SIGNATURE GRÖBNER BASES

Clemens Hofstadler
Institute for Algebra, JKU Linz

Seminar Algebra and Discrete Mathematics
14 October 2021

JOHANNES KEPLER UNIVERSITY LINZ

FWF
Der Wissenschaftsfonds.

Introduction

Today

- Introduction to the topic
- Commutative signature Gröbner bases over fields
- Based on [1], [2] (content), [3] (notation)

Introduction

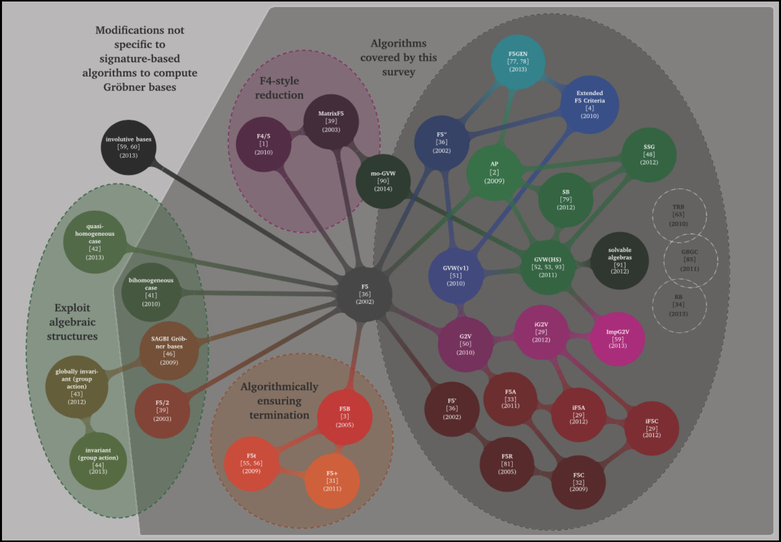

Modifications not specific to signature-based algorithms to compute Gröbner bases
involutive bases [59, 60] (2013)
F4-style reduction
F4/5 [1] (2010)
MatrixF5 [39] (2003)
mo-GVW [90] (2014)
Algorithms covered by this survey
F5GEN [77, 78] (2013)
Extended F5 Criteria [4] (2010)
F5" [36] (2002)
AP [2] (2009)
SSG [48] (2012)
SB [79] (2012)
TRB [63] (2010)
GBGC [85] (2011)
RB [34] (2013)
GVW(v1) [51] (2010)
GVW(HS) [52, 53, 93] (2011)
solvable algebras [91] (2012)
F5 [36] (2002)
G2V [50] (2010)
iG2V [29] (2012)
ImpG2V [59] (2013)
F5' [36] (2002)
F5A [33] (2011)
iF5A [29] (2012)
iF5C [29] (2012)
F5R [81] (2005)
F5C [32] (2009)
Exploit algebraic structures
quasi-homogeneous case [42] (2013)
bihomogeneous case [41] (2010)
SAGBI Gröbner bases [46] (2009)
globally invariant (group action) [43] (2012)
F5/2 [39] (2003)
invariant (group action) [44] (2013)
Algorithmically ensuring termination
F5B [3] (2005)
F5t [55, 56] (2009)
F5+ [31] (2011)

Image taken from [1]

Introduction

Today

- Introduction to the topic
- Commutative signature Gröbner bases over fields
- Based on [1], [2] (content), [3] (notation)

Introduction

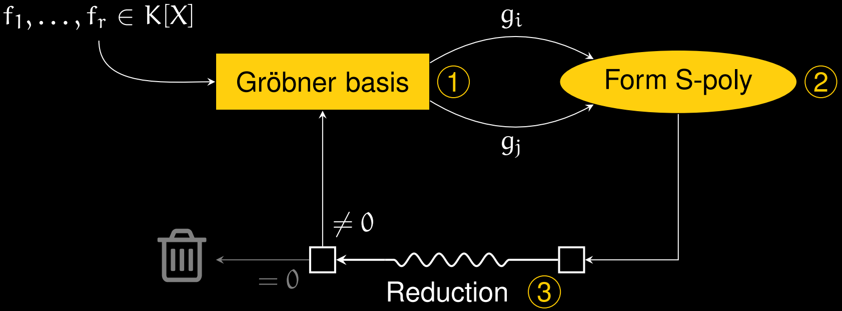
Today

- Introduction to the topic
- Commutative signature Gröbner bases over fields
- Based on [1], [2] (content), [3] (notation)

Next week (Thibaut)

- Recent developments
- Commutative signature Gröbner bases over rings
- Noncommutative signature Gröbner bases over fields

Recap: Buchberger’s algorithm



$f_1, \dots, f_r \in K[X]$

Gröbner basis ①

g_i

g_j

Form S-poly ②

$\neq 0$

$= 0$

Reduction ③

1. Selection: different strategies
2. Construction: S-polynomial: $\mathrm{spol}(g_i, g_j) = \frac{\overset{\mathrm{lcm}(\mathrm{lm}(g_i),\mathrm{lm}(g_j))}{\boxed{M}}}{\mathrm{lt}(g_i)} g_i - \frac{M}{\mathrm{lt}(g_j)} g_j$
3. Reduction: if $m\,\mathrm{lm}(g) \in \mathrm{supp}(f)$, then $f \to f - cmg$

Recap: Buchberger's algorithm

$G = \{g_1, g_2, g_3\} \subseteq \mathbb{Q}[x, y, z]$, with

$g_1 = y^2 - x$ $\qquad$ $g_2 = yz + y$ $\qquad$ $g_3 = xz - y^2$

$$\mathrm{spol}(g_2, g_3) = y^3 - xy$$

Recap: Buchberger's algorithm

$G = \{g_1, g_2, g_3\} \subseteq \mathbb{Q}[x, y, z]$, with

$g_1 = y^2 - x$ $\qquad$ $g_2 = yz + y$ $\qquad$ $g_3 = xz - y^2$

$$\mathrm{spol}(g_2, g_3) = y^3 - xy \quad \xrightarrow{*}_G \quad 0$$

Recap: Buchberger’s algorithm

$G = \{g_1, g_2, g_3\} \subseteq \mathbb{Q}[x, y, z]$, with

$$g_1 = y^2 - x \qquad g_2 = yz + y \qquad g_3 = xz - y^2$$

$$\mathrm{spol}(g_2, g_3) = y^3 - xy \quad \xcancel{\xrightarrow{*}_G \quad 0}$$

Recap: Buchberger's algorithm

$G = \{g_1, g_2, g_3\} \subseteq \mathbb{Q}[x, y, z]$, with

$$g_1 = y^2 - x \qquad g_2 = yz + y \qquad g_3 = xz - y^2$$

$$\operatorname{spol}(g_2, g_3) = y^3 - xy \quad \xcancel{\xrightarrow{*}_G \; 0}$$

Goal Detect such useless computations!

Recap: Buchberger’s algorithm

$G = \{g_1, g_2, g_3\} \subseteq \mathbb{Q}[x, y, z]$, with

$$g_1 = y^2 - x \qquad g_2 = yz + y \qquad g_3 = xz - y^2$$

$$\mathrm{spol}(g_2, g_3) = y^3 - xy \; \xcancel{\xrightarrow{*}_G \; 0}$$

Goal Detect such useless computations!

Idea Add additional information to the polynomials

Recap: Buchberger's algorithm

$G = \{g_1, g_2, g_3\} \subseteq \mathbb{Q}[x, y, z]$, with

$$g_1 = y^2 - x \qquad g_2 = yz + y \qquad g_3 = xz - y^2$$

$$\mathrm{spol}(g_2, g_3) = y^3 - xy \quad \xcancel{\xrightarrow{*}_G \; 0}$$

Goal Detect such useless computations!

Idea Add additional information to the polynomials

This information has to be expressive and lightweight.

Recap: Buchberger's algorithm

$G = \{g_1, g_2, g_3\} \subseteq \mathbb{Q}[x, y, z]$, with

$g_1 = y^2 - x \qquad g_2 = y^2 + y \qquad g_3 = xz \quad y^2$

$$\text{spol}(g_2, g_3) = y^3 \quad xy \quad \cancel{\xrightarrow[G]{*} \; 0}$$

Goal Detect such useless computations!

Idea Add additional information to the polynomials

This information has to be expressive and lightweight.

