

F5

Gröbner bases: review

Rough idea

Signatures

Predicting zero
reductions

The algorithm

Implementation

Why?

Where?

Two variants

Termination (?)

The difficulty

Faugère's original
argument

Non-terminating
example... terminates!

Variants that guarantee
termination

Remarks on Faugère's F5 algorithm

John Perry

(based on joint work with Christian Eder)

Department of Mathematics, The University of Southern Mississippi

Sage Days 12, 21 January 2008

F5: algorithm to compute Gröbner bases of polynomial ideals

(J-C Faugère, 2002)

F5

Gröbner bases: review

Rough idea

Signatures

Predicting zero
reductions

The algorithm

Implementation

Why?

Where?

Two variants

Termination (?)

The difficulty

Faugère's original
argument

Non-terminating
example... terminates!

Variants that guarantee
termination

F5

Gröbner bases: review

Rough idea

Signatures

Predicting zero
reductions

The algorithm

Implementation

Why?

Where?

Two variants

Termination (?)

The difficulty

Faugère's original
argument

Non-terminating
example... terminates!

Variants that guarantee
termination

1 F5

Gröbner bases: review

Rough idea

Signatures

Predicting zero reductions

The algorithm

2 Implementation

Why?

Where?

Two variants

3 Termination (?)

The difficulty

Faugère's original argument

Non-terminating example... terminates!

Variants that guarantee termination

Gröbner bases?

Gröbner basis: “nice form” for generators of polynomial ideal

- “*nice*”: ~~difficult~~ ^{easy!} questions

(B Buchberger, 1965)

Generalizes linear algebra

- *Vector space:* Gaussian elimination \longrightarrow echelon form

$$\left\{ \begin{array}{cccc|c} * & * & * & * & = * \\ * & * & * & * & = * \\ * & * & * & * & = * \\ * & * & * & * & = * \end{array} \right. \longrightarrow \left\{ \begin{array}{cccc|c} * & * & * & * & = * \\ & * & * & * & = * \\ & & * & * & = * \\ & & & * & = * \end{array} \right.$$

- *Polynomial ring:* Buchberger's algorithm \longrightarrow Gröbner basis

F5

Gröbner bases: review

Rough idea

Signatures

Predicting zero
reductions

The algorithm

Implementation

Why?

Where?

Two variants

Termination (?)

The difficulty

Faugère's original
argument

Non-terminating
example... terminates!

Variants that guarantee
termination

Gröbner bases?

Gröbner basis: “nice form” for generators of polynomial ideal

- “*nice*”: ~~difficult~~ ^{easy!} questions

(B Buchberger, 1965)

Generalizes linear algebra

- *Vector space:* Gaussian elimination \longrightarrow echelon form

$$\left\{ \begin{array}{cccc|c} * & * & * & * & = * \\ * & * & * & * & = * \\ * & * & * & * & = * \\ * & * & * & * & = * \end{array} \right. \longrightarrow \left\{ \begin{array}{cccc|c} * & * & * & * & = * \\ & * & * & * & = * \\ & & * & * & = * \\ & & & * & = * \end{array} \right.$$

- *Polynomial ring:* Buchberger's algorithm \longrightarrow Gröbner basis

Buchberger's algorithm

Given $F \in \mathbb{F}[x_1, \dots, x_n]^m$:

- ① $G := F$
- ② Consider all $p, q \in G$
 - ① Compute $S := up - vq$
(u, p cancel lcm(ltp, ltq))
 - ② Top-reduce S over G
(divisibility of lts: $S - u_1g_1 - u_2g_2 - \dots$)
 - ③ $S = 0? \implies$ Append S to G
- ③ Termination: *no new polynomials* created
(Ascending Chain Condition)
 - All GB algorithms follow this general outline (F5 too!)
 - Omitting some details (lt=???)

F5

Gröbner bases: review

Rough idea

Signatures

Predicting zero
reductions

The algorithm

Implementation

Why?

Where?

Two variants

Termination (?)

The difficulty

Faugère's original
argument

Non-terminating
example... terminates!

Variants that guarantee
termination

Buchberger's algorithm

Given $F \in \mathbb{F}[x_1, \dots, x_n]^m$:

- 1 $G := F$
- 2 Consider all $p, q \in G$
 - 1 Compute $S := up - vq$
(u, p cancel $\text{lcm}(\text{lt}p, \text{lt}q)$)
 - 2 Top-reduce S over G
(divisibility of lts: $S - u_1g_1 - u_2g_2 - \dots$)
 - 3 $S = 0? \implies$ Append S to G
- 3 Termination: *no new polynomials* created
(Ascending Chain Condition)
 - All GB algorithms follow this general outline (F5 too!)
 - Omitting some details (lt=???)

F5

Gröbner bases: review

Rough idea

Signatures

Predicting zero
reductions

The algorithm

Implementation

Why?

Where?

Two variants

Termination (?)

The difficulty

Faugère's original
argument

Non-terminating
example... terminates!

Variants that guarantee
termination

Buchberger's algorithm

Given $F \in \mathbb{F}[x_1, \dots, x_n]^m$:

- 1 $G := F$
- 2 Consider all $p, q \in G$
 - 1 Compute $S := up - vq$
(u, p cancel $\text{lcm}(\text{lt}p, \text{lt}q)$)
 - 2 Top-reduce S over G
(divisibility of lts: $S - u_1g_1 - u_2g_2 - \dots$)
 - 3 $S = 0? \implies$ Append S to G
- 3 Termination: *no new polynomials created*
(Ascending Chain Condition)

- All GB algorithms follow this general outline (F5 too!)
- Omitting some details (lt=???)

