Signature Rewriting in Gröbner Basis Computation

Christian Eder
joint work with Bjarke Hammersholt Roune

POLSYS Team, UPMC, Paris, France

June 29, 2013
Signature-based algorithms

The basic idea

Generic signature-based criteria

Rewritable signature criterion in detail
Signatures of polynomials

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 \( e_1, \ldots, e_m \), \( \prec \) a well-ordering on the monomials of \( R_m \), and let \( \alpha \mapsto \alpha : R_m \to R \) such that \( e_i = f_i \) for all \( i \).
2. Each \( p \in I \) can be represented by an \( \alpha = \sum_{i=1}^{m} h_i e_i \in R_m \) such that \( p = \alpha \).
3. A signature of \( p \) is given by \( s(p) = \text{lt}_{\prec}(\alpha) \) with \( p = \alpha \).
4. A minimal signature of \( p \) exists due to \( \prec \).
Signatures of polynomials

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 $e_1, \ldots, e_m$, $\prec$ a well-ordering on the monomials of $R^m$, and let $\alpha \mapsto \overline{\alpha} : R^m \to R$ such that

   $$\overline{e}_i = f_i$$

   for all $i$. 

Signatures of polynomials

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 $e_1, \ldots, e_m$, $\prec$ a well-ordering on the monomials of $R^m$, and let $\alpha \mapsto \overline{\alpha} : R^m \to R$ such that

   \[ \overline{e_i} = f_i \text{ for all } i. \]

2. Each $p \in I$ can be represented by an

   \[ \alpha = \sum_{i=1}^{m} h_i e_i \in R^m \text{ such that } p = \overline{\alpha}. \]
Signatures of polynomials

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 \( e_1, \ldots, e_m \), \( \prec \) a well-ordering on the monomials of \( R^m \), and let \( \alpha \mapsto \overline{\alpha} : R^m \to R \) such that
   \[
   \overline{e}_i = f_i \text{ for all } i.
   \]

2. Each \( p \in I \) can be represented by an
   \[
   \alpha = \sum_{i=1}^{m} h_ie_i \in R^m \text{ such that } p = \overline{\alpha}.
   \]

3. **A signature** of \( p \) is given by
   \[
   s(p) = \text{lt}_\prec(\alpha) \text{ with } p = \overline{\alpha}.
   \]
Signatures of polynomials

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 $e_1, \ldots, e_m$, $\prec$ a well-ordering on the monomials of $R^m$, and let $\alpha \mapsto \overline{\alpha} : R^m \to R$ such that
   \[ \overline{e_i} = f_i \text{ for all } i. \]

2. Each $p \in I$ can be represented by an
   \[ \alpha = \sum_{i=1}^{m} h_i e_i \in R^m \text{ such that } p = \overline{\alpha}. \]

3. A signature of $p$ is given by
   \[ s(p) = \text{lt}_\prec(\alpha) \text{ with } p = \overline{\alpha}. \]

4. A minimal signature of $p$ exists due to $\prec$. 
Notations concerning signatures

Let $\alpha \in R^m$, then $\alpha$ contains all data we need:

- The polynomial data is $\overline{\alpha}$, its leading term denoted by $\text{lt}(\overline{\alpha})$.
- The signature is $s(\alpha) = \text{lt}(\alpha)$.
Notations concerning signatures

Let $\alpha \in R^m$, then $\alpha$ contains all data we need:

- The polynomial data is $\overline{\alpha}$, its leading term denoted by $\text{lt}(\overline{\alpha})$.
- The signature is $s(\alpha) = \text{lt}(\alpha)$.

Moreover, we agree on the following:

- For $\alpha, \beta \in R^m$, let $\alpha \simeq \beta$ if $\alpha = s\beta$ for some $s \in K$. In the same sense we define $\overline{\alpha} \simeq \overline{\beta}$ if $\overline{\alpha} = t\overline{\beta}$ for some $t \in K$.

- $G$ always denotes a finite subset of $R^m$ such that for all $\alpha, \beta \in G$ with $s(\alpha) \simeq s(\beta)$ it holds that $\alpha = \beta$.