Two worlds…

$K[X]$ polynomial ring

$$I = (f_1, \dots, f_r)$$

$$f = \sum_j c_j m_j f_{i_j}, \quad m_j \in [X]$$

Two worlds…

$\mathcal{F}_r$ free $K[X]$-module of rank r	$K[X]$ polynomial ring
$\varepsilon_1, \ldots, \varepsilon_r$	$I = (f_1, \ldots, f_r)$
$\alpha = \sum_j c_j m_j \varepsilon_{i_j}, \quad m_j \in [X]$	$f = \sum_j c_j m_j f_{i_j}, \quad m_j \in [X]$

Two worlds…

$\mathcal{F}_r$ free $K[X]$-module of rank r	$K[X]$ polynomial ring
$\varepsilon_1, \ldots, \varepsilon_r$	$I = (f_1, \ldots, f_r)$
$\alpha = \sum_j c_j m_j \varepsilon_{i_j}, \quad m_j \in [X]$	$f = \sum_j c_j m_j f_{i_j}, \quad m_j \in [X]$
$\preceq_{\mathcal{F}_r}$ module ordering	$\preceq$ monomial ordering

Two worlds…

$\mathcal{F}_r$ free $K[X]$-module of rank r	$K[X]$ polynomial ring
$\varepsilon_1, \ldots, \varepsilon_r$	$I = (f_1, \ldots, f_r)$
$\alpha = \sum_j c_j m_j \varepsilon_{i_j}, \quad m_j \in [X]$	$f = \sum_j c_j m_j f_{i_j}, \quad m_j \in [X]$
$\preceq_{\mathcal{F}_r}$ module ordering	$\preceq$ monomial ordering
$\mathrm{sig}(\alpha) = \max_{\preceq_{\mathcal{F}_r}} m_j \varepsilon_{i_j}$ signature	$\mathrm{lm}(f) = \max_{\preceq} \mathrm{supp}(f)$ leading monomial

. . . in one

Relate the two worlds via $K[X]$-module homomorphism

$$\bar{\cdot}\ : \mathcal{F}_r \to K[X], \quad \alpha = \sum_j c_j m_j \varepsilon_{i_j} \mapsto \overline{\alpha} \coloneqq \sum_j c_j m_j f_{i_j}$$

…in one

Relate the two worlds via $\mathbb{K}[X]$-module homomorphism

$$\bar{\cdot}\ : \mathcal{F}_r \to \mathbb{K}[X], \quad \alpha = \sum_j c_j m_j \varepsilon_{i_j} \mapsto \overline{\alpha} := \sum_j c_j m_j f_{i_j}$$

$$\mathrm{Syz}(f_1, \ldots, f_r) := \{\alpha \in \mathcal{F}_r \mid \overline{\alpha} = 0\}$$

... in one

Relate the two worlds via $K[X]$-module homomorphism

$$\bar{\cdot} : \mathcal{F}_r \to K[X], \quad \alpha = \sum_j c_j m_j \varepsilon_{i_j} \mapsto \overline{\alpha} := \sum_j c_j m_j f_{i_j}$$

Syzygy module

Syzygy

$$\boxed{\mathrm{Syz}(f_1, \dots, f_r)} := \{\boxed{\alpha} \in \mathcal{F}_r \mid \overline{\alpha} = 0\}$$

…in one

Relate the two worlds via $K[X]$-module homomorphism

$$\bar{\cdot} : \mathcal{F}_r \to K[X], \quad \alpha = \sum_j c_j m_j \varepsilon_{i_j} \mapsto \overline{\alpha} := \sum_j c_j m_j f_{i_j}$$

Syzygy module

Syzygy

$$\boxed{\mathrm{Syz}(f_1, \dots, f_r)} := \{\boxed{\alpha} \in \mathcal{F}_r \mid \overline{\alpha} = 0\}$$

$f^{[\alpha]} := (\alpha, f) \in \mathcal{F}_r \times I$ s.t. $f = \overline{\alpha}$

…in one

Relate the two worlds via $K[X]$-module homomorphism

$$\bar{\cdot} : \mathcal{F}_r \to K[X], \quad \alpha = \sum_j c_j m_j \varepsilon_{i_j} \mapsto \overline{\alpha} := \sum_j c_j m_j f_{i_j}$$

Syzygy module

Syzygy

$$\boxed{\mathrm{Syz}(f_1, \dots, f_r)} := \{\boxed{\alpha} \in \mathcal{F}_r \mid \overline{\alpha} = 0\}$$

Signature polynomial

$$\boxed{f^{[\alpha]}} := (\alpha, f) \in \mathcal{F}_r \times I \quad \text{s.t. } f = \overline{\alpha}$$

…in one

Relate the two worlds via $K[X]$-module homomorphism

$$\overline{\cdot} : \mathcal{F}_r \to K[X], \quad \alpha = \sum_j c_j m_j \varepsilon_{i_j} \mapsto \overline{\alpha} := \sum_j c_j m_j f_{i_j}$$

Syzygy module

Syzygy

$$\boxed{\mathrm{Syz}(f_1, \ldots, f_r)} := \{\boxed{\alpha} \in \mathcal{F}_r \mid \overline{\alpha} = 0\}$$

Signature polynomial

$$\boxed{f^{[\alpha]}} := (\alpha, f) \in \mathcal{F}_r \times I \quad \text{s.t. } f = \overline{\alpha}$$

$$I^{[\Sigma]} := \{f^{[\alpha]} \mid \alpha \in \mathcal{F}_r\} \subseteq \mathcal{F}_r \times I$$

. . . in one

Relate the two worlds via $K[X]$-module homomorphism

$$\bar{\cdot} : \mathcal{F}_r \to K[X], \quad \alpha = \sum_j c_j m_j \varepsilon_{i_j} \mapsto \overline{\alpha} := \sum_j c_j m_j f_{i_j}$$

Syzygy module

Syzygy

$$\boxed{\mathrm{Syz}(f_1, \ldots, f_r)} := \{\boxed{\alpha} \in \mathcal{F}_r \mid \overline{\alpha} = 0\}$$

Signature polynomial

$$\boxed{f^{[\alpha]}} := (\alpha, f) \in \mathcal{F}_r \times I \quad \text{s.t. } f = \overline{\alpha}$$

$$I^{[\Sigma]} := \{f^{[\alpha]} \mid \alpha \in \mathcal{F}_r\} \subseteq \mathcal{F}_r \times I$$

$I^{[\Sigma]}$ is a $K[X]$-module with

- $f^{[\alpha]} + g^{[\beta]} = (f + g)^{[\alpha+\beta]}$
- $cm \cdot f^{[\alpha]} = (cmf)^{[cm\alpha]}$

Some remarks

- We require $\preceq$ and $\preceq_{\mathcal{F}_r}$ to be compatible, that is

$$a \preceq b \qquad \text{iff} \qquad a\varepsilon_i \preceq_{\mathcal{F}_r} b\varepsilon_i.$$

- Denote $\preceq_{\mathcal{F}_r}$ by $\preceq$ (Greek letters $\rightsquigarrow \preceq_{\mathcal{F}_r}$, Latin letters $\rightsquigarrow \preceq$)

Some remarks

- We require $\preceq$ and $\preceq_{\mathcal{F}_r}$ to be compatible, that is

$$a \preceq b \qquad \text{iff} \qquad a\varepsilon_i \preceq_{\mathcal{F}_r} b\varepsilon_i.$$

- Denote $\preceq_{\mathcal{F}_r}$ by $\preceq$ (Greek letters $\rightsquigarrow \preceq_{\mathcal{F}_r}$, Latin letters $\rightsquigarrow \preceq$)

- $I^{[\Sigma]}$ (and everything from now on!) depends on $f_1, \ldots, f_r$

Some remarks

- We require $\preceq$ and $\preceq_{\mathcal{F}_r}$ to be compatible, that is

$$a \preceq b \qquad \text{iff} \qquad a\varepsilon_i \preceq_{\mathcal{F}_r} b\varepsilon_i.$$

- Denote $\preceq_{\mathcal{F}_r}$ by $\preceq$ (Greek letters $\rightsquigarrow \preceq_{\mathcal{F}_r}$, Latin letters $\rightsquigarrow \preceq$)
- $I^{[\Sigma]}$ (and everything from now on!) depends on $f_1, \ldots, f_r$
- Recall: “*Additional information has to be lightweight*”

Some remarks

- We require $\preceq$ and $\preceq_{\mathcal{F}_r}$ to be compatible, that is

$$a \preceq b \qquad \text{iff} \qquad a\varepsilon_i \preceq_{\mathcal{F}_r} b\varepsilon_i.$$

- Denote $\preceq_{\mathcal{F}_r}$ by $\preceq$ (Greek letters $\rightsquigarrow \preceq_{\mathcal{F}_r}$, Latin letters $\rightsquigarrow \preceq$)
- $I^{[\Sigma]}$ (and everything from now on!) depends on $f_1, \ldots, f_r$
- Recall: “*Additional information has to be lightweight*”

$f^{[\alpha]} = f$

Some remarks

- We require $\preceq$ and $\preceq_{\mathcal{F}_r}$ to be compatible, that is

$$a \preceq b \qquad \text{iff} \qquad a\varepsilon_i \preceq_{\mathcal{F}_r} b\varepsilon_i.$$

- Denote $\preceq_{\mathcal{F}_r}$ by $\preceq$ (Greek letters $\rightsquigarrow$ $\preceq_{\mathcal{F}_r}$, Latin letters $\rightsquigarrow$ $\preceq$)
- $I^{[\Sigma]}$ (and everything from now on!) depends on $f_1, \dots, f_r$
- Recall: "*Additional information has to be lightweight*"

$f^{[\alpha]} = f$ vs. $f^{(\mathrm{sig}(\alpha))} = f$

Some remarks

- We require $\preceq$ and $\preceq_{\mathcal{F}_r}$ to be compatible, that is

$$a \preceq b \qquad \text{iff} \qquad a\varepsilon_i \preceq_{\mathcal{F}_r} b\varepsilon_i.$$

- Denote $\preceq_{\mathcal{F}_r}$ by $\preceq$ (Greek letters $\rightsquigarrow \preceq_{\mathcal{F}_r}$, Latin letters $\rightsquigarrow \preceq$)
- $I^{[\Sigma]}$ (and everything from now on!) depends on $f_1, \ldots, f_r$
- Recall: "*Additional information has to be lightweight*"

$f^{[\alpha]} = f$

presentation

vs.