F5

Gröbner bases: review

Rough idea

Signatures

Predicting zero
reductions

The algorithm

Implementation

Why?

Where?

Two variants

Termination (?)

The difficulty

Faugère's original
argument

Non-terminating
example... terminates!

Variants that guarantee
termination

Buchberger's algorithm

Given $F \in \mathbb{F}[x_1, \dots, x_n]^m$:

- ① $G := F$
- ② Consider all $p, q \in G$
 - ① Compute $S := up - vq$
(u, p cancel $\text{lcm}(\text{lt}p, \text{lt}q)$)
 - ② Top-reduce S over G
(divisibility of lts: $S - u_1g_1 - u_2g_2 - \dots$)
 - ③ $S = 0? \implies$ Append S to G
- ③ Termination: *no new polynomials created*
(Ascending Chain Condition)
 - All GB algorithms follow this general outline (F5 too!)
 - Omitting some details ($\text{lt}=?\text{?}\text{?}$)

F5

Gröbner bases: review

Rough idea

Signatures

Predicting zero
reductions

The algorithm

Implementation

Why?

Where?

Two variants

Termination (?)

The difficulty

Faugère's original
argument

Non-terminating
example... terminates!

Variants that guarantee
termination

Quick example

Problem: Find Gröbner basis of $\langle xy + 1, y^2 + 1 \rangle$.

① $G = (xy + 1, y^2 + 1)$

① $S = y(xy + 1) - x(y^2 + 1) = y - x$
No top-reduction

② $G = (xy + 1, y^2 + 1, x - y)$

① $S = (xy + 1) - y(x - y) = 1 + y^2$
Top-reduces to zero

② $S = x(y^2 + 1) - y^2(x - y) = x + y^3$
Top-reduces to zero

F5

Gröbner bases: review

Rough idea

Signatures

Predicting zero
reductions

The algorithm

Implementation

Why?

Where?

Two variants

Termination (?)

The difficulty

Faugère's original
argument

Non-terminating
example... terminates!

Variants that guarantee
termination

Quick example

Problem: Find Gröbner basis of $\langle xy + 1, y^2 + 1 \rangle$.

$$\textcircled{1} G = (xy + 1, y^2 + 1)$$

$$\textcircled{1} S = y(xy + 1) - x(y^2 + 1) = y - x$$

No top-reduction

$$\textcircled{2} G = (xy + 1, y^2 + 1, x - y)$$

$$\textcircled{1} S = (xy + 1) - y(x - y) = 1 + y^2$$

Top-reduces to zero

$$\textcircled{2} S = x(y^2 + 1) - y^2(x - y) = x + y^3$$

Top-reduces to zero

F5

Gröbner bases: review

Rough idea

Signatures

Predicting zero
reductions

The algorithm

Implementation

Why?

Where?

Two variants

Termination (?)

The difficulty

Faugère's original
argument

Non-terminating
example... terminates!

Variants that guarantee
termination

Quick example

Problem: Find Gröbner basis of $\langle xy + 1, y^2 + 1 \rangle$.

$$\textcircled{1} \quad G = (xy + 1, y^2 + 1)$$

$$\textcircled{1} \quad S = y(xy + 1) - x(y^2 + 1) = y - x$$

No top-reduction

$$\textcircled{2} \quad G = (xy + 1, y^2 + 1, x - y)$$

$$\textcircled{1} \quad S = (xy + 1) - y(x - y) = 1 + y^2$$

Top-reduces to zero

$$\textcircled{2} \quad S = x(y^2 + 1) - y^2(x - y) = x + y^3$$

Top-reduces to zero

F5

Gröbner bases: review

Rough idea

Signatures

Predicting zero
reductions

The algorithm

Implementation

Why?

Where?

Two variants

Termination (?)

The difficulty

Faugère's original
argument

Non-terminating
example... terminates!

Variants that guarantee
termination

Quick example

Problem: Find Gröbner basis of $\langle xy + 1, y^2 + 1 \rangle$.

$$\textcircled{1} G = (xy + 1, y^2 + 1)$$

$$\textcircled{1} S = y(xy + 1) - x(y^2 + 1) = y - x$$

No top-reduction

$$\textcircled{2} G = (xy + 1, y^2 + 1, x - y)$$

$$\textcircled{1} S = (xy + 1) - y(x - y) = 1 + y^2$$

Top-reduces to zero

$$\textcircled{2} S = x(y^2 + 1) - y^2(x - y) = x + y^3$$

Top-reduces to zero

$$\therefore \text{GB}(\langle xy + 1, y^2 + 1 \rangle) = (xy + 1, y^2 + 1, x - y).$$

F5

Gröbner bases: review

Rough idea

Signatures

Predicting zero
reductions

The algorithm

Implementation

Why?

Where?

Two variants

Termination (?)

The difficulty

Faugère's original
argument

Non-terminating
example... terminates!