- $\alpha \in R^m$ is called a syzygy if $\overline{\alpha} = 0$. 
Reductions concerning signatures

Let \( \alpha \in R^m \), and let \( t \) be a term of \( \overline{\alpha} \). We can \( s \)-reduce \( t \) by \( \beta \in R^m \) if

\[
\begin{align*}
\exists \text{ a term } b & \text{ such that } \text{lt} (b\beta) = t \text{ and } \\
\text{s} (b\beta) & \preceq s (\alpha).
\end{align*}
\]
Let $\alpha \in R^m$, and let $t$ be a term of $\overline{\alpha}$. We can $s$-reduce $t$ by $\beta \in R^m$ if

$\exists$ a term $b$ such that $\text{lt}(b\beta) = t$ and $s(b\beta) \preceq s(\alpha)$.

**Note**

We distinguish 2 types of $s$-reduction:
Reductions concerning signatures

Let $\alpha \in R^m$, and let $t$ be a term of $\alpha$. We can $s$-reduce $t$ by $\beta \in R^m$ if

- $\exists$ a term $b$ such that $\text{lt}(b\beta) = t$ and
- $s(b\beta) \preceq s(\alpha)$.

Note

We distinguish 2 types of $s$-reduction:

1. If $\text{lt}(b\beta) \sim \text{lt}(\alpha) \implies$ top $s$-reduction step;
   otherwise $\implies$ tail $s$-reduction step.
Let $\alpha \in R^m$, and let $t$ be a term of $\bar{\alpha}$. We can $s$-reduce $t$ by $\beta \in R^m$ if

- $\exists$ a term $b$ such that $\text{lt}(b\beta) = t$ and
- $s(b\beta) \preceq s(\alpha)$.

**Note**

We distinguish 2 types of $s$-reduction:

1. If $\text{lt}(b\beta) \simeq \text{lt}(\bar{\alpha}) \implies \text{top } s$-reduction step;
   otherwise $\implies \text{tail } s$-reduction step.

2. If $s(b\beta) \simeq s(\alpha) \implies \text{singular } s$-reduction step;
   otherwise $\implies \text{regular } s$-reduction step.
Signature Gröbner bases

- \( s \)-reductions are always performed w.r.t. a finite basis \( \mathcal{G} \subset R^m \).

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

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

**Note**

In the following we do not need much of the details of signature-based Gröbner basis algorithms, just one property:

**The pair set is ordered by increasing signatures.**
Generic signature-based criteria

Non-minimal signature ( NM )

$s(\alpha)$ not minimal for $\alpha$? $\Rightarrow$ Remove $\alpha$. 

Sketch of proof

1. There exists a syzygy $\beta \in R_m$ such that $\text{lt}(\beta) = s(\alpha)$. $\Rightarrow$ We can represent $\alpha$ with a lower signature.
2. Pairs are handled by increasing signatures. $\Rightarrow$ All relations of lower signature are already taken care of.
Generic signature-based criteria

Non-minimal signature (NM)

$\mathcal{s}(\alpha)$ not minimal for $\alpha$? $\Rightarrow$ Remove $\alpha$.

Sketch of proof

1. There exists a syzygy $\beta \in R^m$ such that $\text{lt}(\beta) = \mathcal{s}(\alpha)$.
   $\Rightarrow$ We can represent $\bar{\alpha}$ with a lower signature.

2. Pairs are handled by increasing signatures.
   $\Rightarrow$ All relations of lower signature are already taken care of.
Generic signature-based criteria

**Rewritable signature ( RW )**

\[ s(\alpha) = s(\beta) \implies \text{Remove either } \alpha \text{ or } \beta. \]
Rewritable signature (RW)

$s(\alpha) = s(\beta) \Rightarrow$ Remove either $\alpha$ or $\beta$.

