# Signature-based Gröbner basis computation

Christian Eder

POLSYS Team, UPMC, Paris, France

March 08, 2013

### Example

Let $I = \langle g_1, g_2 \rangle \in \mathbb{Q}[x, y, z]$ be given where $\mathbf{g_1} = \mathbf{xy} - \mathbf{z^2}$, $\mathbf{g_2} = \mathbf{y^2} - \mathbf{z^2}$, and let $<$ be the graded reverse lexicographical ordering.

# How to predict zero reductions?

## Example

Let $I = \langle g_1, g_2 \rangle \in \mathbb{Q}[x, y, z]$ be given where $\mathbf{g_1} = \mathbf{xy} - \mathbf{z^2}$, $\mathbf{g_2} = \mathbf{y^2} - \mathbf{z^2}$, and let $<$ be the graded reverse lexicographical ordering.

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

so it reduces w.r.t. $G$ to $\mathbf{g_3} = \mathbf{xz^2} - \mathbf{yz^2}$.

# How to predict zero reductions?

**Example**

Let $I = \langle g_1, g_2 \rangle \in \mathbb{Q}[x, y, z]$ be given where $\mathbf{g_1} = \mathbf{xy} - \mathbf{z^2}$, $\mathbf{g_2} = \mathbf{y^2} - \mathbf{z^2}$, and let $<$ be the graded reverse lexicographical ordering.

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

so it reduces w.r.t. $G$ to $\mathbf{g_3} = \mathbf{xz^2} - \mathbf{yz^2}$.

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

# How to predict zero reductions?

## Example

Let $I = \langle g_1, g_2 \rangle \in \mathbb{Q}[x, y, z]$ be given where $\mathbf{g_1 = xy - z^2}$, $\mathbf{g_2 = y^2 - z^2}$, and let $<$ be the graded reverse lexicographical ordering.

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

so it reduces w.r.t. $G$ to $\mathbf{g_3 = xz^2 - yz^2}$.

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

We can reduce even further with $z^2 g_2$:

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

# How to predict zero reductions?

**Example**

Let $I = \langle g_1, g_2 \rangle \in \mathbb{Q}[x, y, z]$ be given where $\mathbf{g_1} = \mathbf{xy} - \mathbf{z^2}$, $\mathbf{g_2} = \mathbf{y^2} - \mathbf{z^2}$, and let $<$ be the graded reverse lexicographical ordering.

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

so it reduces w.r.t. $G$ to $\mathbf{g_3} = \mathbf{xz^2} - \mathbf{yz^2}$.

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

We can reduce even further with $z^2 g_2$:

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

$\Rightarrow$ **How can we discard such zero reductions in advance?**

- The basic problem
- **Generic signature-based algorithms**
  - The basic idea
  - Generic signature-based Gröbner basis algorithm
  - Signature-based criteria
- Implementations and recent work
  - A good decade on signature-based algorithms
  - Implementation in Singular
- And what has really happened?
  - Ongoing work

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

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 $\pi : R^m \to R$ such that

$$\pi(e_i) = f_i \text{ for all } i.$$

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

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

1. Let $R^m$ be generated by $e_1, \dots, e_m$, $\prec$ a well-ordering on the monomials of $R^m$, and let $\pi : R^m \to R$ such that
$$\pi(e_i) = f_i \text{ for all } i.$$
2. Each $p \in I$ can be represented by an
$$s = \sum_{i=1}^{m} h_i e_i \in R^m \text{ such that } p = \pi(s).$$

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

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

1. Let $R^m$ be generated by $e_1, \dots, e_m$, $\prec$ a well-ordering on the monomials of $R^m$, and let $\pi : R^m \to R$ such that
$$\pi(e_i) = f_i \text{ for all } i.$$
2. Each $p \in I$ can be represented by an
$$s = \sum_{i=1}^{m} h_i e_i \in R^m \text{ such that } p = \pi(s).$$
3. **A signature** of $p$ is given by
$$\mathrm{sig}(p) = \mathrm{lm}_{\prec}(s) \text{ with } p = \pi(s).$$

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 $\pi : R^m \to R$ such that
$$\pi(e_i) = f_i \text{ for all } i.$$
2. Each $p \in I$ can be represented by an
$$s = \sum_{i=1}^{m} h_i e_i \in R^m \text{ such that } p = \pi(s).$$
3. **A signature** of $p$ is given by
$$\text{sig}(p) = \text{lm}_{\prec}(s) \text{ with } p = \pi(s).$$
4. **A minimal signature** of $p$ exists due to $\prec$.

# Our example – now with signatures and $\prec_{pot}$

We have already computed the following data:

$$\begin{aligned} g_1 &= xy - z^2,\ \operatorname{sig}(g_1) = e_1,\\ g_2 &= y^2 - z^2,\ \operatorname{sig}(g_2) = e_2,\\ g_3 &= \operatorname{spol}(g_2, g_1) = xg_2 - yg_1\\ \Rightarrow \operatorname{sig}(g_3) &= x\operatorname{sig}(g_2) = xe_2. \end{aligned}$$

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

We have already computed the following data:

$$\begin{aligned} g_1 &= xy - z^2,\ \operatorname{sig}(g_1) = e_1,\\ g_2 &= y^2 - z^2,\ \operatorname{sig}(g_2) = e_2,\\ g_3 &= \operatorname{spol}(g_2, g_1) = xg_2 - yg_1\\ \Rightarrow \operatorname{sig}(g_3) &= x \operatorname{sig}(g_2) = xe_2. \end{aligned}$$

$\operatorname{spol}(g_3, g_1) = yg_3 - z^2 g_1$:

$$\operatorname{sig}\left(\operatorname{spol}(g_3, g_1)\right) = y \operatorname{sig}(g_3) = xye_2.$$

