Signature-based Gröbner Basis Algorithms

Christian Eder

joint work with

Jean-Charles Faugère, Bjarke Hammersholt Roune, John Perry and Justin Gash

GBRELA2013 - Hagenberg, Austria

September 03 – 06, 2013
The basic problem

Signature basics

Signature-based criteria

A decade in signature-based Gröbner Basis algorithms
How to detect zero reductions in advance?

Example

Let \( l = \langle g_1, g_2 \rangle \in \mathbb{Q}[x, y, z] \), \( g_1 = xy - z^2 \), \( g_2 = y^2 - z^2 \).

\(<\) denotes the reverse lexicographical ordering.
How to detect zero reductions in advance?

**Example**

Let \( I = \langle g_1, g_2 \rangle \in \mathbb{Q}[x, y, z], g_1 = xy - z^2, g_2 = y^2 - z^2 \). < denotes the reverse lexicographical ordering.

\[
\text{spol}(g_2, g_1) = xg_2 - yg_1 = xy^2 - xz^2 - xy^2 + yz^2 = -xz^2 + yz^2.
\]

Thus it reduces to \( g_3 = xz^2 - yz^2 \) w.r.t. \( G \).
How to detect zero reductions in advance?

Example

Let \( I = \langle g_1, g_2 \rangle \in \mathbb{Q}[x, y, z] \), \( g_1 = xy - z^2 \), \( g_2 = y^2 - z^2 \). < denotes the reverse lexicographical ordering.

\[
\text{spol}(g_2, g_1) = xg_2 - yg_1 = xy^2 - xz^2 - xy^2 + yz^2 = -xz^2 + yz^2.
\]

Thus it reduces to \( g_3 = xz^2 - yz^2 \) w.r.t. \( G \).

\[
\text{spol}(g_3, g_1) = xyz^2 - y^2z^2 - xyz^2 + z^4 = -y^2z^2 + z^4.
\]
How to detect zero reductions in advance?

Example

Let \( I = \langle g_1, g_2 \rangle \in \mathbb{Q}[x, y, z] \), \( g_1 = xy - z^2 \), \( g_2 = y^2 - z^2 \). < denotes the reverse lexicographical ordering.

\[
spol(g_2, g_1) = xg_2 - yg_1 = xy^2 - xz^2 - xy^2 + yz^2 \\
= -xz^2 + yz^2.
\]

Thus it reduces to \( g_3 = xz^2 - yz^2 \) w.r.t. \( G \).

\[
spol(g_3, g_1) = xyz^2 - y^2z^2 - xyz^2 + z^4 = -y^2z^2 + z^4.
\]

We can reduce further using \( z^2g_2 \):

\[-y^2z^2 + z^4 + y^2z^2 - z^4 = 0.\]
How to detect zero reductions in advance?

Example

Let $I = \langle g_1, g_2 \rangle \in \mathbb{Q}[x, y, z]$, $g_1 = xy - z^2$, $g_2 = y^2 - z^2$. $<$ denotes the reverse lexicographical ordering.

$$spol(g_2, g_1) = xg_2 - yg_1 = xy^2 - xz^2 - xy^2 + yz^2$$
$$= -xz^2 + yz^2.$$

Thus it reduces to $g_3 = xz^2 - yz^2$ w.r.t. $G$.

$$spol(g_3, g_1) = xyz^2 - y^2z^2 - xyz^2 + z^4 = -y^2z^2 + z^4.$$

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

$$-y^2z^2 + z^4 + y^2z^2 - z^4 = 0.$$

How to get rid of this zero reduction?
Let $I = \langle f_1, \ldots, f_m \rangle$.

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

1. Let $R_m$ be generated by $e_1, \ldots, e_m$ and let $\prec$ be a compatible monomial order on the monomials of $R_m$.
2. Let $\alpha \mapsto \alpha: R_m \to R$ such that $e_i = f_i$ for all $i$.
3. Each $f \in I$ can be represented via some $\alpha \in R_m$: $f = \alpha$.
4. A signature of $f$ is given by $s(f) = \text{lt}_\prec(\alpha)$ where $f = \alpha$. 
Let \( I = \langle f_1, \ldots, f_m \rangle \).

**Idea:** Give each \( f \in I \) a bit more structure:

1. Let \( R^m \) be generated by \( e_1, \ldots, e_m \) and let \( \prec \) be a compatible monomial order on the monomials of \( R^m \).
Let \( I = \langle f_1, \ldots, f_m \rangle \).

**Idea:** Give each \( f \in I \) a bit more structure:

1. Let \( R^m \) be generated by \( e_1, \ldots, e_m \) and let \( \prec \) be a compatible monomial order on the monomials of \( R^m \).

2. Let \( \alpha \mapsto \bar{\alpha} : R^m \to R \) such that \( \bar{e_i} = f_i \) for all \( i \).
Let $I = \langle f_1, \ldots, f_m \rangle$.