$f^{(\mathrm{sig}(\alpha))} = f$

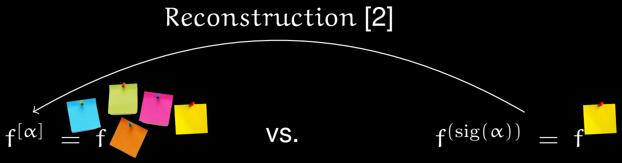
implementation

Some remarks

- We require $\preceq$ and $\preceq_{\mathcal{F}_r}$ to be compatible, that is

$$a \preceq b \qquad \text{iff} \qquad a\varepsilon_i \preceq_{\mathcal{F}_r} b\varepsilon_i.$$

- Denote $\preceq_{\mathcal{F}_r}$ by $\preceq$ (Greek letters $\rightsquigarrow \preceq_{\mathcal{F}_r}$, Latin letters $\rightsquigarrow \preceq$)
- $I^{[\Sigma]}$ (and everything from now on!) depends on $f_1, \dots, f_r$
- Recall: "*Additional information has to be lightweight*"



Reconstruction [2]

$f^{[\alpha]} = f$ vs. $f^{(\mathrm{sig}(\alpha))} = f$

presentation implementation

s-reduction

Definition

Let $f^{[\alpha]}, f'^{[\alpha']}, g^{[\gamma]} \in I^{[\Sigma]}$ with $f, g \neq 0$. Then, $f^{[\alpha]}$ s-reduces to $f'^{[\alpha']}$ by $g^{[\gamma]}$ if there exists $m \in [X]$ such that

- $m \operatorname{lm}(g) \in \operatorname{supp}(f)$
- $f'^{[\alpha']} = f^{[\alpha]} - cm \cdot g^{[\gamma]}$ with $c \in K$ s.t. $m \operatorname{lm}(g)$ cancels
- $\operatorname{sig}(m\gamma) \preceq \operatorname{sig}(\alpha)$

In this case, we write $f^{[\alpha]} \to_{g^{[\gamma]}} f'^{[\alpha']}$.

s-reduction

Definition

Let $f^{[\alpha]}, f'^{[\alpha']}, g^{[\gamma]} \in I^{[\Sigma]}$ with $f, g \neq 0$. Then, $f^{[\alpha]}$ s-reduces to $f'^{[\alpha']}$ by $g^{[\gamma]}$ if there exists $m \in [X]$ such that

- $m \operatorname{lm}(g) \in \operatorname{supp}(f)$
- $f'^{[\alpha']} = f^{[\alpha]} - cm \cdot g^{[\gamma]}$ with $c \in K$ s.t. $m \operatorname{lm}(g)$ cancels
- $\operatorname{sig}(m\gamma) \preceq \operatorname{sig}(\alpha)$

In this case, we write $f^{[\alpha]} \rightarrow_{g^{[\gamma]}} f'^{[\alpha']}$.

Note: If we forget about signatures, this is usual polynomial reduction.

s-reduction

Definition

Let $f^{[\alpha]}, f'^{[\alpha']}, g^{[\gamma]} \in I^{[\Sigma]}$ with $f, g \neq 0$. Then, $f^{[\alpha]}$ s-reduces to $f'^{[\alpha']}$ by $g^{[\gamma]}$ if there exists $m \in [X]$ such that

- $m\,\mathrm{lm}(g) \in \mathrm{supp}(f)$
- $f'^{[\alpha']} = f^{[\alpha]} - cm \cdot g^{[\gamma]}$ with $c \in K$ s.t. $m\,\mathrm{lm}(g)$ cancels
- $\mathrm{sig}(m\gamma) \preceq \mathrm{sig}(\alpha)$

In this case, we write $f^{[\alpha]} \rightarrow_{g^{[\gamma]}} f'^{[\alpha']}$.

Note: If we forget about signatures, this is usual polynomial reduction.

For sets $G^{[\Sigma]} \subseteq I^{[\Sigma]}$:

$$f^{[\alpha]} \rightarrow_{G^{[\Sigma]}} f'^{[\alpha']} \quad \Longleftrightarrow \quad \exists g^{[\gamma]} \in G^{[\Sigma]} : f^{[\alpha]} \rightarrow_{g^{[\gamma]}} f'^{[\alpha']}$$

s-reduction

Definition

Let $f^{[\alpha]}, f'^{[\alpha']}, g^{[\gamma]} \in I^{[\Sigma]}$ with $f, g \neq 0$. Then, $f^{[\alpha]}$ s-reduces to $f'^{[\alpha']}$ by $g^{[\gamma]}$ if there exists $m \in [X]$ such that

- $m \operatorname{lm}(g) \in \operatorname{supp}(f)$
- $f'^{[\alpha']} = f^{[\alpha]} - cm \cdot g^{[\gamma]}$ with $c \in K$ s.t. $m \operatorname{lm}(g)$ cancels
- $\operatorname{sig}(m\gamma) \preceq \operatorname{sig}(\alpha)$

In this case, we write $f^{[\alpha]} \rightarrow_{g^{[\gamma]}} f'^{[\alpha']}$.

Note: If we forget about signatures, this is usual polynomial reduction.

For sets $G^{[\Sigma]} \subseteq I^{[\Sigma]}$:

$$f^{[\alpha]} \rightarrow_{G^{[\Sigma]}} f'^{[\alpha']} \quad \Longleftrightarrow \quad \exists g^{[\gamma]} \in G^{[\Sigma]} : f^{[\alpha]} \rightarrow_{g^{[\gamma]}} f'^{[\alpha']}$$

$\xrightarrow{*}_{G^{[\Sigma]}} :=$ reflexive, transitive closure of $\rightarrow_{G^{[\Sigma]}}$

Signature Gröbner bases

Definition

A set $G^{[\Sigma]} \subseteq I^{[\Sigma]}$ is a...

- signature Gröbner basis of $I^{[\Sigma]}$ if

$$\forall\, f^{[\alpha]} \in I^{[\Sigma]} : \; f^{[\alpha]} \xrightarrow{*}_{G^{[\Sigma]}} 0^{[\alpha']}$$

Signature Gröbner bases

Definition

A set $G^{[\Sigma]} \subseteq I^{[\Sigma]}$ is a…

- signature Gröbner basis of $I^{[\Sigma]}$ if

$$\forall\, f^{[\alpha]} \in I^{[\Sigma]} : \; f^{[\alpha]} \xrightarrow{*}_{G^{[\Sigma]}} 0^{[\alpha']}$$

Corollary

If $G^{[\Sigma]} \subseteq I^{[\Sigma]}$ is a signature Gröbner basis of $I^{[\Sigma]}$, then $\{g \mid g^{[\gamma]} \in G^{[\Sigma]}\}$ is a Gröbner basis of I.

Signature Gröbner bases

Definition

A set $G^{[\Sigma]} \subseteq I^{[\Sigma]}$ is a...

- signature Gröbner basis of $I^{[\Sigma]}$ if

$$\forall\, f^{[\alpha]} \in I^{[\Sigma]} :\; f^{[\alpha]} \xrightarrow{*}_{G^{[\Sigma]}} 0^{[\alpha']}$$

- signature Gröbner basis of $I^{[\Sigma]}$ up to signature $\sigma = m\varepsilon_i$ if

$$\forall\, f^{[\alpha]} \in I^{[\Sigma]} :\; \operatorname{sig}(\alpha) \prec \sigma \implies f^{[\alpha]} \xrightarrow{*}_{G^{[\Sigma]}} 0^{[\alpha']}$$

Corollary

If $G^{[\Sigma]} \subseteq I^{[\Sigma]}$ is a signature Gröbner basis of $I^{[\Sigma]}$, then $\{g \mid g^{[\gamma]} \in G^{[\Sigma]}\}$ is a Gröbner basis of I.

Signature Gröbner bases

Definition

A set $G^{[\Sigma]} \subseteq I^{[\Sigma]}$ is a…

- signature Gröbner basis of $I^{[\Sigma]}$ if

$$\forall\, f^{[\alpha]} \in I^{[\Sigma]} :\; f^{[\alpha]} \xrightarrow{*}_{G^{[\Sigma]}} 0^{[\alpha']}$$

- signature Gröbner basis of $I^{[\Sigma]}$ up to signature $\sigma = m\varepsilon_i$ if

$$\forall\, f^{[\alpha]} \in I^{[\Sigma]} :\; \mathrm{sig}(\alpha) \prec \sigma \implies f^{[\alpha]} \xrightarrow{*}_{G^{[\Sigma]}} 0^{[\alpha']}$$

Corollary

If $G^{[\Sigma]} \subseteq I^{[\Sigma]}$ is a signature Gröbner basis of $I^{[\Sigma]}$, then $\{g \mid g^{[\gamma]} \in G^{[\Sigma]}\}$ is a Gröbner basis of I.