# Our example – now with signatures and $\prec_{pot}$

We have already computed the following data:

$$\begin{aligned} g_1 &= xy - z^2,\ \mathrm{sig}(g_1) = e_1,\\ g_2 &= y^2 - z^2,\ \mathrm{sig}(g_2) = e_2,\\ g_3 &= \mathrm{spol}(g_2, g_1) = xg_2 - yg_1\\ \Rightarrow \mathrm{sig}(g_3) &= x\,\mathrm{sig}(g_2) = xe_2. \end{aligned}$$

$\mathrm{spol}(g_3, g_1) = yg_3 - z^2 g_1$:

$$\mathrm{sig}\left(\mathrm{spol}(g_3, g_1)\right) = y\,\mathrm{sig}(g_3) = xye_2.$$

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

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

We have already computed the following data:

$$g_1 = xy - z^2,\ \mathrm{sig}(g_1) = e_1,$$
$$g_2 = y^2 - z^2,\ \mathrm{sig}(g_2) = e_2,$$
$$g_3 = \mathrm{spol}(g_2, g_1) = xg_2 - yg_1$$
$$\Rightarrow \mathrm{sig}(g_3) = x\,\mathrm{sig}(g_2) = xe_2.$$

$\mathrm{spol}(g_3, g_1) = yg_3 - z^2 g_1$:

$$\mathrm{sig}\left(\mathrm{spol}(g_3, g_1)\right) = y\,\mathrm{sig}(g_3) = xye_2.$$

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

$\Rightarrow$ **We know that $\mathrm{spol}(g_3, g_1)$ will reduce to zero w.r.t. $G$.**

# Why do we know this?

The general idea is to check the signatures of the generated s-polynomials.

# Why do we know this?

The general idea is to check the signatures of the generated s-polynomials.

If $\text{sig}\left(\text{spol}(f,g)\right)$ is not minimal for $\text{spol}(f,g)$ then
$\Rightarrow \text{spol}(f,g)$ is discarded.

# Why do we know this?

The general idea is to check the signatures of the generated s-polynomials.

If $\operatorname{sig}\left(\operatorname{spol}(f,g)\right)$ is not minimal for $\operatorname{spol}(f,g)$ then
$\Rightarrow \operatorname{spol}(f,g)$ is discarded.

**Our goal**

Find and discard as many s-polynomials as possible for which the algorithm computes a non-minimal signature.

# Why do we know this?

The general idea is to check the signatures of the generated s-polynomials.

If $\text{sig}\left(\text{spol}(f, g)\right)$ is not minimal for $\text{spol}(f, g)$ then
$\Rightarrow \text{spol}(f, g)$ is discarded.

**Our goal**

Find and discard as many s-polynomials as possible for which the algorithm computes a non-minimal signature.

**Our task**

We need to take care of the correctness of the signatures throughout the computations.

# Generic signature-based Gröbner basis algorithm

**Input:** Ideal $I = \langle f_1, \dots, f_m \rangle$
**Output:** Gröbner Basis poly($G$) for $I$

1. $G \leftarrow \emptyset$
2. $G \leftarrow G \cup \{(e_i, f_i)\}$ for all $i \in \{1, \dots, m\}$
3. $P \leftarrow \{(g_i, g_j) \mid g_i, g_j \in G, i > j\}$

# Generic signature-based Gröbner basis algorithm

**Input:** Ideal $I = \langle f_1, \dots, f_m \rangle$
**Output:** Gröbner Basis $\text{poly}(G)$ for $I$

1. $G \leftarrow \emptyset$
2. $G \leftarrow G \cup \{(e_i, f_i)\}$ for all $i \in \{1, \dots, m\}$
3. $P \leftarrow \{(g_i, g_j) \mid g_i, g_j \in G, i > j\}$
4. While $P \neq \emptyset$
   (a) Choose $(f, g) \in P$ such that $\text{sig}(\text{spol}(f, g))$ minimal,
   $P \leftarrow P \setminus \{(f, g)\}$
   (b) If $\text{sig}(\text{spol}(f, g))$ minimal for $\text{spol}(f, g)$:

# Generic signature-based Gröbner basis algorithm

**Input:** Ideal $I = \langle f_1, \ldots, f_m \rangle$
**Output:** Gröbner Basis $\mathrm{poly}(G)$ for $I$

1. $G \leftarrow \emptyset$
2. $G \leftarrow G \cup \{(e_i, f_i)\}$ for all $i \in \{1, \ldots, m\}$
3. $P \leftarrow \{(g_i, g_j) \mid g_i, g_j \in G, i > j\}$
4. While $P \neq \emptyset$
   - (a) Choose $(f, g) \in P$ such that $\mathrm{sig}\left(\mathrm{spol}(f, g)\right)$ minimal, $P \leftarrow P \setminus \{(f, g)\}$
   - (b) If $\mathrm{sig}\left(\mathrm{spol}(f, g)\right)$ minimal for $\mathrm{spol}(f, g)$:
     - (i) $h \leftarrow \mathrm{spol}(f, g)$
     - (ii) If $\mathrm{poly}(h) \xrightarrow{G} 0$

# Generic signature-based Gröbner basis algorithm

**Input:** Ideal $I = \langle f_1, \ldots, f_m \rangle$
**Output:** Gröbner Basis $\text{poly}(G)$ for $I$

1. $G \leftarrow \emptyset$
2. $G \leftarrow G \cup \{(e_i, f_i)\}$ for all $i \in \{1, \ldots, m\}$
3. $P \leftarrow \{(g_i, g_j) \mid g_i, g_j \in G, i > j\}$
4. While $P \neq \emptyset$
   (a) Choose $(f, g) \in P$ such that $\text{sig}(\text{spol}(f, g))$ minimal,
   $P \leftarrow P \setminus \{(f, g)\}$
   (b) If $\text{sig}(\text{spol}(f, g))$ minimal for $\text{spol}(f, g)$:
      (i) $h \leftarrow \text{spol}(f, g)$
      (ii) If $\text{poly}(h) \xrightarrow{G} 0$
      (iii) If $\text{poly}(h) \xrightarrow{G} \text{poly}(r) \neq 0$

      $P \leftarrow P \cup \{(r, g) \mid g \in G\}$
      $G \leftarrow G \cup \{r\}$
5. Return $\text{poly}(G)$.