Variants that guarantee
termination

- Bottleneck

- New polynomials \rightarrow new information
 - Top-reduction to zero \nrightarrow no new polynomial
- \nrightarrow new information
- $(100 - \epsilon)\%$ of time: verifying GB, *not* computing
 - Top-reduction *very, very expensive*

F5

Gröbner bases: review

Rough idea

Signatures

Predicting zero
reductions

The algorithm

Implementation

Why?

Where?

Two variants

Termination (?)

The difficulty

Faugère's original
argument

Non-terminating
example... terminates!

Variants that guarantee
termination

Past work

- *Predict zero reductions*
(B Buchberger 1985, R Gebauer-H Möller 1988,
CKR 2002, H Hong-J Perry 2007)
- *Selection strategy*: Pick pairs in clever ways
(B Buchberger 1985, A Giovini et al 1991,
H Möller et al 1992)
- *Forbid some top-reductions*: Involutive bases
(V Gerdt-Y Blinkov 1998)
- *Homogenization*: d -Gröbner bases

F5

Gröbner bases: review

Rough idea

Signatures

Predicting zero
reductions

The algorithm

Implementation

Why?

Where?

Two variants

Termination (?)

The difficulty

Faugère's original
argument

Non-terminating
example... terminates!

Variants that guarantee
termination

① F5

Gröbner bases: review

Rough idea

Signatures

Predicting zero reductions

The algorithm

② Implementation

Why?

Where?

Two variants

③ Termination (?)

The difficulty

Faugère's original argument

Non-terminating example... terminates!

Variants that guarantee termination

F_5 : combined approach

- Homogenize
- d -Gröbner bases
- New point of view:
 - New way to predict zero reductions
 - New selection strategy
- Some systems: *no zero reductions!*

“A new efficient algorithm for computing Gröbner bases
without reduction to zero (F_5)”

F_5

Gröbner bases: review

Rough idea

Signatures

Predicting zero
reductions

The algorithm

Implementation

Why?

Where?

Two variants

Termination (?)

The difficulty

Faugère's original
argument

Non-terminating
example... terminates!

Variants that guarantee
termination

View from linear algebra

- Compute GB \iff Triangularize Sylvester matrix of G
(D Lazard, 1983)
- Triangularize sparse matrix (F4)
(Faugère, 1999)
- Avoid using different rows to re-compute reductions
(Faugère, 2002)

F5

Gröbner bases: review

Rough idea

Signatures

Predicting zero
reductions

The algorithm

Implementation

Why?

Where?

Two variants

Termination (?)

The difficulty

Faugère's original
argument

Non-terminating
example... terminates!

Variants that guarantee
termination

Quick example, revisited

Problem: Find Gröbner basis of $\langle xy + 1, y^2 + 1 \rangle$.

Homogenize: $G = \langle xy + b^2, y^2 + b^2 \rangle$

F5

Gröbner bases: review

Rough idea

Signatures

Predicting zero
reductions

The algorithm

Implementation

Why?

Where?

Two variants

Termination (?)

The difficulty

Faugère's original
argument

Non-terminating
example... terminates!

Variants that guarantee
termination

Quick example, revisited

Problem: Find Gröbner basis of $\langle xy + 1, y^2 + 1 \rangle$.

Homogenize: $G = (xy + b^2, y^2 + b^2)$

$d = 2$:

No cancellations of degree 2...

F5

Gröbner bases: review

Rough idea

Signatures

Predicting zero
reductions

The algorithm

Implementation

Why?

Where?

Two variants

Termination (?)

The difficulty

Faugère's original
argument

Non-terminating
example... terminates!

Variants that guarantee
termination

Quick example, revisited

Problem: Find Gröbner basis of $\langle xy + 1, y^2 + 1 \rangle$.

Homogenize: $G = (xy + b^2, y^2 + b^2)$

$d = 3$:

$$\begin{pmatrix} x^2y & xy^2 & y^3 & xb^2 & yb^2 & \\ & 1 & & 1 & & xg_1 \\ & & 1 & & 1 & yg_1 \\ & & 1 & 1 & & xg_2 \\ & & & 1 & 1 & yg_2 \end{pmatrix}$$

Rows 2, 3 cancel...

F5

Gröbner bases: review

Rough idea

Signatures

Predicting zero
reductions

The algorithm

Implementation

Why?

Where?

Two variants

Termination (?)

The difficulty

Faugère's original
argument

Non-terminating
example... terminates!

Variants that guarantee
termination

Quick example, revisited

Problem: Find Gröbner basis of $\langle xy + 1, y^2 + 1 \rangle$.

Homogenize: $G = (xy + b^2, y^2 + b^2)$

$d = 3$:

$$\begin{pmatrix} x^2y & xy^2 & y^3 & xb^2 & yb^2 & \\ & 1 & & 1 & & xg_1 \\ & & 1 & & 1 & yg_1 \\ & & 1 & 1 & & xg_2 \\ & & & 1 & 1 & yg_2 \\ & & & & 1 & -1 \\ & & & & & g_3 \end{pmatrix}$$

New! $g_3 = xb^2 - yb^2$

F5

Gröbner bases: review

Rough idea

Signatures

Predicting zero
reductions

The algorithm

Implementation

Why?

Where?

Two variants

Termination (?)

The difficulty

Faugère's original
argument

Non-terminating
example... terminates!

Variants that guarantee
termination

Quick example, revisited

Problem: Find Gröbner basis of $\langle xy + 1, y^2 + 1 \rangle$.