Idea: incremental computation

$$\varepsilon_1 \prec \cdots \prec \lambda_2 \prec \lambda_1 \prec \sigma \prec \rho_1 \prec \rho_2 \prec \cdots$$

Signature Gröbner bases

Definition

A set $G^{[\Sigma]} \subseteq I^{[\Sigma]}$ is a...

- signature Gröbner basis of $I^{[\Sigma]}$ if

$$\forall f^{[\alpha]} \in I^{[\Sigma]} : \ f^{[\alpha]} \xrightarrow{*}_{G^{[\Sigma]}} 0^{[\alpha']}$$

- signature Gröbner basis of $I^{[\Sigma]}$ up to signature $\sigma = m\varepsilon_i$ if

$$\forall f^{[\alpha]} \in I^{[\Sigma]} : \ \mathrm{sig}(\alpha) \prec \sigma \implies f^{[\alpha]} \xrightarrow{*}_{G^{[\Sigma]}} 0^{[\alpha']}$$

Corollary

If $G^{[\Sigma]} \subseteq I^{[\Sigma]}$ is a signature Gröbner basis of $I^{[\Sigma]}$, then $\{g \mid g^{[\gamma]} \in G^{[\Sigma]}\}$ is a Gröbner basis of I.

Idea: incremental computation

$$\overset{\downarrow}{\varepsilon_1} \prec \cdots \prec \lambda_2 \prec \lambda_1 \prec \sigma \prec \rho_1 \prec \rho_2 \prec \cdots$$

Signature Gröbner bases

Definition

A set $G^{[\Sigma]} \subseteq I^{[\Sigma]}$ is a…

- signature Gröbner basis of $I^{[\Sigma]}$ if

$$\forall\, f^{[\alpha]} \in I^{[\Sigma]} :\; f^{[\alpha]} \xrightarrow{*}_{G^{[\Sigma]}} 0^{[\alpha']}$$

- signature Gröbner basis of $I^{[\Sigma]}$ up to signature $\sigma = m\varepsilon_i$ if

$$\forall\, f^{[\alpha]} \in I^{[\Sigma]} :\; \operatorname{sig}(\alpha) \prec \sigma \implies f^{[\alpha]} \xrightarrow{*}_{G^{[\Sigma]}} 0^{[\alpha']}$$

Corollary

If $G^{[\Sigma]} \subseteq I^{[\Sigma]}$ is a signature Gröbner basis of $I^{[\Sigma]}$, then $\{g \mid g^{[\gamma]} \in G^{[\Sigma]}\}$ is a Gröbner basis of I.

Idea: incremental computation

$$\overset{\downarrow}{\varepsilon_1} \prec \cdots \prec \lambda_2 \prec \lambda_1 \prec \sigma \prec \rho_1 \prec \rho_2 \prec \cdots$$

Signature Gröbner bases

Definition

A set $G^{[\Sigma]} \subseteq I^{[\Sigma]}$ is a…

- signature Gröbner basis of $I^{[\Sigma]}$ if

$$\forall\, f^{[\alpha]} \in I^{[\Sigma]} :\; f^{[\alpha]} \xrightarrow{*}_{G^{[\Sigma]}} 0^{[\alpha']}$$

- signature Gröbner basis of $I^{[\Sigma]}$ up to signature $\sigma = m\varepsilon_i$ if

$$\forall\, f^{[\alpha]} \in I^{[\Sigma]} :\; \mathrm{sig}(\alpha) \prec \sigma \implies f^{[\alpha]} \xrightarrow{*}_{G^{[\Sigma]}} 0^{[\alpha']}$$

Corollary

If $G^{[\Sigma]} \subseteq I^{[\Sigma]}$ is a signature Gröbner basis of $I^{[\Sigma]}$, then $\{g \mid g^{[\gamma]} \in G^{[\Sigma]}\}$ is a Gröbner basis of I.

Idea: incremental computation

$$\varepsilon_1 \prec \cdots \prec \lambda_2 \prec \lambda_1 \prec \overset{\downarrow}{\sigma} \prec \rho_1 \prec \rho_2 \prec \cdots$$

Signature Gröbner bases

Definition

A set $G^{[\Sigma]} \subseteq I^{[\Sigma]}$ is a. . .

- signature Gröbner basis of $I^{[\Sigma]}$ if

$$\forall\, f^{[\alpha]} \in I^{[\Sigma]} :\; f^{[\alpha]} \xrightarrow{*}_{G^{[\Sigma]}} 0^{[\alpha']}$$

- signature Gröbner basis of $I^{[\Sigma]}$ up to signature $\sigma = m\varepsilon_i$ if

$$\forall\, f^{[\alpha]} \in I^{[\Sigma]} :\; \mathrm{sig}(\alpha) \prec \sigma \implies f^{[\alpha]} \xrightarrow{*}_{G^{[\Sigma]}} 0^{[\alpha']}$$

Corollary

If $G^{[\Sigma]} \subseteq I^{[\Sigma]}$ is a signature Gröbner basis of $I^{[\Sigma]}$, then $\{g \mid g^{[\gamma]} \in G^{[\Sigma]}\}$ is a Gröbner basis of I.

Idea: incremental computation

$$\varepsilon_1 \prec \cdots \prec \lambda_2 \prec \lambda_1 \prec \overset{\downarrow}{\sigma} \prec \rho_1 \prec \rho_2 \prec \cdots$$

Signature Gröbner bases

Definition

A set $G^{[\Sigma]} \subseteq I^{[\Sigma]}$ is a…

- signature Gröbner basis of $I^{[\Sigma]}$ if

$$\forall\, f^{[\alpha]} \in I^{[\Sigma]} :\ f^{[\alpha]} \xrightarrow{*}_{G^{[\Sigma]}} 0^{[\alpha']}$$

- signature Gröbner basis of $I^{[\Sigma]}$ up to signature $\sigma = m\varepsilon_i$ if

$$\forall\, f^{[\alpha]} \in I^{[\Sigma]} :\ \operatorname{sig}(\alpha) \prec \sigma \implies f^{[\alpha]} \xrightarrow{*}_{G^{[\Sigma]}} 0^{[\alpha']}$$

Corollary

If $G^{[\Sigma]} \subseteq I^{[\Sigma]}$ is a signature Gröbner basis of $I^{[\Sigma]}$, then $\{g \mid g^{[\gamma]} \in G^{[\Sigma]}\}$ is a Gröbner basis of I.

Idea: incremental computation

$$\varepsilon_1 \prec \cdots \prec \lambda_2 \prec \lambda_1 \prec \sigma \prec \overset{\downarrow}{\rho_1} \prec \rho_2 \prec \cdots$$

s-reduction

If $f^{[\alpha]} \longrightarrow_{g^{[\gamma]}} f'^{[\alpha']}$, then either

$$\operatorname{sig}(\alpha') = \operatorname{sig}(\alpha) \qquad \text{or} \qquad \operatorname{sig}(\alpha') \prec \operatorname{sig}(\alpha)$$

s-reduction

Recall: “*In an implementation we work with* $\mathrm{f}^{(\mathrm{sig}(\alpha))}$”

If $\mathrm{f}^{[\alpha]} \longrightarrow_{\mathrm{g}^{[\gamma]}} \mathrm{f}'^{[\alpha']}$, then either

$$\mathrm{sig}(\alpha') = \mathrm{sig}(\alpha) \qquad \text{or} \qquad \mathrm{sig}(\alpha') \prec \mathrm{sig}(\alpha)$$

s-reduction

Recall: “*In an implementation we work with* $\mathrm{f}^{(\mathrm{sig}(\alpha))}$”

If $\mathrm{f}^{[\alpha]} \longrightarrow_{\mathrm{g}^{[\gamma]}} \mathrm{f}'^{[\alpha']}$, then either

$\mathrm{sig}(\alpha') = \mathrm{sig}(\alpha)$ or $\mathrm{sig}(\alpha') \prec \mathrm{sig}(\alpha)$

s-reduction

Recall: "*In an implementation we work with* $f^{(\mathrm{sig}(\alpha))}$"

If $f^{[\alpha]} \longrightarrow_{g^{[\gamma]}} f'^{[\alpha']}$, then either

$\boxed{\mathrm{sig}(\alpha') = \mathrm{sig}(\alpha)}$ or $\boxed{\mathrm{sig}(\alpha') \prec \mathrm{sig}(\alpha)}$

happens if

$\mathrm{sig}(m\gamma) \prec \mathrm{sig}(\alpha)$

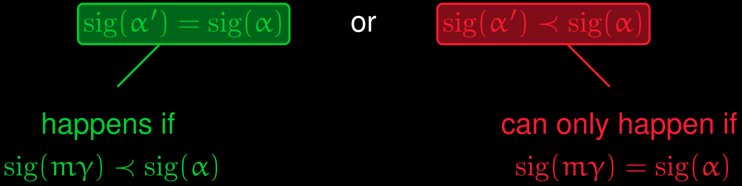
can only happen if

$\mathrm{sig}(m\gamma) = \mathrm{sig}(\alpha)$

s-reduction

Recall: “*In an implementation we work with* $f^{(\mathrm{sig}(\alpha))}$”