**Sketch of proof**

1. $s(\alpha - \beta) \prec s(\alpha), s(\beta)$.
2. Pairs are handled by increasing signatures.
   $\Rightarrow$ All necessary computations of lower signature have already taken place.
   $\Rightarrow$ We can represent $\beta$ by

   \[
   \beta = \alpha + \text{elements of lower signature}.
   \]
Signature-based algorithms
The basic idea
Generic signature-based criteria

Rewritable signature criterion in detail
The concept of rewrite bases

Rewriter and rewritable elements
Rewriter and rewritable elements

- A **rewrite order** $\triangleleft$ is a total order on $\mathcal{G}$ such that $s(\alpha) \mid s(\beta) \Rightarrow \alpha \triangleleft \beta$. (Exists due to $s(\alpha) \simeq s(\beta) \Rightarrow \alpha = \beta$.)
Rewriter and rewratable elements

- A **rewrite order** $\triangleleft$ is a total order on $\mathcal{G}$ such that $s(\alpha) \mid s(\beta) \Rightarrow \alpha \triangleleft \beta$. (Exists due to $s(\alpha) \simeq s(\beta) \Rightarrow \alpha = \beta$.)

- An element $\alpha \in \mathcal{G}$ is a **rewriter in signature** $\mathcal{T}$ if $s(\alpha) \mid \mathcal{T}$. 
Rewriter and rewritable elements

- A **rewrite order** $\triangleright$ is a total order on $G$ such that $s(\alpha) \triangleright s(\beta) \Rightarrow \alpha \triangleright \beta$. (Exists due to $s(\alpha) \simeq s(\beta) \Rightarrow \alpha = \beta$.)

- An element $\alpha \in G$ is a **rewriter in signature** $T$ if $s(\alpha) \triangleright T$.

- The $\triangleleft$-maximal rewriter in signature $T$ is the **canonical rewriter in** $T$. 
The concept of rewrite bases

Rewriter and rewritable elements

- A **rewrite order** \(<\)** is a total order on \( \mathcal{G} \) such that \( s(\alpha) | s(\beta) \Rightarrow \alpha \triangleleft \beta \). (Exists due to \( s(\alpha) \simeq s(\beta) \Rightarrow \alpha = \beta \).)

- An element \( \alpha \in \mathcal{G} \) is a **rewriter in signature** \( T \) if \( s(\alpha) | T \).

- The \( \triangleleft \)-maximal rewriter in signature \( T \) is the **canonical rewriter in** \( T \).

- A multiple of a basis element \( t\alpha \) is called **rewritable** if \( \alpha \) is not the canonical rewriter in \( s(t\alpha) \).
The concept of rewrite bases

Rewrite Bases

G is a rewrite basis in signature T if the canonical rewriter in T is not regular \( s \)-reducible or if T is a syzygy signature.

G is a rewrite basis if it is a rewrite basis in all signatures.

Lemma
If G is a rewrite basis up to signature T then G is also a signature Gröbner basis up to T.
The concept of rewrite bases

Rewrite Bases

▶ \( \mathcal{G} \) is a \textbf{rewrite basis in signature} \( T \) if the canonical rewriter in \( T \) is not regular \( s \)-reducible or if \( T \) is a syzygy signature.
The concept of rewrite bases

Rewrite Bases

- $\mathcal{G}$ is a **rewrite basis in signature** $T$ if the canonical rewriter in $T$ is not regular $s$-reducible or if $T$ is a syzygy signature.
- $\mathcal{G}$ is a **rewrite basis** if it is a rewrite basis in all signatures.
The concept of rewrite bases

Rewrite Bases

- \( G \) is a **rewrite basis in signature** \( T \) if the canonical rewriter in \( T \) is not regular \( s \)-reducible or if \( T \) is a syzygy signature.

- \( G \) is a **rewrite basis** if it is a rewrite basis in all signatures.

**Lemma**

If \( G \) is a rewrite basis up to signature \( T \) then \( G \) is also a signature Gröbner basis up to \( T \).
Improving the rewritable signature criterion

RB (generic rewrite base algorithm)

Let $\alpha$ and $\beta \in G$ such that $s(\alpha) = a \cdot e^i$ and $s(\beta) = b \cdot e^j$.

$\alpha \prec \beta \iff (i < j) \text{ or } (i = j \text{ and } a < b)$

Once an $s$-polynomial in a given signature $T$ is computed all others are rewritable.

