
2. All S-pairs are handled by increasing signature.
   $\Rightarrow$ All relatons $\prec \mathfrak{s}(\alpha)$ are known:

$$\alpha = \beta + \text{ elements of smaller signature}$$

$\square$

Signature-based criteria

S-pairs in signature T

Signature-based criteria

S-pairs in signature T

What are all possible configurations to reach signature T?

Signature-based criteria

S-pairs in signature T

$$\mathfrak{R}_T = \left\{ a\alpha \mid \alpha \text{ handled by the algorithm and } \mathfrak{s}(a\alpha) = T \right\}$$

What are all possible configurations to reach signature T?

Signature-based criteria

S-pairs in signature T

$$\mathfrak{R}_T = \left\{ a\alpha \mid \alpha \text{ handled by the algorithm and } \mathfrak{s}(a\alpha) = T \right\}$$

What are all possible configurations to reach signature T?

Define an order $\trianglelefteq$ on $\mathfrak{R}_T$ and choose the maximal element.

Special cases

$$\mathfrak{R}_T = \left\{ a\alpha \mid \alpha \text{ handled by the algorithm and } \mathfrak{s}(a\alpha) = T \right\}$$

Special cases

$$\mathfrak{R}_T = \Big\{ a\alpha \mid \alpha \text{ handled by the algorithm and } \mathfrak{s}(a\alpha) = T \Big\}$$

Choose $b\beta$ to be an element of $\mathfrak{R}_T$ maximal w.r.t. an order $\trianglelefteq$.

Special cases

$$\mathfrak{R}_T = \left\{ a\alpha \mid \alpha \text{ handled by the algorithm and } \mathfrak{s}(a\alpha) = T \right\}$$

Choose $b\beta$ to be an element of $\mathfrak{R}_T$ maximal w.r.t. an order $\trianglelefteq$.

1. If $b\beta$ is a syzygy $\Longrightarrow$ Go on to next signature.

Special cases

$$\mathfrak{R}_T = \left\{ a\alpha \mid \alpha \text{ handled by the algorithm and } \mathfrak{s}(a\alpha) = T \right\}$$

Choose $b\beta$ to be an element of $\mathfrak{R}_T$ maximal w.r.t. an order $\trianglelefteq$.

1. If $b\beta$ is a syzygy $\Longrightarrow$ Go on to next signature.
2. If $b\beta$ is not part of an S-pair $\Longrightarrow$ Go on to next signature.

Special cases

$$\mathfrak{R}_T = \left\{ a\alpha \mid \alpha \text{ handled by the algorithm and } \mathfrak{s}(a\alpha) = T \right\}$$

Choose $b\beta$ to be an element of $\mathfrak{R}_T$ maximal w.r.t. an order $\trianglelefteq$.

1. If $b\beta$ is a syzygy $\Longrightarrow$ Go on to next signature.
2. If $b\beta$ is not part of an S-pair $\Longrightarrow$ Go on to next signature.

Revisiting our example with $\prec_{\text{pot}}$

$$\mathfrak{s}\left(\text{spol}(g_3, g_1)\right) = xye_2$$

$$\left.\begin{array}{l} g_1 = xy - z^2 \\ g_2 = y^2 - z^2 \end{array}\right\} \Rightarrow \text{psyz}(g_2, g_1) = g_1 e_2 - g_2 e_1 = xye_2 + \ldots$$

Buchberger's criteria?

Buchberger's Product and Chain criterion can be combined with the Rewrite criterion [9, 11, 5]:

Buchberger's criteria?

Buchberger's Product and Chain criterion can be combined with the Rewrite criterion [9, 11, 5]:

Chain criterion is a special case of the Rewrite criterion
$\Rightarrow$ already included.

Buchberger's criteria?

Buchberger's Product and Chain criterion can be combined with the Rewrite criterion [9, 11, 5]:

Chain criterion is a special case of the Rewrite criterion
$\Rightarrow$ already included.

Product criterion is not always (but mostly) included.

Buchberger's criteria?

Buchberger's Product and Chain criterion can be combined with the Rewrite criterion [9, 11, 5]:

Chain criterion is a special case of the Rewrite criterion
$\Rightarrow$ already included.

Product criterion is not always (but mostly) included.

α added to $\mathscr{G}$

▼

Generate all possible principal syzygies with α.
(e.g. **GVW**)

Buchberger's criteria?

Buchberger's Product and Chain criterion can be combined with the Rewrite criterion [9, 11, 5]:

Chain criterion is a special case of the Rewrite criterion
$\Rightarrow$ already included.

Product criterion is not always (but mostly) included.