If $f^{[\alpha]} \longrightarrow_{g^{[\gamma]}} f'^{[\alpha']}$, then either



$\boxed{\mathrm{sig}(\alpha') = \mathrm{sig}(\alpha)}$ or $\boxed{\mathrm{sig}(\alpha') \prec \mathrm{sig}(\alpha)}$

happens if $\mathrm{sig}(m\gamma) \prec \mathrm{sig}(\alpha)$

can only happen if $\mathrm{sig}(m\gamma) = \mathrm{sig}(\alpha)$

$f^{[\alpha]} \longrightarrow_{g^{[\gamma]}} f'^{[\alpha']}$ is a regular s-reduction if $\mathrm{sig}(m\gamma) \prec \mathrm{sig}(\alpha)$

$f^{[\alpha]} \longrightarrow_{g^{[\gamma]}} f'^{[\alpha']}$ is a singular s-reduction if $\mathrm{sig}(m\gamma) = \mathrm{sig}(\alpha)$

s-reduction

Recall: “*In an implementation we work with* $f^{(\mathrm{sig}(\alpha))}$”

If $f^{[\alpha]} \longrightarrow_{g^{[\gamma]}} f'^{[\alpha']}$, then either

$\boxed{\mathrm{sig}(\alpha') = \mathrm{sig}(\alpha)}$ or $\boxed{\mathrm{sig}(\alpha') \prec \mathrm{sig}(\alpha)}$

happens if $\mathrm{sig}(m\gamma) \prec \mathrm{sig}(\alpha)$

can only happen if $\mathrm{sig}(m\gamma) = \mathrm{sig}(\alpha)$

$f^{[\alpha]} \longrightarrow_{g^{[\gamma]}} f'^{[\alpha']}$ is a regular s-reduction if $\mathrm{sig}(m\gamma) \prec \mathrm{sig}(\alpha)$

$f^{[\alpha]} \longrightarrow_{g^{[\gamma]}} f'^{[\alpha']}$ is a singular s-reduction if $\mathrm{sig}(m\gamma) = \mathrm{sig}(\alpha)$

$f^{[\alpha]} \longrightarrow_{g^{[\gamma]}} f'^{[\alpha']}$ is a top s-reduction if $\mathrm{lm}(mg) = \mathrm{lm}(f)$

S-polynomials

Definition

Let $f^{[\alpha]}, g^{[\beta]} \in I^{[\Sigma]}$ with $f, g \neq 0$ and $M = \operatorname{lcm}(\operatorname{lm}(f), \operatorname{lm}(g))$.

$$\operatorname{spol}(f^{[\alpha]}, g^{[\beta]}) \coloneqq \frac{M}{\operatorname{lt}(f)} \cdot f^{[\alpha]} \; - \; \frac{M}{\operatorname{lt}(g)} \cdot g^{[\beta]} \, .$$

S-polynomials

Definition

Let $f^{[\alpha]}, g^{[\beta]} \in I^{[\Sigma]}$ with $f, g \neq 0$ and $M = \operatorname{lcm}(\operatorname{lm}(f), \operatorname{lm}(g))$.

$$\operatorname{spol}(f^{[\alpha]}, g^{[\beta]}) \coloneqq \frac{M}{\operatorname{lt}(f)} \cdot f^{[\alpha]} - \frac{M}{\operatorname{lt}(g)} \cdot g^{[\beta]}.$$

S-polynomials

Definition

Let $f^{[\alpha]}, g^{[\beta]} \in I^{[\Sigma]}$ with $f, g \neq 0$ and $M = \mathrm{lcm}(\mathrm{lm}(f), \mathrm{lm}(g))$.

$$\mathrm{spol}(f^{[\alpha]}, g^{[\beta]}) \coloneqq \underbrace{\frac{M}{\mathrm{lt}(f)} \cdot f^{[\alpha]}}_{= f'^{[\alpha']}} - \underbrace{\frac{M}{\mathrm{lt}(g)} \cdot g^{[\beta]}}_{= g'^{[\beta']}}.$$

If $h^{[\delta]} = \mathrm{spol}(f^{[\alpha]}, g^{[\beta]})$ and $\sigma = \max\{\mathrm{sig}(\alpha'), \mathrm{sig}(\beta')\}$, then either

$$\mathrm{sig}(\delta) = \sigma \qquad \text{or} \qquad \mathrm{sig}(\delta) \prec \sigma$$

S-polynomials

Definition

Let $f^{[\alpha]}, g^{[\beta]} \in I^{[\Sigma]}$ with $f, g \neq 0$ and $M = \operatorname{lcm}(\operatorname{lm}(f), \operatorname{lm}(g))$.

$$\operatorname{spol}(f^{[\alpha]}, g^{[\beta]}) := \underbrace{\frac{M}{\operatorname{lt}(f)} \cdot f^{[\alpha]}}_{= f'^{[\alpha']}} - \underbrace{\frac{M}{\operatorname{lt}(g)} \cdot g^{[\beta]}}_{= g'^{[\beta']}}.$$

If $h^{[\delta]} = \operatorname{spol}(f^{[\alpha]}, g^{[\beta]})$ and $\sigma = \max\{\operatorname{sig}(\alpha'), \operatorname{sig}(\beta')\}$, then either

$\operatorname{sig}(\delta) = \sigma$ or $\operatorname{sig}(\delta) \prec \sigma$

S-polynomials

Definition

Let $f^{[\alpha]}, g^{[\beta]} \in I^{[\Sigma]}$ with $f, g \neq 0$ and $M = \operatorname{lcm}(\operatorname{lm}(f), \operatorname{lm}(g))$.

$$\operatorname{spol}(f^{[\alpha]}, g^{[\beta]}) \coloneqq \underbrace{\frac{M}{\operatorname{lt}(f)} \cdot f^{[\alpha]}}_{= f'^{[\alpha']}} - \underbrace{\frac{M}{\operatorname{lt}(g)} \cdot g^{[\beta]}}_{= g'^{[\beta']}} .$$

If $h^{[\delta]} = \operatorname{spol}(f^{[\alpha]}, g^{[\beta]})$ and $\sigma = \max\{\operatorname{sig}(\alpha'), \operatorname{sig}(\beta')\}$, then either

$\boxed{\operatorname{sig}(\delta) = \sigma}$ or $\boxed{\operatorname{sig}(\delta) \prec \sigma}$

happens if

$\operatorname{sig}(\alpha') \neq \operatorname{sig}(\beta')$

can only happen if

$\operatorname{sig}(\alpha') = \operatorname{sig}(\beta')$

S-polynomials

Definition

Let $f^{[\alpha]}, g^{[\beta]} \in I^{[\Sigma]}$ with $f, g \neq 0$ and $M = \operatorname{lcm}(\operatorname{lm}(f), \operatorname{lm}(g))$.

$$\operatorname{spol}(f^{[\alpha]}, g^{[\beta]}) \coloneqq \underbrace{\frac{M}{\operatorname{lt}(f)} \cdot f^{[\alpha]}}_{= f'^{[\alpha']}} - \underbrace{\frac{M}{\operatorname{lt}(g)} \cdot g^{[\beta]}}_{= g'^{[\beta']}}.$$

If $h^{[\delta]} = \operatorname{spol}(f^{[\alpha]}, g^{[\beta]})$ and $\sigma = \max\{\operatorname{sig}(\alpha'), \operatorname{sig}(\beta')\}$, then either

$\boxed{\operatorname{sig}(\delta) = \sigma}$ or $\boxed{\operatorname{sig}(\delta) \prec \sigma}$

happens if

$\operatorname{sig}(\alpha') \neq \operatorname{sig}(\beta')$

can only happen if

$\operatorname{sig}(\alpha') = \operatorname{sig}(\beta')$

$\operatorname{spol}(f^{[\alpha]}, g^{[\beta]})$ is a regular S-polynomial if $\operatorname{sig}(\alpha') \neq \operatorname{sig}(\beta')$

$\operatorname{spol}(f^{[\alpha]}, g^{[\beta]})$ is a singular S-polynomial if $\operatorname{sig}(\alpha') = \operatorname{sig}(\beta')$

S-polynomial criterion

Theorem (S-polynomial criterion)

Let $\sigma = m\varepsilon_j$ and let $G^{[\Sigma]} \subseteq I^{[\Sigma]}$ be such that for all $\varepsilon_i \prec \sigma$ there exists $g_i^{[\gamma_i]} \in G^{[\Sigma]}$ with $\mathrm{sig}(\gamma_i) = \varepsilon_i$. Assume that all regular S-polynomials $p^{[\pi]}$ of $G^{[\Sigma]}$ with $\mathrm{sig}(\pi) \prec \sigma$ regular s-reduce to $p'^{[\pi']}$ such that

- $p' = 0$, or
- $p'^{[\pi']}$ is singular top s-reducible.

Then, $G^{[\Sigma]}$ is a signature Gröbner basis of $I^{[\Sigma]}$ up to signature σ.