# Generic signature-based Gröbner basis algorithm

**Input:** Ideal $I = \langle f_1, \ldots, f_m \rangle$
**Output:** Gröbner Basis $\text{poly}(G)$ for $I$

1. $G \leftarrow \emptyset$
2. $G \leftarrow G \cup \{(e_i, f_i)\}$ for all $i \in \{1, \ldots, m\}$
3. $P \leftarrow \{(g_i, g_j) \mid g_i, g_j \in G, i > j\}$
4. While $P \neq \emptyset$
   (a) Choose $(f, g) \in P$ such that $\text{sig}\,(\text{spol}(f, g))$ minimal,
   $P \leftarrow P \setminus \{(f, g)\}$
   (b) If $\text{sig}\,(\text{spol}(f, g))$ minimal for $\text{spol}(f, g)$:
      (i) $h \leftarrow \text{spol}(f, g)$
      (ii) If $\text{poly}(h) \xrightarrow{G} 0 \Leftarrow$ **signature-safe**
      (iii) If $\text{poly}(h) \xrightarrow{G} \text{poly}(r) \neq 0 \Leftarrow$ **signature-safe**
      & $\nexists g \in G$ such that $m\,\text{sig}(g) = \text{sig}(r)$ and
      $m\,\text{lm}(\text{poly}(g)) = \text{lm}(\text{poly}(r))$
      $P \leftarrow P \cup \{(r, g) \mid g \in G\}$
      $G \leftarrow G \cup \{r\}$
5. Return $\text{poly}(G)$.

# Signature-safe reductions

Let $p$ and $q$ in $R$ be given such that $m \operatorname{lm}(q) = \operatorname{lm}(p)$, $c = \frac{\operatorname{lc}(p)}{\operatorname{lc}(q)}$.
Assume

$$p - cmq.$$

# Signature-safe reductions

Let $p$ and $q$ in $R$ be given such that $m\,\mathrm{lm}(q) = \mathrm{lm}(p)$, $c = \frac{\mathrm{lc}(p)}{\mathrm{lc}(q)}$.
Assume

$$p - cmq.$$

**signature-safe:** $\mathrm{sig}(p - cmq) \quad = \quad \mathrm{sig}(p)$

# Signature-safe reductions

Let $p$ and $q$ in $R$ be given such that $m\,\mathrm{lm}(q) = \mathrm{lm}(p)$, $c = \frac{\mathrm{lc}(p)}{\mathrm{lc}(q)}$.
Assume

$$p - cmq.$$

**signature-safe:** $\mathrm{sig}(p - cmq) \quad = \quad \mathrm{sig}(p)$

**signature-increasing:** $\mathrm{sig}(p - cmq) \quad = \quad m\,\mathrm{sig}(q)$

# Signature-safe reductions

Let $p$ and $q$ in $R$ be given such that $m\,\mathrm{lm}(q) = \mathrm{lm}(p)$, $c = \frac{\mathrm{lc}(p)}{\mathrm{lc}(q)}$.
Assume

$$p - cmq.$$

$$\begin{aligned}
\textbf{signature-safe:}\quad & \mathrm{sig}(p - cmq) &=& \quad \mathrm{sig}(p) \\
\textbf{signature-increasing:}\quad & \mathrm{sig}(p - cmq) &=& \quad m\,\mathrm{sig}(q) \\
\textbf{signature-decreasing:}\quad & \mathrm{sig}(p - cmq) &\prec& \quad \mathrm{sig}(p), m\,\mathrm{sig}(q)
\end{aligned}$$

**Termination**

- If $\text{sig}(r) = m\,\text{sig}(g)$ and $\text{lm}\,(\text{poly}(r)) = m\,\text{lm}\,(\text{poly}(g))$ is not added to $G$.
- Each new element in $G$ enlarges $\langle(\text{sig}(r), \text{lm}(\text{poly}(r)))\rangle$.

# How does this work?

**Termination**

- If $\text{sig}(r) = m\,\text{sig}(g)$ and $\text{lm}\,(\text{poly}(r)) = m\,\text{lm}\,(\text{poly}(g))$ is not added to $G$.
- Each new element in $G$ enlarges $\langle(\text{sig}(r), \text{lm}(\text{poly}(r)))\rangle$.

**Correctness**

- All possible s-polynomials are taken care of: signature-increasing reduction $\Rightarrow$ new pair in the next step.
- All elements $r$ with $\text{poly}(r) \neq 0$ are added to $G$ besides those fulfilling $\text{sig}(r) = m\,\text{sig}(g)$ and $\text{lm}\,(\text{poly}(r)) = m\,\text{lm}\,(\text{poly}(g))$.

**Non-minimal signature ( NM )**

$\mathrm{sig}(h)$ not minimal for $h$? $\Rightarrow$ Remove $h$.

## Non-minimal signature ( NM )

$\operatorname{sig}(h)$ not minimal for $h$? $\Rightarrow$ Remove $h$.

### Sketch of proof

1. There exists a syzygy $s \in R^m$ such that $\operatorname{lm}(s) = \operatorname{sig}(h)$.
   $\Rightarrow$ We can represent $h$ with a lower signature.
2. Pairs are handled by increasing signatures.
   $\Rightarrow$ All relations of lower signature are already taken care of.

□

**Non-minimal signature ( NM )**

sig($h$) not minimal for $h$? $\Rightarrow$ Remove $h$.

### Sketch of proof

1. There exists a syzygy $s \in R^m$ such that $\mathrm{lm}(s) = \mathrm{sig}(h)$.
   $\Rightarrow$ We can represent $h$ with a lower signature.
2. Pairs are handled by increasing signatures.
   $\Rightarrow$ All relations of lower signature are already taken care of.

□

### Our example with $\prec_{\mathrm{pot}}$ revisited

$\mathrm{sig}\left(\mathrm{spol}(g_3, g_1)\right) = xye_2$

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

**Rewritable signature ( RW )**

$\mathrm{sig}(g) = \mathrm{sig}(h)$? $\Rightarrow$ Remove either $g$ or $h$.