$\alpha \prec \beta \iff s(\alpha) \lt(\alpha) \prec s(\beta) \lt(\beta)$

For any signature $T$ define $M_T = \{ t_\alpha \mid \alpha \in G, s(t_\alpha) = T \}$

Choose $t_\alpha$ such that $\lt(t_\alpha)$ is minimal.

Difference: There might be no such $s$-polynomial.
Improving the rewritable signature criterion

RB (generic rewrite base algorithm)

F5
(as presented in [Fa02])

Let \( \alpha \) and \( \beta \) \( \in G \) such that \( s(\alpha) = a^{e_i} \) and \( s(\beta) = b^{e_j} \).

\[ \alpha \triangleleft \beta \iff (i < j) \text{ or } (i = j \text{ and } a < b) \]

Once an \( s \)-polynomial in a given signature \( T \) is computed all others are rewritable.

\[ \alpha \triangleleft \beta \iff s(\alpha) \prec s(\beta) \]

For any signature \( T \) define \( M_T = \{ t_\alpha | \alpha \in G, s(t_\alpha) = T \} \)

Choose \( t_\alpha \) such that \( \prec t_\alpha \) is minimal.

Difference: There might be no such \( s \)-polynomial
Improving the rewritable signature criterion

RB (generic rewrite base algorithm)

F5
(as presented in [Fa02])

AP/GVW/SB

Let $\alpha$ and $\beta \in G$ such that $s(\alpha) = a^i e_i$ and $s(\beta) = b^j e_j$.

$\alpha \triangleright \beta \iff (i < j) \text{ or } (i = j \text{ and } a < b)$

Once an $s$-polynomial in a given signature $T$ is computed all others are rewritable.

$\alpha \triangleright \beta \iff s(\alpha) \prec s(\beta)$

For any signature $T$ define $M_T = \{ t_\alpha | \alpha \in G, s(t_\alpha) = T \}$

Choose $t_\alpha$ such that $\prec t_\alpha$ is minimal.

Difference: There might be no such $s$-polynomial.
Let $\alpha$ and $\beta \in \mathcal{G}$ such that $s(\alpha) = ae_i$ and $s(\beta) = be_j$. 
Let $\alpha$ and $\beta \in G$ such that $s(\alpha) = ae_i$ and $s(\beta) = be_j$.

\[
\alpha \triangleleft \beta \iff (i < j) \text{ or } (i = j \text{ and } a < b)
\]

Once an $s$-polynomial in a given signature $T$ is computed all others are rewritable.
Improving the rewritable signature criterion

Let $\alpha$ and $\beta \in G$ such that $s(\alpha) = ae_i$ and $s(\beta) = be_j$.

$\alpha \triangleleft \beta \iff \begin{cases} i < j \text{ or } (i = j \text{ and } a < b) \end{cases}$

Once an $s$-polynomial in a given signature $T$ is computed all others are rewritable.

For any signature $T$ define

\[ M_T = \{ t\alpha \mid \alpha \in G, s(t\alpha) = T \} \]

Choose $t\alpha$ such that $\text{lt}(t\alpha)$ is minimal.
Improving the rewritable signature criterion

RB (generic rewrite base algorithm)

F5 (as presented in [Fa02])

AP/GVW/SB

Let $\alpha$ and $\beta \in G$ such that $s(\alpha) = ae_i$ and $s(\beta) = be_j$.

$\alpha \triangleleft \beta \iff (i < j) \text{ or } (i = j \text{ and } a < b)$

Once an $s$-polynomial in a given signature $T$ is computed all others are rewritable.

$\alpha \triangleleft \beta \iff \frac{s(\alpha)}{\text{lt}(\alpha)} < \frac{s(\beta)}{\text{lt}(\beta)}$

For any signature $T$ define $M_T = \{ t\alpha | \alpha \in G, s(t\alpha) = T \}$

Choose $t\alpha$ such that $\text{lt}(t\alpha)$ is minimal.

