A (short) survey on signature-based Gr"obner Basis Algorithms

Christian Eder, Jean-Charles Faug"ere, John Perry and Bjarke Hammersholt Roune

ACA 2014, New York, US

July 10, 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

$$g_1 = xy - z^2, \quad g_2 = y^2 - z^2$$
How to detect zero reductions in advance?

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

\[
\begin{align*}
g_1 &= xy - z^2, \quad g_2 = y^2 - z^2 \\
\text{spol}(g_2, g_1) &= xg_2 - yg_1 = xy^2 - xz^2 - xy^2 + yz^2 \\
&= -xz^2 + yz^2.
\end{align*}
\]

\[\implies g_3 = xz^2 - yz^2.\]
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

\begin{align*}
g_1 &= xy - z^2, \quad g_2 = y^2 - z^2
\end{align*}

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

\[
= -xz^2 + yz^2.
\]

\[\implies g_3 = xz^2 - yz^2.\]

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

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

\[
  g_1 = xy - z^2, \quad g_2 = y^2 - z^2
\]

Then

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

Therefore

\[
  g_3 = xz^2 - yz^2.
\]

Then

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

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

\[
  -y^2 z^2 + z^4 + y^2 z^2 - z^4 = 0.
\]
Let $l = \langle f_1, \ldots, f_m \rangle$.

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

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

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

Signatures

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

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

- 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 $\alpha \mapsto \overline{\alpha} : R^m \to R$ 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 \( R^m \) be generated by \( e_1, \ldots, e_m \) and let \( \prec \) be a compatible monomial order on the monomials of \( R^m \).

- Let \( \alpha \mapsto \overline{\alpha} : R^m \rightarrow R \) such that \( \overline{e_i} = f_i \) for all \( i \).

- 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:

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

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

- **A signature** of $f$ is given by $\sigma(f) = \text{lt}_\prec(\alpha)$ 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 \( R^m \) be generated by \( e_1, \ldots, e_m \) and let \( \prec \) be a compatible monomial order on the monomials of \( R^m \).

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

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

- **A signature** of \( f \) is given by \( s(f) = \text{lt}_{\prec}(\alpha) \) where \( f = \overline{\alpha} \).

- An element \( \alpha \in R^m \) with \( \overline{\alpha} = 0 \) is called a **syzygy**.
Our example again – with signatures and $\langle\text{pot}\rangle$

\[ g_1 = xy - z^2, \ s(g_1) = e_1, \]
\[ g_2 = y^2 - z^2, \ s(g_2) = e_2. \]
Our example again – with signatures and $\prec_{\text{pot}}$

\[
g_1 = xy - z^2, \quad s(g_1) = e_1, \\
g_2 = y^2 - z^2, \quad s(g_2) = e_2.
\]

\[
g_3 = \text{spol}(g_2, g_1) = xg_2 - yg_1 \\
\Rightarrow s(g_3) = xs(g_2) = xe_2.
\]
Our example again – with signatures and $\preceq_{\text{pot}}$

\[ g_1 = xy - z^2, \quad s(g_1) = e_1, \]
\[ g_2 = y^2 - z^2, \quad s(g_2) = e_2. \]

\[ g_3 = \text{spol}(g_2, g_1) = xg_2 - yg_1 \]
\[ \Rightarrow s(g_3) = xs(g_2) = xe_2. \]

\[ \text{spol}(g_3, g_1) = yg_3 - z^2 g_1 \]
\[ \Rightarrow s(\text{spol}(g_3, g_1)) = ys(g_3) = xye_2. \]

Note that $s(\text{spol}(g_3, g_1)) = xye_2$ and $lm(g_1) = xy$. 

4 / 16
Our example again – with signatures and $\prec_{\text{pot}}$

\[ g_1 = xy - z^2, \ s(g_1) = e_1, \]
\[ g_2 = y^2 - z^2, \ s(g_2) = e_2. \]

\[ g_3 = \text{spol}(g_2, g_1) = xg_2 - yg_1 \]
\[ \Rightarrow s(g_3) = x \ s(g_2) = xe_2. \]

\[ \text{spol}(g_3, g_1) = yg_3 - z^2 g_1 \]
\[ \Rightarrow s(\text{spol}(g_3, g_1)) = y \ s(g_3) = yxe_2. \]

Note that $s(\text{spol}(g_3, g_1)) = yxe_2$ and $\text{lm}(g_1) = xy$. 
Think in the module

\[ \alpha \in R^m \implies \text{polynomial } \overline{\alpha} \text{ with } \text{lt} (\overline{\alpha}), \text{signature } s(\alpha) = \text{lt} (\alpha) \]
Think in the module

\[ \alpha \in R^m \implies \text{polynomial } \overline{\alpha} \text{ with } \text{lt}(\overline{\alpha}), \text{signature } s(\alpha) = \text{lt}(\alpha) \]

S-pairs/S-polynomials:

\[ \text{spol} \left( \overline{\alpha}, \overline{\beta} \right) = a\overline{\alpha} - b\overline{\beta} \implies \text{spair} \left( \alpha, \beta \right) = a\alpha - b\beta \]
Think in the module

\[ \alpha \in R^m \Rightarrow \text{polynomial } \overline{\alpha} \text{ with } \text{lt} (\overline{\alpha}) \text{, signature } s(\alpha) = \text{lt} (\alpha) \]