S-polynomial criterion

Theorem (S-polynomial criterion)

Let $\sigma = m\varepsilon_j$ and let $G^{[\Sigma]} \subseteq I^{[\Sigma]}$ be such that for all $\varepsilon_i \prec \sigma$ there exists $g_i^{[\gamma_i]} \in G^{[\Sigma]}$ with $\mathrm{sig}(\gamma_i) = \varepsilon_i$. Assume that all regular S-polynomials $p^{[\pi]}$ of $G^{[\Sigma]}$ with $\mathrm{sig}(\pi) \prec \sigma$ regular s-reduce to $p'^{[\pi']}$ such that

- $p' = 0$, or
- $p'^{[\pi']}$ is singular top s-reducible.

Then, $G^{[\Sigma]}$ is a signature Gröbner basis of $I^{[\Sigma]}$ up to signature σ.

S-polynomial criterion

Theorem (S-polynomial criterion)

Let $\sigma = m\varepsilon_j$ and let $G^{[\Sigma]} \subseteq I^{[\Sigma]}$ be such that for all $\varepsilon_i \prec \sigma$ there exists $g_i^{[\gamma_i]} \in G^{[\Sigma]}$ with $\mathrm{sig}(\gamma_i) = \varepsilon_i$. Assume that all regular S-polynomials $p^{[\pi]}$ of $G^{[\Sigma]}$ with $\mathrm{sig}(\pi) \prec \sigma$ regular s-reduce to $p'^{[\pi']}$ such that

- $p' = 0$, or
- $p'^{[\pi']}$ is singular top s-reducible.

Then, $G^{[\Sigma]}$ is a signature Gröbner basis of $I^{[\Sigma]}$ up to signature σ.

S-polynomial criterion

Theorem (S-polynomial criterion)

Let $\sigma = m\varepsilon_j$ and let $G^{[\Sigma]} \subseteq I^{[\Sigma]}$ be such that for all $\varepsilon_i \prec \sigma$ there exists $g_i^{[\gamma_i]} \in G^{[\Sigma]}$ with $\operatorname{sig}(\gamma_i) = \varepsilon_i$. Assume that all regular S-polynomials $p^{[\pi]}$ of $G^{[\Sigma]}$ with $\operatorname{sig}(\pi) \prec \sigma$ regular s-reduce to $p'^{[\pi']}$ such that

- $p' = 0$, or
- $p'^{[\pi']}$ is singular top s-reducible.

Then, $G^{[\Sigma]}$ is a signature Gröbner basis of $I^{[\Sigma]}$ up to signature σ.

S-polynomial criterion

Theorem (S-polynomial criterion)

Let $\sigma = m\varepsilon_j$ and let $G^{[\Sigma]} \subseteq I^{[\Sigma]}$ be such that for all $\varepsilon_i \prec \sigma$ there exists $g_i^{[\gamma_i]} \in G^{[\Sigma]}$ with $\operatorname{sig}(\gamma_i) = \varepsilon_i$. Assume that all regular S-polynomials $p^{[\pi]}$ of $G^{[\Sigma]}$ with $\operatorname{sig}(\pi) \prec \sigma$ regular s-reduce to $p'^{[\pi']}$ such that

- $p' = 0$, or
- $p'^{[\pi']}$ is singular top s-reducible.

Then, $G^{[\Sigma]}$ is a signature Gröbner basis of $I^{[\Sigma]}$ up to signature σ.

S-polynomial criterion

Theorem (S-polynomial criterion)

Let $\sigma = m\varepsilon_j$ and let $G^{[\Sigma]} \subseteq I^{[\Sigma]}$ be such that for all $\varepsilon_i \prec \sigma$ there exists $g_i^{[\gamma_i]} \in G^{[\Sigma]}$ with $\mathrm{sig}(\gamma_i) = \varepsilon_i$. Assume that all regular S-polynomials $p^{[\pi]}$ of $G^{[\Sigma]}$ with $\mathrm{sig}(\pi) \prec \sigma$ regular s-reduce to $p'^{[\pi']}$ such that

- $p' = 0$, or
- $p'^{[\pi']}$ is singular top s-reducible.

Then, $G^{[\Sigma]}$ is a signature Gröbner basis of $I^{[\Sigma]}$ up to signature σ.

S-polynomial criterion

Proof idea.

$\mathrm{h}^{[\delta]}$ s.t.
$\mathrm{sig}(\delta) \prec \sigma$ minimal

S-polynomial criterion

Proof idea.

$$\begin{tikzcd} h^{[\delta]} \text{ s.t. } \\ \mathrm{sig}(\delta) \prec \sigma \text{ minimal} \arrow[d, "*", "G^{[\Sigma]}"'] \\ 0 \end{tikzcd}$$

S-polynomial criterion

Proof idea.

$$\begin{tikzcd}
\begin{array}{c} h^{[\delta]} \text{ s.t.} \\ \mathrm{sig}(\delta) \prec \sigma \text{ minimal} \end{array} \arrow[r, dashed, "\text{construct}"] \arrow[d, "*", "G^{[\Sigma]}"'] & \begin{array}{c} p^{[\pi]} \text{ regular S-poly} \\ \text{s.t. } \mathrm{sig}(\delta) = \mathrm{sig}(m\pi) \end{array} \\
0 &
\end{tikzcd}$$

S-polynomial criterion

Proof idea.

$$\begin{tikzcd}
\begin{array}{c} h^{[\delta]} \text{ s.t.} \\ \operatorname{sig}(\delta) \prec \sigma \text{ minimal} \end{array} \arrow[r, dashed, "\text{construct}"] \arrow[dd, "*", "G^{[\Sigma]}"'] & \begin{array}{c} p^{[\pi]} \text{ regular S-poly} \\ \text{s.t. } \operatorname{sig}(\delta) = \operatorname{sig}(m\pi) \end{array} \arrow[d, "*_r", "G^{[\Sigma]}"'] \\
& p'^{[\pi']} \\
0 &
\end{tikzcd}$$

S-polynomial criterion

Proof idea.

$$\begin{tikzcd}
\begin{array}{c} h^{[\delta]} \text{ s.t.} \\ \mathrm{sig}(\delta) \prec \sigma \text{ minimal} \end{array} \arrow[rr, dashed, "\text{construct}"] \arrow[dd, "*", "G^{[\Sigma]}"'] & & \begin{array}{c} p^{[\pi]} \text{ regular S-poly} \\ \text{s.t. } \mathrm{sig}(\delta) = \mathrm{sig}(m\pi) \end{array} \arrow[d, "*_r", "G^{[\Sigma]}"'] & \\
 & & p'^{[\pi']} \arrow[dl, dashed] \arrow[dr, dashed] & \\
0 & p' = 0 & & \begin{array}{c} p'^{[\pi']} \\ \text{sing. top s-red.} \end{array}
\end{tikzcd}$$

S-polynomial criterion

Proof idea.

$$\begin{tikzcd}
h^{[\delta]} \text{ s.t.} \\ \mathrm{sig}(\delta) \prec \sigma \text{ minimal} \arrow[rr, dashed, "\text{construct}"] \arrow[dd, "*", "G^{[\Sigma]}"'] & & p^{[\pi]} \text{ regular S-poly} \\ \text{s.t. } \mathrm{sig}(\delta) = \mathrm{sig}(m\pi) \arrow[d, "*_r", "G^{[\Sigma]}"'] & \\
& & p'^{[\pi']} \arrow[dl, dashed] \arrow[dr, dashed] & \\
0 & p' = 0 \arrow[l, dashed, "\text{Lemma}"'] & & p'^{[\pi']} \\ \text{sing. top s-red.}
\end{tikzcd}$$

S-polynomial criterion

Proof idea.

$$\begin{tikzcd}
\begin{array}{c} h^{[\delta]} \text{ s.t.} \\ \mathrm{sig}(\delta) \prec \sigma \text{ minimal} \end{array} \arrow[rr, dashed, "\text{construct}"] \arrow[dd, "*", "G^{[\Sigma]}"'] & & \begin{array}{c} p^{[\pi]} \text{ regular S-poly} \\ \text{s.t. } \mathrm{sig}(\delta) = \mathrm{sig}(m\pi) \end{array} \arrow[d, "*_r", "G^{[\Sigma]}"'] & \\
& & p'^{[\pi']} \arrow[dl, dashed] \arrow[dr, dashed] & \\
0 & p' = 0 \arrow[l, dashed, "\text{Lemma}"] & & \begin{array}{c} p'^{[\pi']} \\ \text{sing. top s-red.} \end{array} \arrow[dll, dashed, bend left, "\begin{array}{c} \text{Lemma} \\ + \\ \text{tech. details} \end{array}"] \\
& \begin{array}{c} h^{[\delta]} \\ \text{sing. top s-red.} \end{array} & &
\end{tikzcd}$$

S-polynomial criterion

Proof idea.