Difference: There might be no such $s$-polynomial
Example for differences in the rewritable signature criterion

Let $K$ be the finite field with 13 elements and let $R := K[x, y, z, t]$. Let $<$ be the graded reverse lexicographic monomial ordering. Consider the three input elements

$$g_1 := -2y^3 - x^2 z - 2x^2 t - 3y^2 t,$$
$$g_2 := 3xyz + 2xyt,$$
$$g_3 := 2xyz - 2yz^2 + 2z^3 + 4yzt.$$
Example for differences in the rewritable signature criterion

Let $K$ be the finite field with 13 elements and let $R := K[x, y, z, t]$. Let $<$ be the graded reverse lexicographic monomial ordering. Consider the three input elements

$$g_1 := -2y^3 - x^2 z - 2x^2 t - 3y^2 t,$$
$$g_2 := 3xyz + 2xyt,$$
$$g_3 := 2xyz - 2yz^2 + 2z^3 + 4yzt.$$

<table>
<thead>
<tr>
<th>$\alpha_i \in \mathcal{G}$</th>
<th>reduced from</th>
<th>$\text{lt}(\alpha_i)$</th>
<th>$\mathcal{s}(\alpha_i)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\alpha_1$</td>
<td>$e_1$</td>
<td>$y^3$</td>
<td>$e_1$</td>
</tr>
<tr>
<td>$\alpha_2$</td>
<td>$e_2$</td>
<td>$xyz$</td>
<td>$e_2$</td>
</tr>
<tr>
<td>$\alpha_3$</td>
<td>$y^2 \alpha_2 - xz \alpha_1 = S(\alpha_2, \alpha_1)$</td>
<td>$x^3 z^2$</td>
<td>$y^2 e_2$</td>
</tr>
<tr>
<td>$\alpha_4$</td>
<td>$e_3$</td>
<td>$yz^2$</td>
<td>$e_3$</td>
</tr>
<tr>
<td>$\alpha_5$</td>
<td>$x \alpha_4 - z \alpha_2 = S(\alpha_4, \alpha_2)$</td>
<td>$xz^3$</td>
<td>$xe_3$</td>
</tr>
<tr>
<td>$\alpha_6$</td>
<td>$y^2 \alpha_4 - z^2 \alpha_1 = S(\alpha_4, \alpha_1)$</td>
<td>$x^2 z^3$</td>
<td>$y^2 e_3$</td>
</tr>
<tr>
<td>$\alpha_7$</td>
<td>$y \alpha_5 - z^2 \alpha_2 = S(\alpha_5, \alpha_2)$</td>
<td>$x^2 y^2 t$</td>
<td>$xye_3$</td>
</tr>
<tr>
<td>$\alpha_8$</td>
<td>$x \alpha_5 - \alpha_6 = S(\alpha_5, \alpha_6)$</td>
<td>$z^5$</td>
<td>$x^2 e_3$</td>
</tr>
<tr>
<td>$\alpha_9$</td>
<td>$x \alpha_6 - z \alpha_3 = S(\alpha_6, \alpha_3)$</td>
<td>$x^4 zt$</td>
<td>$xy^2 e_3$</td>
</tr>
<tr>
<td>$\alpha_{10}$</td>
<td>$y \alpha_8 - z^3 \alpha_4 = S(\alpha_8, \alpha_4)$</td>
<td>$x^3 y^2 t$</td>
<td>$x^2 ye_3$</td>
</tr>
<tr>
<td>$\alpha_{11}$</td>
<td>$x^3 \alpha_4 - y \alpha_3 = S(\alpha_4, \alpha_3)$</td>
<td>$x^4 yt$</td>
<td>$x^3 e_3$</td>
</tr>
<tr>
<td>$\alpha_{12}$</td>
<td>$z \alpha_{11} - x^3 \alpha_2 = S(\alpha_{11}, \alpha_2)$</td>
<td>$x^3 zt^3$</td>
<td>$x^3 ze_3$</td>
</tr>
<tr>
<td>$\alpha_{13}$</td>
<td>$y \alpha_{10} - x^3 \alpha_1 = S(\alpha_{10}, \alpha_1)$</td>
<td>$x^5 zt$</td>
<td>$x^2 y^2 e_3$</td>
</tr>
<tr>
<td>$\alpha_{14}$</td>
<td>$x \alpha_{12} - \alpha_9 = S(\alpha_{12}, \alpha_9)$</td>
<td>$x^4 t^4$</td>
<td>$x^4 ze_3$</td>
</tr>
</tbody>
</table>
Example for differences in the rewritable signature criterion