**Rewritable signature ( RW )**

$\text{sig}(g) = \text{sig}(h)? \Rightarrow$ Remove either $g$ or $h$.

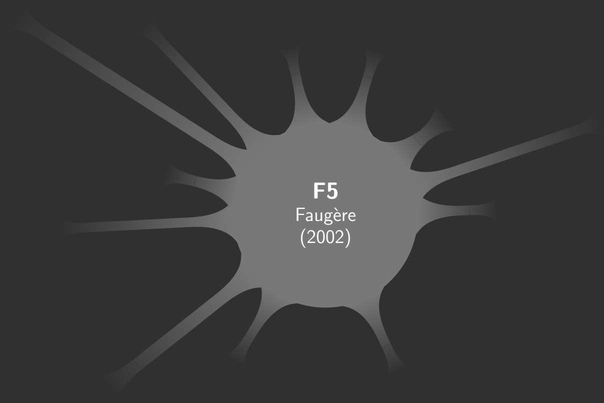
### Sketch of proof

1. $\text{sig}(g - h) \prec \text{sig}(g), \text{sig}(h)$.
2. Pairs are handled by increasing signatures.
   $\Rightarrow$ All necessary computations of lower signature have already taken place.
   $\Rightarrow$ We can represent $h$ by

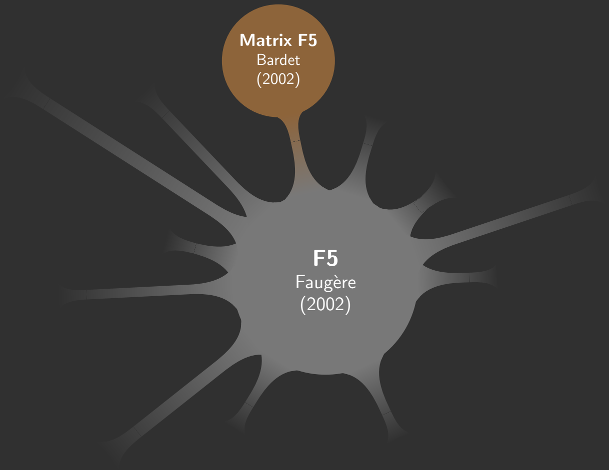
$$h = g + \text{ elements of lower signature.}$$

□

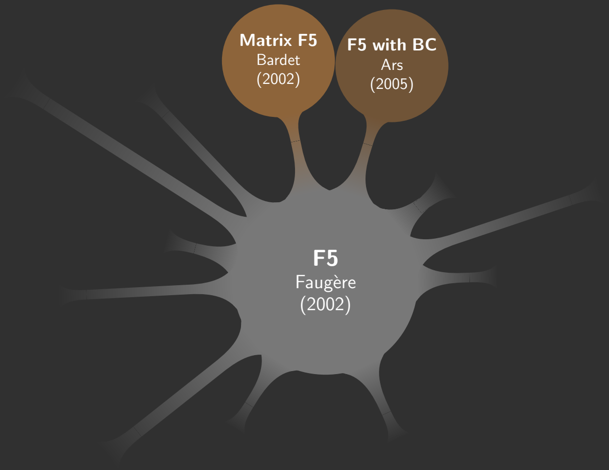
# A good decade on signature-based algorithms



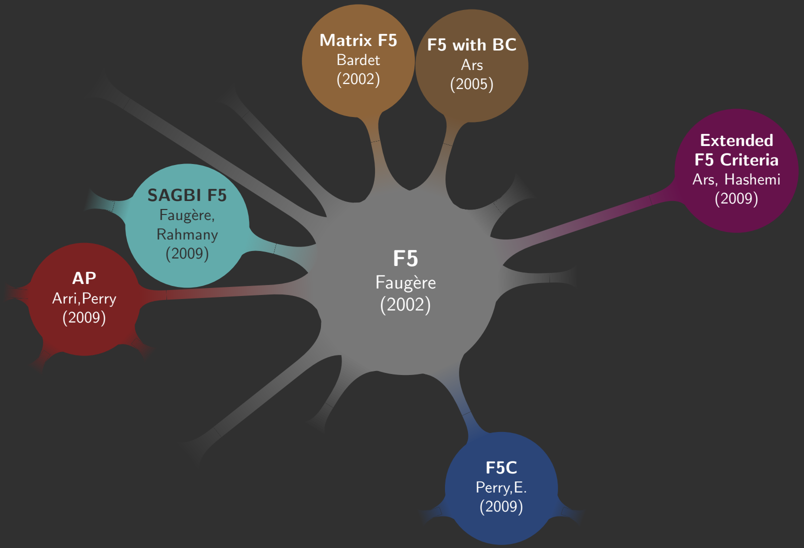
# A good decade on signature-based algorithms



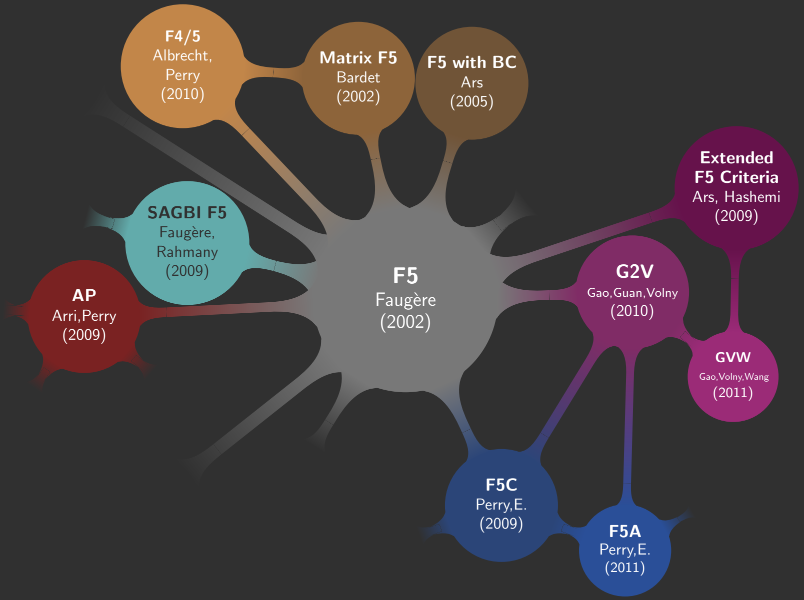
# A good decade on signature-based algorithms