$$\begin{tikzcd}
\begin{array}{c} h^{[\delta]} \text{ s.t.} \\ \operatorname{sig}(\delta) \prec \sigma \text{ minimal} \end{array} \arrow[rrr, dashed, "\text{construct}"] \arrow[dd, "*", "G^{[\Sigma]}"'] & & & \begin{array}{c} p^{[\pi]} \text{ regular S-poly} \\ \text{s.t. } \operatorname{sig}(\delta) = \operatorname{sig}(m\pi) \end{array} \arrow[d, "*_r", "G^{[\Sigma]}"'] & \\
 & & & p'^{[\pi']} \arrow[dl, dashed] \arrow[dr, dashed] & \\
0 & & p' = 0 \arrow[ll, dashed, "\text{Lemma}"'] & & \begin{array}{c} p'^{[\pi']} \\ \text{sing. top s-red.} \end{array} \arrow[dll, dashed, bend left, "\begin{array}{c} \text{Lemma} \\ + \\ \text{tech. details} \end{array}"] \\
\begin{array}{c} h'^{[\delta']} \text{ s.t.} \\ \operatorname{sig}(\delta') \prec \operatorname{sig}(\delta) \end{array} & & \begin{array}{c} h^{[\delta]} \\ \text{sing. top s-red.} \end{array} \arrow[ll, "G^{[\Sigma]}"'] & &
\end{tikzcd}$$

S-polynomial criterion

Proof idea.

$$\begin{tikzcd}
\begin{array}{c} h^{[\delta]} \text{ s.t.} \\ \mathrm{sig}(\delta) \prec \sigma \text{ minimal} \end{array} \arrow[rr, dashed, "\text{construct}"] \arrow[dd, "*", "G^{[\Sigma]}"'] & & \begin{array}{c} p^{[\pi]} \text{ regular S-poly} \\ \text{s.t. } \mathrm{sig}(\delta) = \mathrm{sig}(m\pi) \end{array} \arrow[d, "*_r", "G^{[\Sigma]}"'] & \\
& & p'^{[\pi']} \arrow[dl, dashed] \arrow[dr, dashed] & \\
0 & p' = 0 \arrow[l, dashed, "\text{Lemma}"] & & \begin{array}{c} p'^{[\pi']} \\ \text{sing. top s-red.} \end{array} \arrow[dll, dashed, bend left, "\begin{array}{c} \text{Lemma} \\ + \\ \text{tech. details} \end{array}"'] \\
\begin{array}{c} h'^{[\delta']} \text{ s.t.} \\ \mathrm{sig}(\delta') \prec \mathrm{sig}(\delta) \end{array} \arrow[u, "*", "G^{[\Sigma]}"'] & \begin{array}{c} h^{[\delta]} \\ \text{sing. top s-red.} \end{array} \arrow[l, "G^{[\Sigma]}"] & &
\end{tikzcd}$$

Signature-based algorithm

Input: $f_1, \dots, f_r \in K[X]$

Output: A sig. GB of $(f_1, \dots, f_r)$

```
$G^{[\Sigma]} \leftarrow \emptyset$
$P \leftarrow \{f_1^{[\varepsilon_1]}, \dots, f_r^{[\varepsilon_r]}\}$
while $P \neq \emptyset$ do
    choose $p^{[\pi]} \in P$ with minimal signature
    $P \leftarrow P \setminus \{p^{[\pi]}\}$
    $p'^{[\pi']} \leftarrow$ result of regular s-reducing $p^{[\pi]}$
    if $p' \neq 0$ and $p'^{[\pi']}$ is not singular top s-reducible then
        $G^{[\Sigma]} \leftarrow G^{[\Sigma]} \cup \{p'^{[\pi']}\}$
        $P \leftarrow P \cup \{$all regular S-polys between $p'^{[\pi']}$ and $G^{[\Sigma]}\}$
return $G^{[\Sigma]}$
```

Signature-based algorithm

Input: $f_1, \ldots, f_r \in K[X]$

Output: A sig. GB of $(f_1, \ldots, f_r)$

```
$G^{[\Sigma]} \leftarrow \emptyset$
$P \leftarrow \{f_1^{[\varepsilon_1]}, \ldots$
while $P \neq \emptyset$
    choose
    $P \leftarrow P \setminus$
    $p'^{[\pi']} \leftarrow$
    if $p' \neq 0$ ducible then
        $G^{[\Sigma]} \leftarrow$
        $P \leftarrow P \cup$ n $p'^{[\pi']}$ and $G^{[\Sigma]}\}$
return $G^{[\Sigma]}$
```

Elimination criteria

Let $\mathrm{p}^{[\pi]} \in \mathrm{I}^{[\Sigma]}$ and let $\mathrm{G}^{[\Sigma]} \subseteq \mathrm{I}^{[\Sigma]}$ be a signature Gröbner basis up to signature $\mathrm{sig}(\pi)$. Then $\mathrm{p}^{[\pi]}$ s-reduces to zero, if…

Elimination criteria

Let $\mathrm{p}^{[\pi]} \in \mathrm{I}^{[\Sigma]}$ and let $\mathrm{G}^{[\Sigma]} \subseteq \mathrm{I}^{[\Sigma]}$ be a signature Gröbner basis up to signature $\mathrm{sig}(\pi)$. Then $\mathrm{p}^{[\pi]}$ s-reduces to zero, if…

- Syzygy criterion:
- F5 criterion:
- Singular criterion:

Elimination criteria

Let $p^{[\pi]} \in I^{[\Sigma]}$ and let $G^{[\Sigma]} \subseteq I^{[\Sigma]}$ be a signature Gröbner basis up to signature $\operatorname{sig}(\pi)$. Then $p^{[\pi]}$ s-reduces to zero, if…

- Syzygy criterion: …there exists a syzygy $\alpha \in \operatorname{Syz}(f_1, \dots, f_r)$ and $m \in [X]$ such that $\operatorname{sig}(\pi) = m \operatorname{sig}(\alpha)$;
- F5 criterion:
- Singular criterion:

Elimination criteria

Let $p^{[\pi]} \in I^{[\Sigma]}$ and let $G^{[\Sigma]} \subseteq I^{[\Sigma]}$ be a signature Gröbner basis up to signature $\mathrm{sig}(\pi)$. Then $p^{[\pi]}$ s-reduces to zero, if…

- Syzygy criterion: …there exists a syzygy $\alpha \in \mathrm{Syz}(f_1, \dots, f_r)$ and $m \in [X]$ such that $\mathrm{sig}(\pi) = m\,\mathrm{sig}(\alpha)$;
- F5 criterion: …there exists a trivial syzygy $\alpha \in \mathrm{Syz}(f_1, \dots, f_r)$ and $m \in [X]$ such that $\mathrm{sig}(\pi) = m\,\mathrm{sig}(\alpha)$;
- Singular criterion:

Elimination criteria

Let $p^{[\pi]} \in I^{[\Sigma]}$ and let $G^{[\Sigma]} \subseteq I^{[\Sigma]}$ be a signature Gröbner basis up to signature $\mathrm{sig}(\pi)$. Then $p^{[\pi]}$ s-reduces to zero, if…

- Syzygy criterion: …there exists a syzygy $\alpha \in \mathrm{Syz}(f_1, \ldots, f_r)$ and $m \in [X]$ such that $\mathrm{sig}(\pi) = m\,\mathrm{sig}(\alpha)$;
- F5 criterion: …there exists a trivial syzygy $\alpha \in \mathrm{Syz}(f_1, \ldots, f_r)$ and $m \in [X]$ such that $\mathrm{sig}(\pi) = m\,\mathrm{sig}(\alpha)$;
- Singular criterion: …there exists a regular s-reduced element $g^{[\gamma]} \in G^{[\Sigma]}$ such that $\mathrm{sig}(\gamma) = \mathrm{sig}(\pi)$;

Signature-based algorithm

Input: $f_1, \ldots, f_r \in K[X]$

Output: A sig. GB of $(f_1, \ldots, f_r)$

```
$G^{[\Sigma]} \leftarrow \emptyset$, $H \leftarrow \emptyset$
$P \leftarrow \{f_1^{[\varepsilon_1]}, \ldots, f_r^{[\varepsilon_r]}\}$
while $P \neq \emptyset$ do
    choose $p^{[\pi]} \in P$ with minimal signature
    $P \leftarrow P \setminus \{p^{[\pi]}\}$
    if not Syzygy, F5 or Singular criterion then
        $p'^{[\pi']} \leftarrow$ result of regular s-reducing $p^{[\pi]}$
        if $p' = 0$ then
            $H \leftarrow H \cup \{\pi'\}$
        else if $p'^{[\pi']}$ is not singular top s-reducible then
            $G^{[\Sigma]} \leftarrow G^{[\Sigma]} \cup \{p'^{[\pi']}\}$
            $P \leftarrow P \cup \{$all regular S-polys between $p'^{[\pi']}$ and $G^{[\Sigma]}\}$
return $G^{[\Sigma]}$
```