Homogenize: $G = (xy + b^2, y^2 + b^2)$

$d = 3$:

$$\begin{pmatrix} x^2y & xy^2 & y^3 & xb^2 & yb^2 & \\ & 1 & & 1 & & xg_1 \\ & & 1 & & 1 & yg_1 \\ & & \cancel{x} & & \cancel{x} & \cancel{xg_2} \xrightarrow{g_3} \\ & & & 1 & & yg_2 \\ & & & & 1 & -1 \\ & & & & & g_3 \end{pmatrix}$$

linear dependence: $\cancel{xg_2} \xrightarrow{g_3}$

$$(xg_2 = g_3 + yg_1)$$

F5

Gröbner bases: review

Rough idea

Signatures

Predicting zero
reductions

The algorithm

Implementation

Why?

Where?

Two variants

Termination (?)

The difficulty

Faugère's original
argument

Non-terminating
example... terminates!

Variants that guarantee
termination

Quick example, revisited

Problem: Find Gröbner basis of $\langle xy + 1, y^2 + 1 \rangle$.

Homogenize: $G = (xy + b^2, y^2 + b^2)$

$d = 4$:

$$\begin{pmatrix} x^3y & x^2y^2 & xy^3 & y^4 & x^2b^2 & xyb^2 & y^2b^2 & b^4 & \\ & 1 & & & & 1 & & & x^2g_1 \\ & & 1 & & & & 1 & & xyg_1 \\ & & & 1 & & & & 1 & y^2g_1 \\ & & & & & 1 & & & 1 & b^2g_1 \\ & & & & 1 & & & & & 1 & y^2g_2 \\ & & & & & 1 & -1 & & & & xg_3 \\ & & & & & & 1 & -1 & & & yg_3 \end{pmatrix}$$

Rows 4, 7 cancel... **but we will not consider them!**

Why not?

Later.

F5

Gröbner bases: review

Rough idea

Signatures

Predicting zero
reductions

The algorithm

Implementation

Why?

Where?

Two variants

Termination (?)

The difficulty

Faugère's original
argument

Non-terminating
example... terminates!

Variants that guarantee
termination

Outline

1 F5

Gröbner bases: review

Rough idea

Signatures

Predicting zero reductions

The algorithm

2 Implementation

Why?

Where?

Two variants

3 Termination (?)

The difficulty

Faugère's original argument

Non-terminating example... terminates!

Variants that guarantee termination

Signatures: Observations

- $\text{Sig}(p) = tg_i?$
 - $1 \leq i \leq m$ (inputs: (g_1, \dots, g_m))
 - $g = h_1g_1 + \dots + h_{i-1}g_{i-1} + (t + \dots)g_i$ ($\exists h_1, \dots, h_i, \text{lt}(h_i) = t$)
- this definition = algorithmic behavior
 \neq Faugère's definition
- “easy” record-keeping: list of rules
- “easily” reject certain useless pairs:
 - Use yg_3 w/sig xyg_2 , not xyg_2
 - Use xg_3 w/sig x^2g_2 , not x^2g_2
 - ...
- Criterion “Rewritten”

(J-C Faugère 2007?, J Gash 2008,
C Eder-J Perry submitted)

Signatures: Observations

- $\text{Sig}(p) = tg_i?$
 - $1 \leq i \leq m$ (inputs: (g_1, \dots, g_m))
 - $g = h_1g_1 + \dots + h_{i-1}g_{i-1} + (t + \dots)g_i$ ($\exists h_1, \dots, h_i, \text{lt}(h_i) = t$)
- this definition = algorithmic behavior
 \neq Faugère's definition
- “easy” record-keeping: list of rules
- “easily” reject certain useless pairs:
 - Use yg_3 w/sig xyg_2 , not xyg_2
 - Use xg_3 w/sig x^2g_2 , not x^2g_2
 - ...
- Criterion “Rewritten”

(J-C Faugère 2007?, J Gash 2008,
C Eder-J Perry submitted)

Faugère's characterization

Theorem (Faugère, 2002)

$$(A) \iff (B) \text{ where}$$

(A) G a Gröbner basis

(B) $\forall p, q \in G$ where

- $u\text{Sig}(p), v\text{Sig}(q)$ not rewritable, and
- $u\text{Sig}(p), v\text{Sig}(q)$ minimal

S -polynomial $up - vq$ top-reduces to zero w/out changing signature

(highly paraphrased, slightly generalized)

F5

Gröbner bases: review

Rough idea

Signatures

**Predicting zero
reductions**

The algorithm

Implementation

Why?

Where?

Two variants

Termination (?)

The difficulty

Faugère's original
argument

Non-terminating
example... terminates!

Variants that guarantee
termination

1 F5

Gröbner bases: review

Rough idea

Signatures

Predicting zero reductions

The algorithm

2 Implementation

Why?

Where?

Two variants

3 Termination (?)

The difficulty

Faugère's original argument

Non-terminating example... terminates!

Variants that guarantee termination

How to predict zero reductions?

- Recall

$$\left(\begin{array}{cccccccc} x^3y & x^2y^2 & xy^3 & y^4 & x^2b^2 & xyb^2 & y^2b^2 & b^4 & & \\ & & & & & & & & & \vdots \\ & & & & & & 1 & & -1 & b^2g_1 \\ & & & & & & & & & \vdots \\ & & & & & & 1 & -1 & & yg_3 \end{array} \right)$$

We did not cancel. *Why not?*

- S*-poly top-reduces to zero
- can predict this*

How?