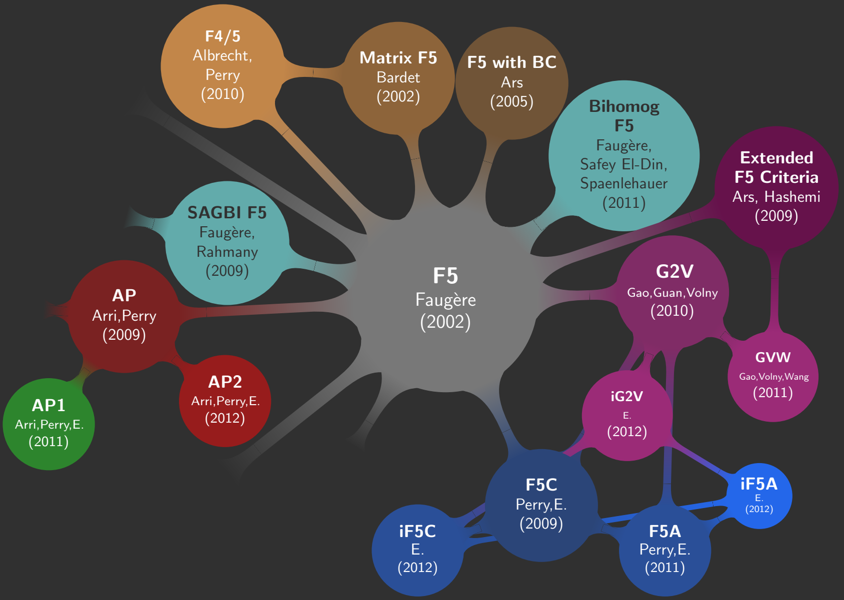
# A good decade on signature-based algorithms



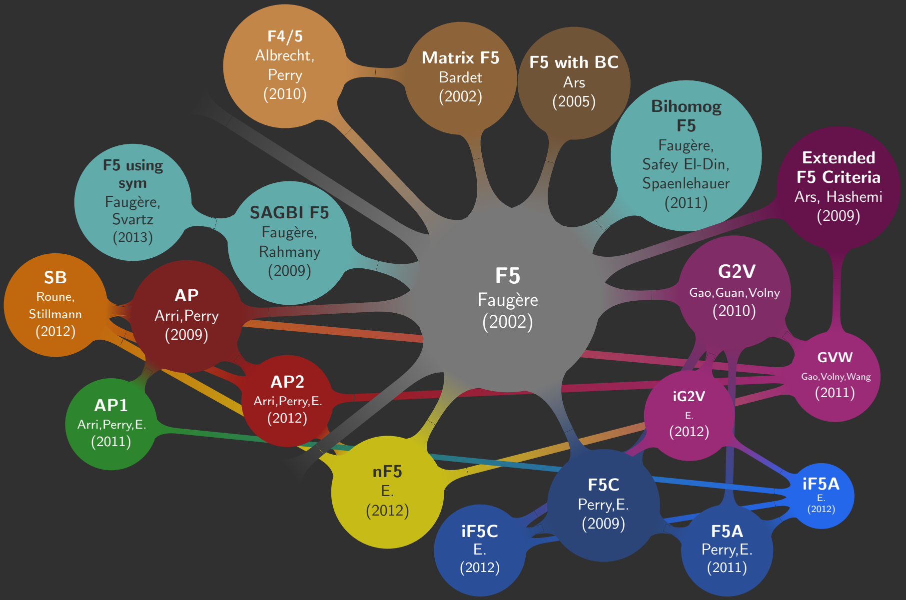
# A good decade on signature-based algorithms



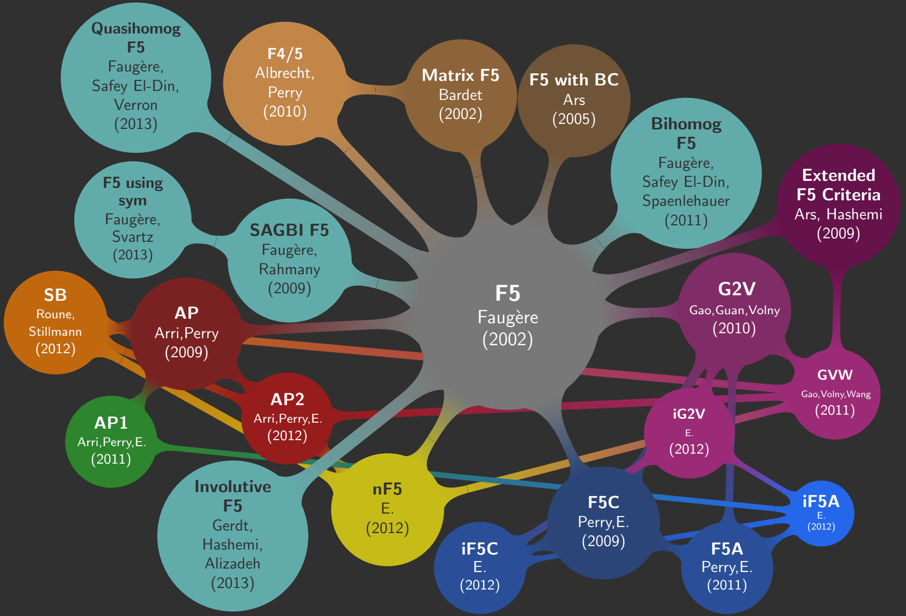
# A good decade on signature-based algorithms