Let $K$ be the finite field with 13 elements and let $R := K[x, y, z, t]$. Let $<$ be the graded reverse lexicographic monomial ordering. Consider the three input elements

$$g_1 := -2y^3 - x^2z - 2x^2t - 3y^2t,$$  
$$g_2 := 3xyz + 2xyt,$$  
$$g_3 := 2xyz - 2yz^2 + 2z^3 + 4yzt.$$

<table>
<thead>
<tr>
<th>$\alpha_i \in G$</th>
<th>reduced from</th>
<th>$\text{lt} (\overline{\alpha_i})$</th>
<th>$s(\alpha_i)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\alpha_1$</td>
<td>$e_1$</td>
<td>$y^3$</td>
<td>$e_1$</td>
</tr>
<tr>
<td>$\alpha_2$</td>
<td>$e_2$</td>
<td>$xyz$</td>
<td>$e_2$</td>
</tr>
<tr>
<td>$\alpha_3$</td>
<td>$y^2\alpha_2 - xz\alpha_1 = S(\alpha_2, \alpha_1)$</td>
<td>$x^3z^2$</td>
<td>$y^2e_2$</td>
</tr>
<tr>
<td>$\alpha_4$</td>
<td>$e_3$</td>
<td>$yz^2$</td>
<td>$e_3$</td>
</tr>
<tr>
<td>$\alpha_5$</td>
<td>$x\alpha_4 - z\alpha_2 = S(\alpha_4, \alpha_2)$</td>
<td>$xz^3$</td>
<td>$xe_3$</td>
</tr>
<tr>
<td>$\alpha_6$</td>
<td>$y^2\alpha_4 - z^2\alpha_1 = S(\alpha_4, \alpha_1)$</td>
<td>$x^2z^3$</td>
<td>$y^2e_3$</td>
</tr>
<tr>
<td>$\alpha_7$</td>
<td>$y\alpha_5 - z^2\alpha_2 = S(\alpha_5, \alpha_2)$</td>
<td>$x^2y^2t$</td>
<td>$xye_3$</td>
</tr>
<tr>
<td>$\alpha_8$</td>
<td>$x\alpha_5 - \alpha_6 = S(\alpha_5, \alpha_6)$</td>
<td>$z^5$</td>
<td>$x^2e_3$</td>
</tr>
<tr>
<td>$\alpha_9$</td>
<td>$x\alpha_6 - z\alpha_3 = S(\alpha_6, \alpha_3)$</td>
<td>$x^4zt$</td>
<td>$xy^2e_3$</td>
</tr>
<tr>
<td>$\alpha_{10}$</td>
<td>$y\alpha_8 - z^3\alpha_4 = S(\alpha_8, \alpha_4)$</td>
<td>$x^3y^2t$</td>
<td>$x^2ye_3$</td>
</tr>
<tr>
<td>$\alpha_{11}$</td>
<td>$x^3\alpha_4 - y\alpha_3 = S(\alpha_4, \alpha_3)$</td>
<td>$x^4yt$</td>
<td>$x^3e_3$</td>
</tr>
<tr>
<td>$\alpha_{12}$</td>
<td>$z\alpha_{11} - x^3\alpha_2 = S(\alpha_{11}, \alpha_2)$</td>
<td>$x^3zt^3$</td>
<td>$x^3ze_3$</td>
</tr>
<tr>
<td>$\alpha_{13}$</td>
<td>$y\alpha_{10} - x^3\alpha_1 = S(\alpha_{10}, \alpha_1)$</td>
<td>$x^5zt$</td>
<td>$x^2y^2e_3$</td>
</tr>
<tr>
<td>$\alpha_{14}$</td>
<td>$x\alpha_{12} - \alpha_9 = S(\alpha_{12}, \alpha_9)$</td>
<td>$x^4t^4$</td>
<td>$x^4ze_3$</td>
</tr>
</tbody>
</table>
Example for differences in the rewritable signature criterion

Let $K$ be the finite field with 13 elements and let $R := K[x, y, z, t]$. Let $<$ be the graded reverse lexicographic monomial ordering. Consider the three input elements

$g_1 := -2y^3 - x^2 z - 2x^2 t - 3y^2 t$,  $g_2 := 3xyz + 2xyt$,

$g_3 := 2xyz - 2yz^2 + 2z^3 + 4yzt$.