How to predict zero reductions?

- Recall

$$\left(\begin{array}{cccccccc} x^3y & x^2y^2 & xy^3 & y^4 & x^2b^2 & xyb^2 & y^2b^2 & b^4 & & \\ & & & & & & & & & \vdots \\ & & & & & & 1 & & -1 & b^2g_1 \\ & & & & & & & & & \vdots \\ & & & & & & 1 & -1 & & yg_3 \end{array} \right)$$

We did not cancel. *Why not?*

- S -poly top-reduces to zero
- can predict this*

How?

F5

Gröbner bases: review

Rough idea

Signatures

Predicting zero
reductions

The algorithm

Implementation

Why?

Where?

Two variants

Termination (?)

The difficulty

Faugère's original
argument

Non-terminating
example... terminates!

Variants that guarantee
termination

Faugère's criterion

Theorem

If

- $u\text{Sig}(p) = ug_i$; and
- $\text{lt}(q) \mid u, \exists q \in \text{GB}_{\text{prev}}(g_1, \dots, g_{i-1})$;

then $u\text{Sig}(p)$ is not minimal.

Definition

$FC(u\text{Sig}(p))$: $\text{lt}(q) \mid u \exists q \in G_{\text{prev}}$

Corollary

*In S -polynomial $up - vq$,
if $FC(u\text{Sig}(p))$ or $FC(v\text{Sig}(q))$
then we need not compute S .*

Faugère's criterion

Theorem

If

- $u\text{Sig}(p) = ug_i$; and
- $\text{lt}(q) \mid u, \exists q \in \text{GB}_{\text{prev}}(g_1, \dots, g_{i-1})$;

then $u\text{Sig}(p)$ is not minimal.

Definition

$FC(u\text{Sig}(p))$: $\text{lt}(q) \mid u \exists q \in G_{\text{prev}}$

Corollary

*In S -polynomial $up - vq$,
if $FC(u\text{Sig}(p))$ or $FC(v\text{Sig}(q))$
then we need not compute S .*

In the example...

- Recall

$$\left(\begin{array}{cccccccc} x^3y & x^2y^2 & xy^3 & y^4 & x^2b^2 & xyb^2 & y^2b^2 & b^4 & & \\ & & & & & & & & & \vdots \\ & & & & & 1 & & -1 & b^2g_1 & \\ & & & & & & & & & \vdots \\ & & & & & 1 & -1 & & yg_3 & \end{array} \right)$$

- $G_{\text{prev}} = (g_1)$

- $\text{Sig}(g_3) = xg_2$

- $y\text{Sig}(g_3) = xyg_2$, and $\text{lt}(g_1) \mid xy\dots$

FC \implies no need to compute S-polynomial

Why?

In the example...

- Recall

$$\left(\begin{array}{cccccccc} x^3y & x^2y^2 & xy^3 & y^4 & x^2b^2 & xyb^2 & y^2b^2 & b^4 & & \\ & & & & & & & & & \vdots \\ & & & & & & 1 & & -1 & b^2g_1 \\ & & & & & & & & & \vdots \\ & & & & & & 1 & -1 & & yg_3 \end{array} \right)$$

- $G_{\text{prev}} = (g_1)$
- $\text{Sig}(g_3) = xg_2$
- $y\text{Sig}(g_3) = xyg_2$, and $\text{lt}(g_1) \mid xy\dots$

FC \implies no need to compute S-polynomial

Why?

F5

Gröbner bases: review

Rough idea

Signatures

**Predicting zero
reductions**

The algorithm

Implementation

Why?

Where?

Two variants

Termination (?)

The difficulty

Faugère's original
argument

Non-terminating
example... terminates!

Variants that guarantee
termination

Why? Trivial syzygies

Recall $\gamma g_3 = \gamma [xg_2 - \gamma g_1] \dots$

F5

Gröbner bases: review

Rough idea

Signatures

**Predicting zero
reductions**

The algorithm

Implementation

Why?

Where?

Two variants

Termination (?)

The difficulty

Faugère's original
argument

Non-terminating
example... terminates!

Variants that guarantee
termination

Why? Trivial syzygies

Recall $\gamma g_3 = \gamma [xg_2 - \gamma g_1] \dots$

$$\begin{aligned} \therefore \gamma g_3 &= \gamma [xg_2 - \gamma g_1] \\ &= x\gamma g_2 - \gamma^2 g_1 \end{aligned}$$

F5

Gröbner bases: review

Rough idea

Signatures

**Predicting zero
reductions**

The algorithm

Implementation

Why?

Where?

Two variants

Termination (?)

The difficulty

Faugère's original
argument

Non-terminating
example... terminates!

Variants that guarantee
termination

Why? Trivial syzygies

Recall $\gamma g_3 = \gamma [xg_2 - \gamma g_1] \dots$

$$\begin{aligned} \therefore \gamma g_3 &= \gamma [xg_2 - \gamma g_1] \\ &= x\gamma g_2 - \gamma^2 g_1 \end{aligned}$$

Trivially $g_1 g_2 - g_2 g_1 = 0$.