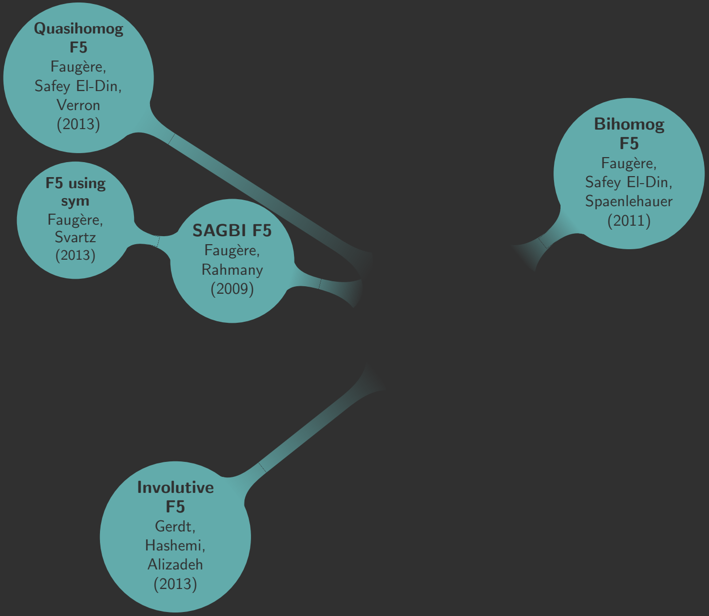
# A good decade on signature-based algorithms



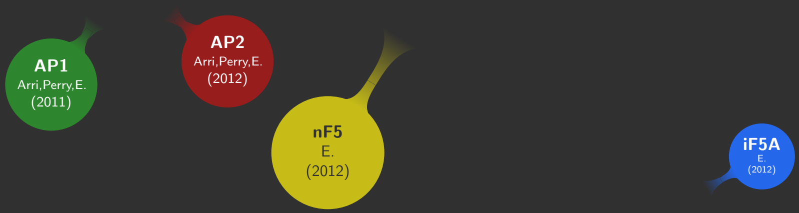
# A good decade on signature-based algorithms



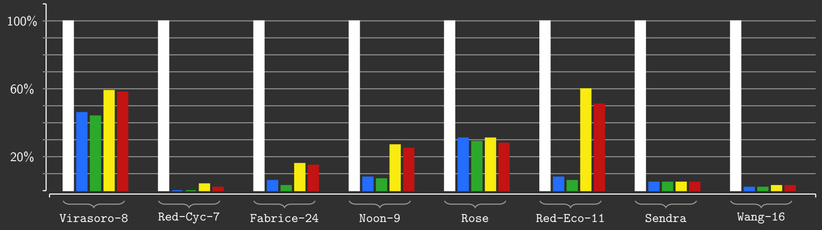
# A good decade on signature-based algorithms



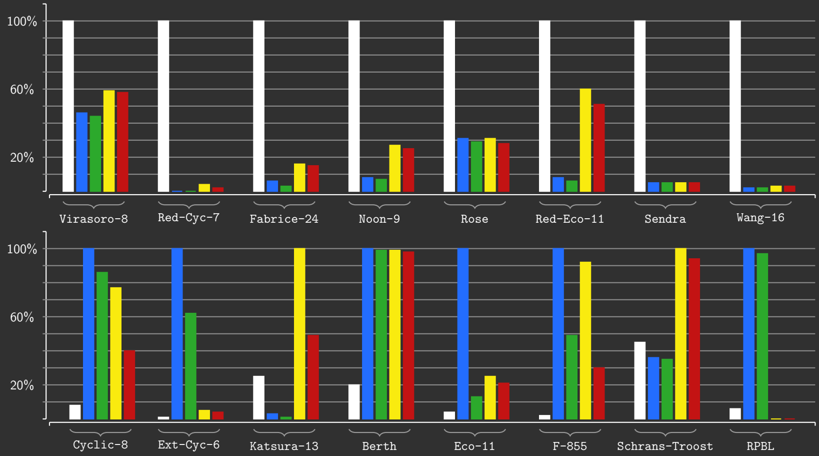
# Implemented in Singular



# Implementation in Singular



# Implementation in Singular



# And what has really happened?

**Rather boring**

- We have (hopefully) understood the criteria.
- We have proven termination of F5 et al.
- We have implemented signature-based Buchberger-style Gröbner basis algorithms quite a lot.

# And what has really happened?

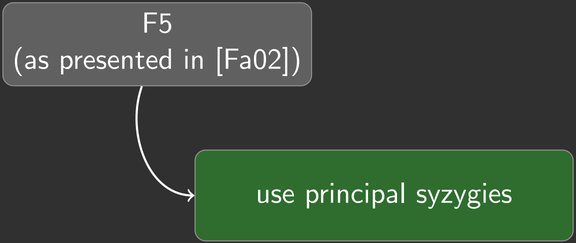
**Rather boring**

- We have (hopefully) understood the criteria.
- We have proven termination of F5 et al.
- We have implemented signature-based Buchberger-style Gröbner basis algorithms quite a lot.

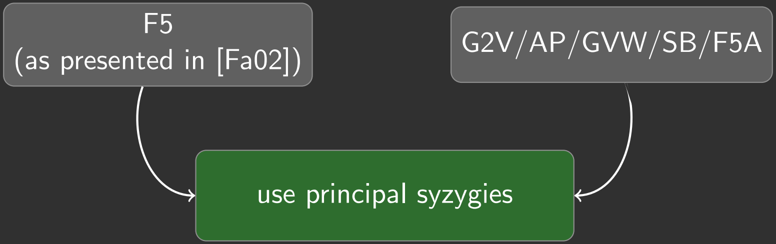
**At least some new ideas**

- We use different module monomial orderings on the signatures to allow non-incremental computations.
- We have improved the incremental variants a bit (reduced intermediate bases)
- There are some slight improvements on the signature-based criteria.