Signature-based algorithm

Input: $f_1, \ldots, f_r \in K[X]$

Output: A sig. GB of $(f_1, \ldots, f_r)$

```
$G^{[\Sigma]} \leftarrow \emptyset$, $H \leftarrow \emptyset$
$P \leftarrow \{f_1^{[\varepsilon_1]}, \ldots, f_r^{[\varepsilon_r]}\}$
while $P \neq \emptyset$ do
    choose $p^{[\pi]} \in P$ with minimal signature
    $P \leftarrow P \setminus \{p^{[\pi]}\}$
    if not Syzygy, F5 or Singular criterion then
        $p'^{[\pi']} \leftarrow$ result of regular s-reducing $p^{[\pi]}$
        if $p' = 0$ then
            $H \leftarrow H \cup \{\pi'\}$
        else if $p'^{[\pi']}$ is not singular top s-reducible then
            $G^{[\Sigma]} \leftarrow G^{[\Sigma]} \cup \{p'^{[\pi']}\}$
            $P \leftarrow P \cup \{$all regular S-polys between $p'^{[\pi']}$ and $G^{[\Sigma]}\}$
return $G^{[\Sigma]}$
```

Signature-based algorithm

Input: $f_1, \ldots, f_r \in K[X]$

Output: A sig. GB of $(f_1, \ldots, f_r)$ and a GB of $\mathrm{Syz}(f_1, \ldots, f_r)$

```
$G^{[\Sigma]} \leftarrow \emptyset$, $H \leftarrow \emptyset$
$P \leftarrow \{f_1^{[\varepsilon_1]}, \ldots, f_r^{[\varepsilon_r]}\}$
while $P \neq \emptyset$ do
    choose $p^{[\pi]} \in P$ with minimal signature
    $P \leftarrow P \setminus \{p^{[\pi]}\}$
    if not Syzygy, F5 or Singular criterion then
        $p'^{[\pi']} \leftarrow$ result of regular s-reducing $p^{[\pi]}$
        if $p' = 0$ then
            $H \leftarrow H \cup \{\pi'\}$
        else if $p'^{[\pi']}$ is not singular top s-reducible then
            $G^{[\Sigma]} \leftarrow G^{[\Sigma]} \cup \{p'^{[\pi']}\}$
            $P \leftarrow P \cup \{$all regular S-polys between $p'^{[\pi']}$ and $G^{[\Sigma]}\}$
return $G^{[\Sigma]}$, $H$
```

Concrete instantiations

Hyperparameters:

- Module ordering ($\preceq_{\mathtt{pot}}, \preceq_{\mathtt{top}}$)
- Selection of S-polynomials (usually by signature)
  - What in case of ties? ($\trianglelefteq_{\mathtt{add}}, \trianglelefteq_{\mathtt{lm}}$)
- Which elimination criteria are used to which extent?

Concrete instantiations

Hyperparameters:

- Module ordering ($\preceq_{\mathtt{pot}}$, $\preceq_{\mathtt{top}}$)
- Selection of S-polynomials (usually by signature)
  - What in case of ties? ($\trianglelefteq_{\mathtt{add}}$, $\trianglelefteq_{\mathtt{lm}}$)
- Which elimination criteria are used to which extent?

Algorithms:

- F5: $\preceq_{\mathtt{deg-pot}}$, $\trianglelefteq_{\mathtt{add}}$, F4-style reduction, no Syzygy crit., F5 crit. only for trivial syzygies among $f_i^{[\varepsilon_i]}$
- Many F5 variants (change reduction style, interreduce intermediate bases, ensure termination)
- G2V: $\preceq_{\mathtt{pot}}$, $\trianglelefteq_{\mathtt{add}}$, full Syzygy criterion, consider coefficients for s-reduction
- GVW: free choice of module ordering, $\trianglelefteq_{\mathtt{lm}}$, extended Syzygy criterion

Reconstruction

Recall: “*In an implementation we work with* $f^{(\mathrm{sig}(\alpha))}$”

We do **not** get

$G^{[\Sigma]} = \{g_1^{[\gamma_1]}, \ldots, g_m^{[\gamma_m]}\}$	and	$H = \{\alpha_1, \ldots, \alpha_k\}$
sig. GB of $(f_1, \ldots, f_r)$		GB of $\mathrm{Syz}(f_1, \ldots, f_r)$

but only

$G^{(\Sigma)} = \{g_1^{(\mathrm{sig}(\gamma_1))}, \ldots, g_m^{(\mathrm{sig}(\gamma_m))}\}$	and	$H' = \{\mathrm{sig}(\alpha_1), \ldots, \mathrm{sig}(\alpha_k)\}$
sig. labelled GB of $(f_1, \ldots, f_r)$		GB of $\mathrm{lt}(\mathrm{Syz}(f_1, \ldots, f_r))$

Reconstruction

Recall: “*In an implementation we work with* $f^{(\mathrm{sig}(\alpha))}$”

We do **not** get

$G^{[\Sigma]} = \{g_1^{[\gamma_1]}, \ldots, g_m^{[\gamma_m]}\}$ and $H = \{\alpha_1, \ldots, \alpha_k\}$

sig. GB of $(f_1, \ldots, f_r)$ GB of $\mathrm{Syz}(f_1, \ldots, f_r)$

but only

$G^{(\Sigma)} = \{g_1^{(\mathrm{sig}(\gamma_1))}, \ldots, g_m^{(\mathrm{sig}(\gamma_m))}\}$ and $H' = \{\mathrm{sig}(\alpha_1), \ldots, \mathrm{sig}(\alpha_k)\}$

sig. labelled GB of $(f_1, \ldots, f_r)$ GB of $\mathrm{lt}(\mathrm{Syz}(f_1, \ldots, f_r))$

We can recover this information!

Reconstruction

Step 1: Reconstruct $\mathrm{G}^{[\Sigma]}$ from $\mathrm{G}^{(\Sigma)}$

Step 2: Use $\mathrm{G}^{[\Sigma]}$ and H' to reconstruct H

Reconstruction

Step 1: Reconstruct $G^{[\Sigma]}$ from $G^{(\Sigma)}$

```
$G^{[\Sigma]} \leftarrow \emptyset$
while $G^{(\Sigma)} \neq \emptyset$ do
    choose $f^{(\sigma)} \in G^{(\Sigma)}$ with minimal signature and remove
    find $m \in [X], g^{[\gamma]} \in G^{[\Sigma]} \cup \{f_1^{[\varepsilon_1]}, \ldots, f_r^{[\varepsilon_r]}\}$ s.t. $\mathrm{sig}(m\gamma) = \sigma$
    $g'^{[\gamma']} \leftarrow$ result of regular s-reducing $m \cdot g^{[\gamma]}$ by $G^{[\Sigma]}$
    $G^{[\Sigma]} \leftarrow G^{[\Sigma]} \cup \{g'^{[\gamma']}\}$
```

Step 2: Use $G^{[\Sigma]}$ and H' to reconstruct H

Reconstruction

Step 1: Reconstruct $G^{[\Sigma]}$ from $G^{(\Sigma)}$

```
$G^{[\Sigma]} \leftarrow \emptyset$
**while** $G^{(\Sigma)} \neq \emptyset$ **do**
    choose $f^{(\sigma)} \in G^{(\Sigma)}$ with minimal signature and remove
    find $m \in [X], g^{[\gamma]} \in G^{[\Sigma]} \cup \{f_1^{[\varepsilon_1]}, \dots, f_r^{[\varepsilon_r]}\}$ s.t. $\mathrm{sig}(m\gamma) = \sigma$
    $g'^{[\gamma']} \leftarrow$ result of regular s-reducing $m \cdot g^{[\gamma]}$ by $G^{[\Sigma]}$
    $G^{[\Sigma]} \leftarrow G^{[\Sigma]} \cup \{g'^{[\gamma']}\}$
```

Step 2: Use $G^{[\Sigma]}$ and H' to reconstruct H

```
$H \leftarrow \emptyset$
**for** $\sigma \in H'$ **do**
    find $m \in [X], g^{[\gamma]} \in G^{[\Sigma]}$ s.t. $\mathrm{sig}(m\gamma) = \sigma$
    $0^{[\gamma']} \leftarrow$ result of regular s-reducing $m \cdot g^{[\gamma]}$ by $G^{[\Sigma]}$
    $H \leftarrow H \cup \{\gamma'\}$
```

Is it all worth it?

Is it all worth it?

Short answer: Not so clear

Is it all worth it?

Short answer: Not so clear

Long answer:

- For Gröbner basis + module information: yes
- Just for Gröbner basis computation: probably

Is it all worth it?

Short answer: Not so clear

Long answer:

- For Gröbner basis + module information: yes
- Just for Gröbner basis computation: probably

Evidence:

- The reconstruction of module information is pretty fast
- Intractable problems could be solved with F5 (cyclic 10, HFE, C^*)
- For generic input F4 seems to be the fastest (among the available options)

References

[1] Christian Eder and Jean-Charles Faugère. *A survey on signature-based algorithms for computing Gröbner bases*, Journal of Symbolic Computation, 80 : 719–784, 2017.

[2] Shuhong Gao, Frank Volny IV, and Mingsheng Wang. *A new framework for computing Gröbner bases*. Mathematics of Computation, 85(297): 449 – 465, 2015.

[3] Yao Sun and Dingkang Wang. *Solving detachability problem for the polynomial ring by signature-based Gröbner basis algorithms*. arXiv preprint arXiv:1108.1301, 2011.