Why? Trivial syzygies

Recall $\gamma g_3 = \gamma [xg_2 - \gamma g_1] \dots$

$$\begin{aligned} \therefore \gamma g_3 &= \gamma [xg_2 - \gamma g_1] \\ &= x\gamma g_2 - \gamma^2 g_1 \end{aligned}$$

Trivially $g_1 g_2 - g_2 g_1 = 0$.

$$\begin{aligned} \therefore \gamma g_3 &= x\gamma g_2 - \gamma^2 g_1 \\ &\quad - \left[(xy + b^2) g_2 - (y^2 + b^2) g_1 \right] \\ &= -b^2 g_2 + b^2 g_1 \end{aligned}$$

F5

Gröbner bases: review

Rough idea

Signatures

Predicting zero
reductions

The algorithm

Implementation

Why?

Where?

Two variants

Termination (?)

The difficulty

Faugère's original
argument

Non-terminating
example... terminates!

Variants that guarantee
termination

Why? Trivial syzygies

Recall $\gamma g_3 = \gamma [xg_2 - \gamma g_1] \dots$

$$\begin{aligned}\therefore \gamma g_3 &= \gamma [xg_2 - \gamma g_1] \\ &= x\gamma g_2 - \gamma^2 g_1\end{aligned}$$

Trivially $g_1 g_2 - g_2 g_1 = 0$.

$$\begin{aligned}\therefore \gamma g_3 &= x\gamma g_2 - \gamma^2 g_1 \\ &\quad - \left[(xy + b^2) g_2 - (y^2 + b^2) g_1 \right] \\ &= -b^2 g_2 + b^2 g_1\end{aligned}$$

$\text{Sig}(\gamma g_3)$ not minimal!

F5

Gröbner bases: review

Rough idea

Signatures

Predicting zero
reductions

The algorithm

Implementation

Why?

Where?

Two variants

Termination (?)

The difficulty

Faugère's original
argument

Non-terminating
example... terminates!

Variants that guarantee
termination

F5

Gröbner bases: review

Rough idea

Signatures

Predicting zero
reductions

The algorithm

Implementation

Why?

Where?

Two variants

Termination (?)

The difficulty

Faugère's original
argument

Non-terminating
example... terminates!

Variants that guarantee
termination

Outline

1 F5

Gröbner bases: review

Rough idea

Signatures

Predicting zero reductions

The algorithm

2 Implementation

Why?

Where?

Two variants

3 Termination (?)

The difficulty

Faugère's original argument

Non-terminating example... terminates!

Variants that guarantee termination

The F5 Algorithm

① Each stage: Incremental strategy

- ① Compute $\text{GB}(g_1)$
- ② Compute $\text{GB}(g_1, g_2)$
- ③ ...

② d -GB's \rightsquigarrow $\text{GB}(g_1, \dots, g_i)$

③ only S -polys with

- signatures that do not satisfy (FC); *and*
- non-rewritable components.

④ Top-reduce, but not if reduction...

- ① satisfies (FC); *or*
- ② rewritable.

⑤ Track new polys with signature

The F5 Algorithm

- 1 Each stage: Incremental strategy
 - 1 Compute $\text{GB}(g_1)$
 - 2 Compute $\text{GB}(g_1, g_2)$
 - 3 ...
- 2 d -GB's \rightsquigarrow $\text{GB}(g_1, \dots, g_i)$
- 3 only S -polys with
 - signatures that do not satisfy (FC); *and*
 - non-rewritable components.
- 4 Top-reduce, but not if reduction...
 - 1 satisfies (FC); *or*
 - 2 rewritable.
- 5 Track new polys with signature

The F5 Algorithm

- 1 Each stage: Incremental strategy
 - 1 Compute $\text{GB}(g_1)$
 - 2 Compute $\text{GB}(g_1, g_2)$
 - 3 ...
- 2 d -GB's \rightsquigarrow $\text{GB}(g_1, \dots, g_i)$
- 3 only S -polys with
 - signatures that do not satisfy (FC); *and*
 - non-rewritable components.
- 4 Top-reduce, but not if reduction...
 - 1 satisfies (FC); *or*
 - 2 rewritable.
- 5 Track new polys with signature

Certain details omitted...

Zero reductions?

Definition

If $G = (g_1, \dots, g_m)$ has trivial syzygies *only*,
then G is a **regular sequence**.

*Many systems are regular sequences;
many non-regular systems can be rewritten as regular.*

Corollary

*If input to F5 is a regular sequence,
then no zero reductions occur.*

Zero reductions?

Definition

If $G = (g_1, \dots, g_m)$ has trivial syzygies *only*,
then G is a **regular sequence**.

*Many systems are regular sequences;
many non-regular systems can be rewritten as regular.*

Corollary

*If input to F5 is a regular sequence,
then no zero reductions occur.*

F5

Gröbner bases: review

Rough idea

Signatures

Predicting zero
reductions

The algorithm

Implementation

Why?

Where?

Two variants

Termination (?)

The difficulty

Faugère's original
argument

Non-terminating
example... terminates!

Variants that guarantee
termination

Relation to Buchberger's criteria?

None.

- F5 needs to compute signatures
- Buchberger's criteria ignorant of signatures
- Mixing leads to non-termination
- (but see Gash, 2008)

F5

Gröbner bases: review

Rough idea

Signatures

Predicting zero
reductions

The algorithm

Implementation

Why?

Where?

Two variants

Termination (?)

The difficulty

Faugère's original
argument

Non-terminating
example... terminates!