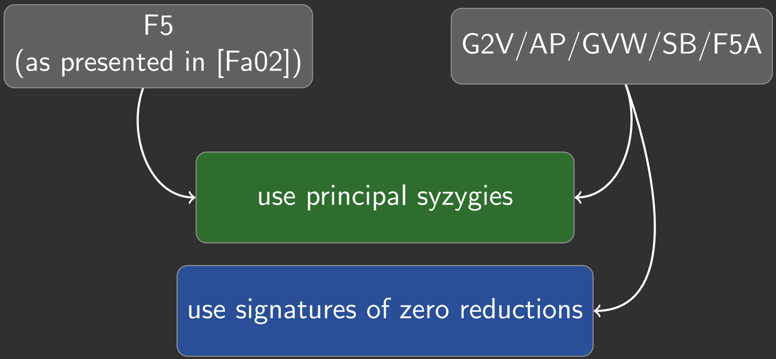
# Improving the non-minimal signature criterion



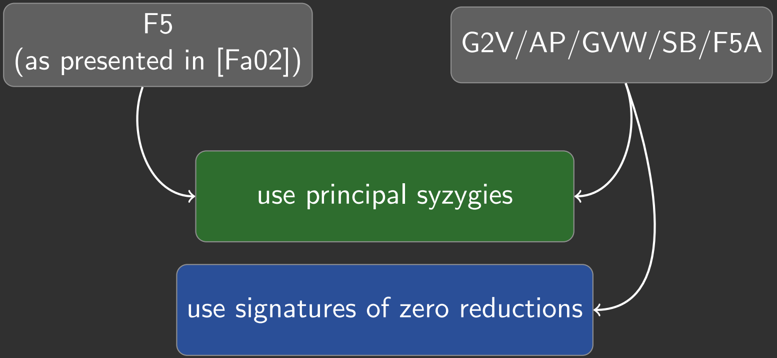
# Improving the non-minimal signature criterion



# Improving the non-minimal signature criterion



# Improving the non-minimal signature criterion




**Remark**

This helps only if the input sequence is not regular.

# Improving the rewritable signature criterion

F5
(as presented in [Fa02])

Fix a total ordering $\lhd$ on $G$.

---

A basis element $g \in G$ is a rewriter in signature $T$ if $\text{sig}(g) \mid T$.

---

The $\lhd$-maximal rewriter in $T$ is the canonical rewriter.

---

An element $mg$ is rewritable if $g$ is not the canonical rewriter in $\text{sig}(mg)$.

# Improving the rewritable signature criterion

| F5 (as presented in [Fa02]) | AP/GVW/SB |
| --- | --- |
| Fix a total ordering $\lhd$ on $G$. | For any signature $T$ define $M_T = \{mg \mid g \in G, \mathrm{sig}(mg) = T\}$ |
| A basis element $g \in G$ is a rewriter in signature $T$ if $\mathrm{sig}(g) \mid T$. | Choose $mg$ such that $m \,\mathrm{lm}\,(\mathrm{poly}(g))$ is minimal. |
| The $\lhd$-maximal rewriter in $T$ is the canonical rewriter. | Compute the correspon-ding $s$-polynomial with $mg$. |
| An element $mg$ is rewritable if $g$ is not the canonical rewriter in $\mathrm{sig}(mg)$. | |

# Improving the rewritable signature criterion

**F5 (as presented in [Fa02])**

Fix a total ordering $\lhd$ on $G$.

A basis element $g \in G$ is a rewriter in signature $T$ if $\mathrm{sig}(g) \mid T$.

The $\lhd$-maximal rewriter in $T$ is the canonical rewriter.

An element $mg$ is rewritable if $g$ is not the canonical rewriter in $\mathrm{sig}(mg)$.

**AP/GVW/SB**

For any signature $T$ define $M_T = \{mg \mid g \in G, \mathrm{sig}(mg) = T\}$

Choose $mg$ such that $m \operatorname{lm}(\mathrm{poly}(g))$ is minimal.

Compute the corresponding $s$-polynomial with $mg$.

**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

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

# 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

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

| $g_i \in G$ | reduced from | $\operatorname{lm}(\operatorname{poly}(g_i))$ | $\operatorname{sig}(g_i)$ |
|---|---|---|---|
| $g_1$ | $\mathbf{e}_1$ | $y^3$ | $\mathbf{e}_1$ |
| $g_2$ | $\mathbf{e}_2$ | $xyz$ | $\mathbf{e}_2$ |
| $g_3$ | $y^2g_2 - xzg_1 = \operatorname{spol}(g_2, g_1)$ | $x^3z^2$ | $y^2\mathbf{e}_2$ |
| $g_4$ | $\mathbf{e}_3$ | $yz^2$ | $\mathbf{e}_3$ |
| $g_5$ | $xg_3 - zg_2 = \operatorname{spol}(g_3, g_2)$ | $xz^3$ | $x\mathbf{e}_3$ |
| $g_6$ | $y^2g_3 - z^2g_1 = \operatorname{spol}(g_3, g_1)$ | $x^2z^3$ | $y^2\mathbf{e}_3$ |
| $g_7$ | $yg_5 - z^2g_2 = \operatorname{spol}(g_5, g_2)$ | $x^2y^2t$ | $xy\mathbf{e}_3$ |
| $g_8$ | $xg_5 - g_6 = \operatorname{spol}(g_5, g_6)$ | $z^5$ | $x^2\mathbf{e}_3$ |
| $g_9$ | $xg_6 - zg_3 = \operatorname{spol}(g_6, g_3)$ | $x^4zt$ | $xy^2\mathbf{e}_3$ |
| $g_{10}$ | $yg_8 - z^3g_4 = \operatorname{spol}(g_8, g_4)$ | $x^3y^2t$ | $x^2y\mathbf{e}_3$ |
| $g_{11}$ | $x^3g_4 - yg_3 = \operatorname{spol}(g_4, g_3)$ | $x^4yt$ | $x^3\mathbf{e}_3$ |
| $g_{12}$ | $zg_{11} - x^3g_2 = \operatorname{spol}(g_{11}, g_2)$ | $x^3zt^3$ | $x^3z\mathbf{e}_3$ |
| $g_{13}$ | $yg_{10} - x^3g_1 = \operatorname{spol}(g_{10}, g_1)$ | $x^5zt$ | $x^2y^2\mathbf{e}_3$ |
| $g_{14}$ | $xg_{12} - g_9 = \operatorname{spol}(g_{12}, g_9)$ | $x^4t^4$ | $x^4z\mathbf{e}_3$ |