α added to $\mathscr{G}$

▼

Generate all possible principal syzygies with α.
(e.g. **GVW**)

S-pair fulfilling Product criterion not detected by Rewrite criterion

▼

Add one corresponding syzygy.
(e.g. **SBA** in **Singular**)

Experimental results

Implementation done in **Singular** [4]

Benchmark	STD	SBA $\prec_{pot}$	SBA $\prec_{lt}$	
	ZR	ZR	ZR	ZR / PC
cyclic-8	4284	243	771	771 / 0
cyclic-8-h	5843	243	771	771 / 0
eco-11	3476	0	614	614 / 0
eco-11-h	5429	502	629	608 / 0
katsura-11	3933	0	348	304 / 0
katsura-11-h	3933	0	348	304 / 0
noon-9	25508	0	682	646 / 0
noon-9-h	25508	0	682	646 / 0
binomial-6-2	21	6	15	8 / 7
binomial-6-3	20	13	15	9 / 6
binomial-7-3	27	24	21	21 / 0
binomial-7-4	41	16	19	16 / 3
binomial-8-3	53	23	27	27 / 0
binomial-8-4	40	31	26	26 / 0

And what's about SBA using $\prec_{\textbf{pot}}$?

Conjecture [5]

Every S-polynomial fulfilling the Product criterion is also detected by the Rewrite criterion in **SBA** using $\prec_{\text{pot}}$.

And what's about SBA using $\prec_{pot}$?

Conjecture [5]
Every S-polynomial fulfilling the Product criterion is also detected by the Rewrite criterion in **SBA** using $\prec_{pot}$.

- We checked several million examples, all fulfilling the conjecture.
- Until now we cannot prove this.

And what's about SBA using $\prec_{\text{pot}}$?

Conjecture [5]

Every S-polynomial fulfilling the Product criterion is also detected by the Rewrite criterion in **SBA** using $\prec_{\text{pot}}$.

- We checked several million examples, all fulfilling the conjecture.
- Until now we cannot prove this.

Ongoing work:

1. Describe in detail the connection between our conjecture and Moreno-Socías conjecture [12].
2. Try to exploit even more algebraic structures for predicting zero reductions.

References I

[1] Buchberger, B. Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystems. *Aequ. Math.*, 4(3):374–383, 1970.

[2] Buchberger, B. A criterion for detecting unnecessary reductions in the construction of Gröbner bases. In *EUROSAM '79, An International Symposium on Symbolic and Algebraic Manipulation*, volume 72 of *Lecture Notes in Computer Science*, pages 3–21. Springer, 1979.

[3] Buchberger, B. Gröbner Bases: An Algorithmic Method in Polynomial Ideal Theory. pages 184–232, 1985.

[4] Decker, W., Greuel, G.-M., Pfister, G., and Schönemann, H. SINGULAR *4-0-0 — A computer algebra system for polynomial computations*, 2014. `http://www.singular.uni-kl.de`.

[5] Eder, C. Predicting zero reductions in Gröbner basis computations. submitted to Journal of Symbolc Computation, preprint at `http://arxiv.org/abs/1404.0161`, 2014.

[6] Eder, C. and Faugère, J.-C. A survey on signature-based Groebner basis algorithms. *http://arxiv.org/abs/1404.1774*, 2014.

[7] Faugère, J.-C. A new efficient algorithm for computing Gröbner bases (F4). *Journal of Pure and Applied Algebra*, 139(1–3):61–88, June 1999. `http://www-salsa.lip6.fr/~jcf/Papers/F99a.pdf`.

References II

[8] Faugère, J.-C. A new efficient algorithm for computing Gröbner bases without reduction to zero F5. In *ISSAC'02, Villeneuve d'Ascq, France*, pages 75–82, July 2002. Revised version from `http://fgbrs.lip6.fr/jcf/Publications/index.html`.

[9] Gao, S., Volny IV, F., and Wang, D. A new algorithm for computing Groebner bases (rev. 2013).
`http://www.math.clemson.edu/~sgao/papers/gvw_R130704.pdf`, 2013.

[10] Gebauer, R. and Möller, H. M. On an installation of Buchberger's algorithm. *Journal of Symbolic Computation*, 6(2-3):275–286, October/December 1988.

[11] Gerdt, V. P. and Hashemi, A. On the use of Buchberger criteria in G2V algorithm for calculating Gröbner bases. *Program. Comput. Softw.*, 39(2):81–90, March 2013.

[12] Moreno-Socías, G. Degrevlex Gröbner bases of generic complete intersections. *Journal of Pure and Applied Algebra*, 180(3):263 – 283, 2003.