S-pairs/S-polynomials:

\[ \text{spol} \left( \overline{\alpha}, \overline{\beta} \right) = a\overline{\alpha} - b\overline{\beta} \Rightarrow \text{spair} \left( \alpha, \beta \right) = a\alpha - b\beta \]

s-reductions:

\[ \overline{\gamma} - d\overline{\delta} \Rightarrow \gamma - d\delta \]
Think in the module

\[ \alpha \in R^m \implies \text{polynomial } \overline{\alpha} \text{ with } \text{lt}(\overline{\alpha}), \text{signature } s(\alpha) = \text{lt}(\alpha) \]

S-pairs/S-polynomials:

\[ \text{spol}(\overline{\alpha}, \beta) = a\overline{\alpha} - b\beta \implies \text{spair}(\alpha, \beta) = a\alpha - b\beta \]

$s$-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

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

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

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

$$\mathcal{K}_T = \{ a\alpha \mid \alpha \text{ handled by the algorithm and } s(a\alpha) = T \}$$
Signature-based criteria

S-pairs in signature $T$

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

- What are all possible configurations to reach signature $T$?
- Define an order $\triangleleft$ on $\mathcal{R}_T$ and choose the maximal element.
Special cases

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

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

Choose \( b\beta \) to be an element of \( \mathcal{R}_T \) maximal w.r.t. an order \( \trianglelefteq \).
Special cases

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

Choose \( b\beta \) to be an element of \( \mathcal{R}_T \) maximal w.r.t. an order \( \preceq \).

1. If \( b\beta \) is a syzygy \( \implies \) Go on to next signature.
Special cases

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

Choose \( b\beta \) to be an element of \( \mathcal{R}_T \) maximal w.r.t. an order \( \sqsubseteq \).

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

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

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

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

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

$s(spol(g_3, g_1)) = xye_2$

$g_1 = xy - z^2$

$g_2 = y^2 - z^2$ \Rightarrow psyz(g_2, g_1) = g_1e_2 - g_2e_1 = xye_2 + \ldots$
Where are the differences?

There are three different choices you can make:
Where are the differences?

There are three different choices you can make:

1. Choose a module monomial order \(\prec\) compatible to \(<\).

   ▶ \(\alpha \in G \lessdot_{\prec} \beta\) syzygy
   ▶ \(\beta\) added to \(G\) after \(\alpha\) or \(s(\alpha) \lessdot_{\prec} s(\beta) \lessdot_{\prec} \alpha\).
Where are the differences?

There are three different choices you can make:

1. Choose a module monomial order $\prec$ compatible to $\prec$.

2. Choose an order on the pair set $P$.
   Common choice: By increasing signature
Where are the differences?

There are three different choices you can make:

1. Choose a module monomial order $\prec$ compatible to $\lt$.

2. Choose an order on the pair set $P$.
   Common choice: By increasing signature

3. Choose a rewrite order $\triangleleft$ on $R_T$ such that $\alpha \triangleleft \beta$:
   Common choices:
   - $\alpha \in \mathcal{G} \triangleleft \beta$ syzygy
   - $\beta$ added to $\mathcal{G}$ after $\alpha$ or $\text{lt}(\alpha) \lt \text{lt}(\beta) \lt \text{lt}(\overline{\alpha})$.  

Buchberger’s criteria?

Buchberger’s Product and Chain criterion can be combined with easily:
Buchberger’s criteria?

Buchberger’s Product and Chain criterion can be combined with easily:

Chain criterion is a special case of the Rewrite criterion ⇒ already included.
Buchberger’s criteria?

Buchberger’s Product and Chain criterion can be combined with easily:

- **Chain criterion** is a special case of the Rewrite criterion ⇒ already included.

- **Product criterion** is not always (but mostly) included.

\[
\begin{align*}
\alpha & \text{ added to } G \\
\Rightarrow & \text{ Generate all possible principal syzygies with } \alpha \\
& \text{ (e.g. } GVW) \\
\end{align*}
\]

\[
\begin{align*}
& \text{ S-pair fulfilling Product criterion} \\
& \Rightarrow & \text{ Add one corresponding syzygy.} \\
& \text{(e.g. } SB \text{ in Singular}) \\
\end{align*}
\]
Buchberger’s criteria?

Buchberger’s Product and Chain criterion can be combined with easily:

Chain criterion is a special case of the Rewrite criterion
\[ \Rightarrow \text{already included.} \]

Product criterion is not always (but mostly) included.

\[ \alpha \text{ added to } G \]

\[ \nabla \]

Generate all possible principal syzygies with \( \alpha \).

(e.g. GVW)
Buchberger’s criteria?
Buchberger’s Product and Chain criterion can be combined with easily:

Chain criterion is a special case of the Rewrite criterion  
⇒ already included.

Product criterion is not always (but mostly) included.

\[ \alpha \text{ added to } G \]

\[ \text{Generate all possible principal syzygies with } \alpha. \]
\[ (\text{e.g. GVW}) \]

S-pair fulfilling Product criterion not detected by Rewrite criterion  
\[ \text{Add one corresponding syzygy.} \]
\[ (\text{e.g. SB in Singular}) \]
References I


References III