Variants that guarantee
termination

Relation to Buchberger's criteria?

None.

- F5 needs to compute signatures
- Buchberger's criteria ignorant of signatures
- Mixing leads to non-termination
- (but see Gash, 2008)

F5

Gröbner bases: review

Rough idea

Signatures

Predicting zero
reductions

The algorithm

Implementation

Why?

Where?

Two variants

Termination (?)

The difficulty

Faugère's original
argument

Non-terminating
example... terminates!

Variants that guarantee
termination

① F5

Gröbner bases: review
Rough idea
Signatures
Predicting zero reductions
The algorithm

② Implementation

Why?
Where?
Two variants

③ Termination (?)

The difficulty
Faugère's original argument
Non-terminating example... terminates!
Variants that guarantee termination

F5

Gröbner bases: review

Rough idea

Signatures

Predicting zero
reductions

The algorithm

Implementation

Why?

Where?

Two variants

Termination (?)

The difficulty

Faugère's original
argument

Non-terminating
example... terminates!

Variants that guarantee
termination

Motivation

- little public code...
 - Stegers: Magma
 - I don't have Magma
 - I like Sage, can use Maple
 - FGb source code not public
- compare with other algorithms
 - selection strategy
 - predicting zero reduction
 - time/space tradeoff?

① F5

Gröbner bases: review
Rough idea
Signatures
Predicting zero reductions
The algorithm

② Implementation

Why?
Where?
Two variants

③ Termination (?)

The difficulty
Faugère's original argument
Non-terminating example... terminates!
Variants that guarantee termination

F5

Gröbner bases: review

Rough idea

Signatures

Predicting zero
reductions

The algorithm

Implementation

Why?

Where?

Two variants

Termination (?)

The difficulty

Faugère's original
argument

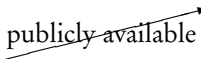
Non-terminating
example... terminates!

Variants that guarantee
termination

Implementations (1)

- Faugère (2002)
 - C, interfaces w/Maple
 - *Very* fast
 - Several variants: F5, F5', F5", ...?
 - Source code not publicly available, binary download
- Stegers (2005)
 - Interpreted Magma code
 - Respectable timings
 - Variant "F5R"
 - <http://wwwcsif.cs.ucdavis.edu/~stegers/>
- Others
 - Unstable implementations
 - Magma implementation?

Implementations (2)

- Perry (2007)
 - Interpreted Maple code
 - Embarassingly slow
 - Source code publicly available  unmaintained
- Eder, Perry (2008)
 - Interpreted Singular code
 - Respectable timings
 - New variant “F5C”
 - <http://www.math.usm.edu/perry/research.html>

Implementations (3)

- Albrecht (2008)
 - Interpreted Sage/Python code
 - Faster than Eder, Perry (2008)
 - Variants F5, F5R, F5C
 - http://bitbucket.org/malb/algebraic_attacks/
- King (2008)
 - Compiled Sage/Cython code
 - Faster than Eder, Perry (2008) and Albrecht (2008)?
 - Variant F5R; variants F5 and F5C by Perry
 - <http://www.math.usm.edu/perry/research.html>
- Eder (in progress)
 - *F5 in Singular kernel*
 - Access to many Singular optimizations
 - Sage uses Singular, so direct benefit to Sage
 - Source code will be publicly available

So you want to implement F5...

- Faugère's pseudocode:

`www-spaces.lip6.fr/@papers/F02a.pdf`

(2004 edition, corrected!)

- Stegers' pseudocode:

`wwwcsif.cs.ucdavis.edu/~stegers/`

(contains errors)

- Perry's pseudocode:

`www.math.usm.edu/perry/research.html`

(used for Singular, Sage implementations)

① F5

Gröbner bases: review
Rough idea
Signatures
Predicting zero reductions
The algorithm

② Implementation

Why?
Where?
Two variants

③ Termination (?)

The difficulty
Faugère's original argument
Non-terminating example... terminates!
Variants that guarantee termination

F5

Gröbner bases: review
Rough idea
Signatures
Predicting zero
reductions
The algorithm

Implementation

Why?
Where?
Two variants

Termination (?)

The difficulty
Faugère's original
argument
Non-terminating
example... terminates!
Variants that guarantee
termination

Reduced Gröbner basis

- Some inefficiency in F5
 - Not all top-reductions allowed
 - Redundant lt's added
 - Necessary this stage, but...
 - ... *not* next stages, *not* for GB
- *Reduced* Gröbner basis?
 - Pruning of redundant lt's
 - Well-known optimization
- “Naïve” F5 does not use RGB

F5

Gröbner bases: review

Rough idea

Signatures

Predicting zero
reductions

The algorithm

Implementation

Why?

Where?

Two variants

Termination (?)

The difficulty

Faugère's original
argument

Non-terminating
example... terminates!

Variants that guarantee
termination

Reduced Gröbner basis

- Some inefficiency in F5
 - Not all top-reductions allowed
 - Redundant lt's added
 - Necessary this stage, but...
 - ... *not* next stages, *not* for GB
- *Reduced* Gröbner basis?
 - Pruning of redundant lt's
 - Well-known optimization
- “Naïve” F5 does not use RGB

F5

Gröbner bases: review

Rough idea

Signatures

Predicting zero
reductions

The algorithm

Implementation

Why?

Where?

Two variants

Termination (?)