# 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

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

| $g_i \in G$ | reduced from | $\text{lm}(\text{poly}(g_i))$ | $\text{sig}(g_i)$ |
|---|---|---|---|
| $g_1$ | $\mathbf{e}_1$ | $y^3$ | $\mathbf{e}_1$ |
| $g_2$ | $\mathbf{e}_2$ | $xyz$ | $\mathbf{e}_2$ |
| $g_3$ | $y^2g_2 - xzg_1 = \text{spol}(g_2, g_1)$ | $x^3z^2$ | $y^2\mathbf{e}_2$ |
| $g_4$ | $\mathbf{e}_3$ | $yz^2$ | $\mathbf{e}_3$ |
| $g_5$ | $xg_3 - zg_2 = \text{spol}(g_3, g_2)$ | $xz^3$ | $x\mathbf{e}_3$ |
| $g_6$ | $y^2g_3 - z^2g_1 = \text{spol}(g_3, g_1)$ | $x^2z^3$ | $y^2\mathbf{e}_3$ |
| $g_7$ | $yg_5 - z^2g_2 = \text{spol}(g_5, g_2)$ | $x^2y^2t$ | $xy\mathbf{e}_3$ |
| $g_8$ | $xg_5 - g_6 = \text{spol}(g_5, g_6)$ | $z^5$ | $x^2\mathbf{e}_3$ |
| $g_9$ | $xg_6 - zg_3 = \text{spol}(g_6, g_3)$ | $x^4zt$ | $xy^2\mathbf{e}_3$ |
| $g_{10}$ | $yg_8 - z^3g_4 = \text{spol}(g_8, g_4)$ | $x^3y^2t$ | $x^2y\mathbf{e}_3$ |
| $g_{11}$ | $x^3g_4 - yg_3 = \text{spol}(g_4, g_3)$ | $x^4yt$ | $x^3\mathbf{e}_3$ |
| $g_{12}$ | $zg_{11} - x^3g_2 = \text{spol}(g_{11}, g_2)$ | $x^3zt^3$ | $x^3z\mathbf{e}_3$ |
| $g_{13}$ | $yg_{10} - x^3g_1 = \text{spol}(g_{10}, g_1)$ | $x^5zt$ | $x^2y^2\mathbf{e}_3$ |
| $g_{14}$ | $xg_{12} - g_9 = \text{spol}(g_{12}, g_9)$ | $x^4t^4$ | $x^4z\mathbf{e}_3$ |

# Why am I here?

- **F4:**
  linear algebra for reduction purposes
- **Heuristics:**
  orderings on signatures; orderings for critical pairs (sugar degree), reducers
- **Parallelisation:**
  modular methods, parallel criteria checks
- **Computation of syzygies:**
  implementation
- **Generalization of signature-based criteria:**
  more terms per signature, relaxing criteria for combination with Buchberger's criteria

# Bibliography


[AP10] M. Albrecht und J. Perry. F4/5

[A05] G. Ars. Applications des bases de Groeobner a la cryptographie

[AH09] G. Ars und A. Hashemi. Extended F5 Criteria

[AP11] A. Arri und J. Perry. The F5 Criterion revised

[E12a] C. Eder. Improving incremental signature-based Gröbner bases algorithms

[E12b] C. Eder. Sweetening the sour taste of inhomogeneous signature-based Gröbner basis computations

[EGP11] C. Eder, J. Gash and J. Perry. Modifying Faugère's F5 Algorithm to ensure termination

[EP10] C. Eder and J. Perry. F5C: A variant of Faugère's F5 Algorithm with reduced Gröbner bases

[EP11] C. Eder and J. Perry. Signature-based algorithms to compute Gröbner bases

[ER13] C. Eder and B. H. Roune. Signature Rewriting in Gröbner Basis Computation

[Fa02] J.-C. Faugère. A new efficient algorithm for computing Gröbner bases without reduction to zero $F_5$

[FR09] J.-C. Faugère and S. Rahmany. Solving systems of polynomial equations with symmetries using SAGBI-Gröbner bases

[FSS11] J.-C. Faugère, M. Safey El-Din and P.-J. Spaenlehauer. Gröbner Bases of Bihomogeneous Ideals Generated by Polynomials of Bidegree (1,1)

[FSV13] J.-C. Faugère, M. Safey El-Din and T. Verron. Computing Gröbner bases for quasi-homogeneous systems

[FS12] J.-C. Faugère and J. Svartz. Solving Polynomial Systems Globally Invariant Under an Action of the Symmetric Group and Application to the Equilibria of N vortices in the Plane

[Ga12a] V. Galkin. Termination of original $F_5$

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

[GGV10] S. Gao, Y. Guan and F. Volny IV. A New Incremental Algorithm for Computing Gröbner Bases

[GHA13] V. Gerdt, A. Hashemi and B. M.-Alizadeh. Involutive Bases Algorithm Incorporating F5 Criterion

[GVW11] S. Gao, F. Volny IV and M. Wang. A New Algorithm For Computing Grobner Bases

[MSWZ12] X. Ma, Y. Sun, D. Wang, and Y. Zhang. A Signature-Based Algorithm for Computing Groebner Bases in Solvable Polynomial Algebras

[PHW13] S. Pan, Y. Hu and B. Wang. The Termination of Algorithms for Computing Gröbner Bases

[RS12] B. H. Roune and M. Stillman. Practical Gröbner Basis Computation

[SW10] Y. Sun und D. Wang. A new proof of the F5 Algorithm

[SW11] Y. Sun and D. Wang. A Generalized Criterion for Signature Related Gröbner Basis Algorithms