<table>
<thead>
<tr>
<th>$\alpha_i \in G$</th>
<th>reduced from</th>
<th>$\text{lt} (\alpha_i)$</th>
<th>$s(\alpha_i)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\alpha_1$</td>
<td>$\mathbf{e}_1$</td>
<td>$y^3$</td>
<td>$\mathbf{e}_1$</td>
</tr>
<tr>
<td>$\alpha_2$</td>
<td>$\mathbf{e}_2$</td>
<td>$xyz$</td>
<td>$\mathbf{e}_2$</td>
</tr>
<tr>
<td>$\alpha_3$</td>
<td>$y^2\alpha_2 - xz\alpha_1 = S(\alpha_2, \alpha_1)$</td>
<td>$x^3 z^2$</td>
<td>$y^2 \mathbf{e}_2$</td>
</tr>
<tr>
<td>$\alpha_4$</td>
<td>$\mathbf{e}_3$</td>
<td>$yz^2$</td>
<td>$\mathbf{e}_3$</td>
</tr>
<tr>
<td>$\alpha_5$</td>
<td>$x\alpha_4 - z \alpha_2 = S(\alpha_4, \alpha_2)$</td>
<td>$xz^3$</td>
<td>$x \mathbf{e}_3$</td>
</tr>
<tr>
<td>$\alpha_6$</td>
<td>$y^2\alpha_4 - z^2 \alpha_1 = S(\alpha_4, \alpha_1)$</td>
<td>$x^2 z^3$</td>
<td>$y^2 \mathbf{e}_3$</td>
</tr>
<tr>
<td>$\alpha_7$</td>
<td>$y\alpha_5 - z^2 \alpha_2 = S(\alpha_5, \alpha_2)$</td>
<td>$x^2 y^2 t$</td>
<td>$xy \mathbf{e}_3$</td>
</tr>
<tr>
<td>$\alpha_8$</td>
<td>$x\alpha_5 - \alpha_6 = S(\alpha_5, \alpha_6)$</td>
<td>$z^5$</td>
<td>$x^2 \mathbf{e}_3$</td>
</tr>
<tr>
<td>$\alpha_9$</td>
<td>$x\alpha_6 - z \alpha_3 = S(\alpha_6, \alpha_3)$</td>
<td>$x^4 zt$</td>
<td>$xy^2 \mathbf{e}_3$</td>
</tr>
<tr>
<td>$\alpha_{10}$</td>
<td>$y\alpha_8 - z^3 \alpha_4 = S(\alpha_8, \alpha_4)$</td>
<td>$x^3 y^2 t$</td>
<td>$x^2 y \mathbf{e}_3$</td>
</tr>
<tr>
<td>$\alpha_{11}$</td>
<td>$x^3 \alpha_4 - y \alpha_3 = S(\alpha_4, \alpha_3)$</td>
<td>$x^4 yt$</td>
<td>$x^3 \mathbf{e}_3$</td>
</tr>
<tr>
<td>$\alpha_{12}$</td>
<td>$z \alpha_{11} - x^3 \alpha_2 = S(\alpha_{11}, \alpha_2)$</td>
<td>$x^3 zt^3$</td>
<td>$x^3 \mathbf{z e}_3$</td>
</tr>
<tr>
<td>$\alpha_{13}$</td>
<td>$y\alpha_{10} - x^3 \alpha_1 = S(\alpha_{10}, \alpha_1)$</td>
<td>$x^5 zt$</td>
<td>$x^2 y^2 \mathbf{e}_3$</td>
</tr>
<tr>
<td>$\alpha_{14}$</td>
<td>$x\alpha_{12} - \alpha_9 = S(\alpha_{12}, \alpha_9)$</td>
<td>$x^4 t^4$</td>
<td>$x^4 \mathbf{z e}_3$</td>
</tr>
</tbody>
</table>


[Ga12b] V. Galkin. Simple signature-based Groebner basis algorithm