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

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

2. Let $\alpha \mapsto \overline{\alpha} : R^m \rightarrow R$ such that $\overline{e}_i = f_i$ for all $i$.

3. Each $f \in I$ can be represented via some $\alpha \in R^m$: $f = \overline{\alpha}$
Let $I = \langle f_1, \ldots, f_m \rangle$.

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

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

2. Let $\alpha \mapsto \overline{\alpha} : R^m \to R$ such that $\overline{e_i} = f_i$ for all $i$.

3. Each $f \in I$ can be represented via some $\alpha \in R^m$: $f = \overline{\alpha}$

4. **A signature** of $f$ is given by $s(f) = \text{lt}_{\prec}(\alpha)$ where $f = \overline{\alpha}$. 
Our example again – now with signatures and $\prec_{\text{pot}}$

\[ g_1 = xy - z^2, \quad s(g_1) = e_1, \]
\[ g_2 = y^2 - z^2, \quad s(g_2) = e_2, \]
\[ g_3 = \text{spol}(g_2, g_1) = xg_2 - yg_1 \]
\[ \Rightarrow s(g_3) = x \cdot s(g_2) = xe_2. \]
Our example again – now with signatures and \( \prec_{\text{pot}} \)

\[
g_1 = xy - z^2, \ s(g_1) = e_1,
\]
\[
g_2 = y^2 - z^2, \ s(g_2) = e_2,
\]
\[
g_3 = \text{spol}(g_2, g_1) = xg_2 - yg_1
\]
\[
\Rightarrow s(g_3) = x s(g_2) = xe_2.
\]

\[
\text{spol}(g_3, g_1) = yg_3 - z^2 g_1:
\]
\[
\ s (\text{spol}(g_3, g_1)) = y s(g_3) = xye_2.
\]
Our example again – now with signatures and $\prec_{pot}$

\[ g_1 = xy - z^2, \, s(g_1) = e_1, \]

\[ g_2 = y^2 - z^2, \, s(g_2) = e_2, \]

\[ g_3 = \text{spol}(g_2, g_1) = xg_2 - yg_1 \]

\[ \Rightarrow s(g_3) = x \cdot s(g_2) = xe_2. \]

\[ \text{spol}(g_3, g_1) = yg_3 - z^2g_1: \]

\[ s(\text{spol}(g_3, g_1)) = y \cdot s(g_3) = xye_2. \]

Note that $s(\text{spol}(g_3, g_1)) = xye_2$ and $\text{lm}(g_1) = xy$. 
Our example again – now with signatures and $\prec_{\text{pot}}$

\[
g_1 = xy - z^2, \; s(g_1) = e_1, \\
g_2 = y^2 - z^2, \; s(g_2) = e_2, \\
g_3 = \text{spol}(g_2, g_1) = xg_2 - yg_1
\]

$\Rightarrow s(g_3) = x \cdot s(g_2) = xe_2.$

\[
\text{spol}(g_3, g_1) = yg_3 - z^2g_1:
\]

\[
s\left(\text{spol}(g_3, g_1)\right) = y \cdot s(g_3) = yxe_2.
\]

Note that $s\left(\text{spol}(g_3, g_1)\right) = yxe_2$ and $\text{lm}(g_1) = xy.$

$\Rightarrow \text{We know that } \text{spol}(g_3, g_1) \text{ reduces to zero w.r.t. } G.$
How do we know this?

**General idea**: Per signature we only need to compute 1 element for $G$. 

Choose 1 and remove the others.

**Our goal**: Make good choices.

**Our task**: Keep signatures correct.
**General idea:** Per signature we only need to compute 1 element for $G$.

Several elements with the same signature?
**General idea:** Per signature we only need to compute 1 element for $G$.

Several elements with the same signature?

Choose 1 and remove the others.
**General idea**: Per signature we only need to compute 1 element for $G$.

Several elements with the same signature?

Choose 1 and remove the others.

**Our goal**: Make good choices.
How do we know this?

**General idea:** Per signature we only need to compute 1 element for $G$.

Several elements with the same signature?

Choose 1 and remove the others.

**Our goal:** Make good choices.

**Our task:** Keep signatures correct.
\( \alpha \in \mathbb{R}^m \) stores all data needed:

- Polynomial \( \overline{\alpha} \) with leading term \( \text{lt}(\overline{\alpha}) \).

- Signature \( s(\overline{\alpha}) = s(\alpha) = \text{lt}(\alpha) \).
\( \alpha \in R^m \) stores all data needed:

- Polynomial \( \overline{\alpha} \) with leading term \( \text{lt} (\overline{\alpha}) \).
- Signature \( [s(\alpha) = ] s(\alpha) = \text{lt} (\alpha) \).

**Conventions:**

- \( \alpha \in R^m \) with \( \overline{\alpha} = 0 \) is a syzygy.

- \( s \)-reduction \( \equiv \) polynomial reduction \textbf{while retaining} signature

- \( s \)-reductions are always w.r.t. a finite basis \( G \subset R^m \).
Signature-based Gröbner Bases

- \( \mathcal{G} \) is a **signature-based Gröbner Basis in signature** \( T \) if all \( \alpha \in R^m \) with \( s(\alpha) = T \) \( s \)-reduce to zero w.r.t. \( \mathcal{G} \).

- \( \mathcal{G} \) is a **signature-based Gröbner Basis** if \( \mathcal{G} \) is a signature-based Gröbner Basis in all signatures.

- If \( \mathcal{G} \) is a signature-based Gröbner Basis then \( \{ \overline{\alpha} \mid \alpha \in \mathcal{G} \} \) is a Gröbner Basis for \( \langle f_1, \ldots, f_m \rangle \).
Signature-based Gröbner Bases

- $G$ is a **signature-based Gröbner Basis in signature** $T$ if all $\alpha \in R^m$ with $s(\alpha) = T$ $s$-reduce to zero w.r.t. $G$.

- $G$ is a **signature-based Gröbner Basis** if $G$ is a signature-based Gröbner Basis in all signatures.

- If $G$ is a signature-based Gröbner Basis then $\{\overline{\alpha} \mid \alpha \in G\}$ is a Gröbner Basis for $\langle f_1, \ldots, f_m \rangle$.

**Remark**

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

The pair set is ordered by increasing signature.
The basic problem

Signature basics

Signature-based criteria

A decade in signature-based Gröbner Basis algorithms
Signature-based criteria

\[ s(\alpha) = s(\beta) \implies \text{Compute 1, remove 1.} \]
Signature-based criteria

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

Sketch of proof

1. \( s(\alpha - \beta) \prec s(\alpha), s(\beta) \).
2. All S-pairs are handled by increasing signature.
   \( \Rightarrow \) All relations \( \prec s(\alpha) \) are known:
   \[ \alpha = \beta + \text{elements of smaller signature} \]
Signature-based criteria

S-pairs in signature $T$

Define an order on $R_T$ and choose the maximal element.
Signature-based criteria

S-pairs in signature $T$

What are all possible configurations to reach signature $T$?
S-signature-based criteria

What are all possible configurations to reach signature $T$?

$\mathcal{R}_T = \{ a\alpha \mid \alpha \text{ handled by the algorithm and } s(a\alpha) = T \}$
What are all possible configurations to reach signature $T$?

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

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

\[ R_T = \left\{ a\alpha \mid \alpha \text{ handled by the algorithm and } s(a\alpha) = T \right\} \]
Special cases

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

1. If $a\alpha$ is a syzygy $\implies$ Go on to next signature.
Special cases

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

1. If \( a\alpha \) is a syzygy \( \implies \) Go on to next signature.
2. If \( a\alpha \) is not part of an S-pair \( \implies \) Go on to next signature.
Special cases

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

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

Revisiting our example with $\prec_{pot}$

$$s \left( spol(g_3, g_1) \right) = xye_2$$
$$g_1 = xy - z^2$$
$$g_2 = y^2 - z^2$$

$$\implies psyz(g_2, g_1) = g_1 e_2 - g_2 e_1 = xye_2 + \ldots$$
The basic problem

Signature basics

Signature-based criteria

A decade in signature-based Gröbner Basis algorithms
A decade in signature-based Gröbner Basis algorithms

F5
Faugère (2002)
A decade in signature-based Gröbner Basis algorithms

- **Quasihomog F5**
  - Faugère, Safey El-Din, Verron (2013)

- **F5 using sym**
  - Faugère, Svartz (2013)

- **SAGBI F5**
  - Faugère, Rahmany (2009)

- **Matrix F5**
  - Bardet (2002)

- **F5 with BC**
  - Aris (2005)

- **Bihomog F5**
  - Faugère, Safey El-Din, Spaenlehauer (2011)

- **Extended F5 Criteria**
  - Aris, Hashemi (2009)

- **F4/5**
  - Albrecht, Perry (2010)

- **Involutive F5**
  - Gerdt, Hashemi, Alizadeh (2013)

- **Matrix F5**
  - Bardet (2002)

- **F5C**
  - Perry, E. (2009)

- **iF5A**
  - E. (2012)

- **F5A**
  - Perry, E. (2011)

- **F5 with BC**
  - Aris (2005)

- **AP**
  - Arri, Perry (2009)

- **AP1**
  - Arri, Perry, E. (2011)

- **AP2**
  - Arri, Perry, E. (2012)

- **SB**
  - Roune, Stillmann (2012)

- **nF5**
  - E. (2012)
[FL10] J.-C. Faugère and S. Lachartre. Parallel Gaussian Elimination for Gröbner bases computations in finite fields