The difficulty

Faugère's original
argument

Non-terminating
example... terminates!

Variants that guarantee
termination

F5R (Stegers, 2006)

- Compute GB G of $\langle f_1, \dots, f_i \rangle$ (usual F5)
- Compute RGB B of $\langle G \rangle$ (easy: interreduce G)
- Compute GB of $\langle f_1, \dots, f_{i+1} \rangle$
 - Use G for critical pairs, B for top-reduction
- *Many* fewer reductions than F5, but...
- Same # polys considered, generated

F5

Gröbner bases: review

Rough idea

Signatures

Predicting zero
reductions

The algorithm

Implementation

Why?

Where?

Two variants

Termination (?)

The difficulty

Faugère's original
argument

Non-terminating
example... terminates!

Variants that guarantee
termination

F5C (Eder and Perry, 2008–2009)

- Compute GB G of $\langle f_1, \dots, f_i \rangle$ (usual F5)
- Compute RGB B of $\langle G \rangle$ (usual F5R)
- Compute GB of $\langle f_1, \dots, f_{i+1} \rangle$
 - Use B for top-reduction *and* for critical pairs
 - Modify rewrite rules
- Significantly fewer reductions than F5R, and...
- Fewer polys considered, generated

F5

Gröbner bases: review

Rough idea

Signatures

Predicting zero
reductions

The algorithm

Implementation

Why?

Where?

Two variants

Termination (?)

The difficulty

Faugère's original
argument

Non-terminating
example... terminates!

Variants that guarantee
termination

#Critical pairs, #Polynomials in variants

F5

Gröbner bases: review

Rough idea

Signatures

Predicting zero
reductions

The algorithm

Implementation

Why?

Where?

Two variants

Termination (?)

The difficulty

Faugère's original
argument

Non-terminating
example... terminates!

Variants that guarantee
termination

F5, F5R			F5C		
i	$\#G_{\text{curr}}$	$\max \{\#P_d\}$	i	$\#G_{\text{curr}}$	$\max \{\#P_d\}$
2	2	N/A	2	2	N/A
3	4	1	3	4	1
4	8	2	4	8	2
5	16	4	5	15	4
6	32	8	6	29	6
7	60	17	7	51	12
8	132	29	8	109	29
9	524	89	9	472	71
10	1165	276	10	778	89

#Reductions

variant:	F5	F5R	F5C
Katsura-5	346	289	222
Katsura-6	8,357	2,107	1,383
Katsura-7	1,025,408	24,719	10,000
Cyclic-5	441	457	415
Cyclic-6	36,139	17,512	10,970

(Top-reduction, normal forms)

(*Many* more in Gebauer-Möller: > 1,500,000 in Cyclic-6)

F5

Gröbner bases: review

Rough idea

Signatures

Predicting zero
reductions

The algorithm

Implementation

Why?

Where?

Two variants

Termination (?)

The difficulty

Faugère's original
argument

Non-terminating
example... terminates!

Variants that guarantee
termination

1 F5

Gröbner bases: review
Rough idea
Signatures
Predicting zero reductions
The algorithm

2 Implementation

Why?
Where?
Two variants

3 Termination (?)

The difficulty
Faugère's original argument
Non-terminating example... terminates!
Variants that guarantee termination

F5

Gröbner bases: review

Rough idea

Signatures

Predicting zero
reductions

The algorithm

Implementation

Why?

Where?

Two variants

Termination (?)

The difficulty

Faugère's original
argument

Non-terminating
example... terminates!

Variants that guarantee
termination

Termination: the difficulty

Termination?

- Buchberger: ACC \implies S -polys reduce to zero eventually
- Faugère: S -polys w/minimal signatures computed, *but...*

F5

Gröbner bases: review

Rough idea

Signatures

Predicting zero
reductions

The algorithm

Implementation

Why?

Where?

Two variants

Termination (?)

The difficulty

Faugère's original
argument

Non-terminating
example... terminates!

Variants that guarantee
termination

Termination: the difficulty

Termination?

- Buchberger: ACC \implies S -polys reduce to zero eventually
- Faugère: S -polys w/minimal signatures computed, *but...*
 - Some top-reductions forbidden
 - Regular system: no zero reductions
 - How recognize GB property?

F5

Gröbner bases: review

Rough idea

Signatures

Predicting zero
reductions

The algorithm

Implementation

Why?

Where?

Two variants

Termination (?)

The difficulty

Faugère's original
argument

Non-terminating
example... terminates!

Variants that guarantee
termination

① F5

Gröbner bases: review

Rough idea

Signatures

Predicting zero reductions

The algorithm

② Implementation

Why?

Where?

Two variants

③ Termination (?)

The difficulty

Faugère's original argument

Non-terminating example... terminates!

Variants that guarantee termination

F5

Gröbner bases: review

Rough idea

Signatures

Predicting zero
reductions

The algorithm

Implementation

Why?

Where?

Two variants

Termination (?)

The difficulty

**Faugère's original
argument**

Non-terminating
example... terminates!

Variants that guarantee
termination

Faugère's original argument

Theorem

*If reduction stage concludes without zero reductions,
then ideal of lt's has increased.*

Example

S-polynomial of $f_1 = xy + 1$, $f_2 = y^2 + 1$ did not reduce to zero;
new polynomial $x - y$;
new lt x !

F5

Gröbner bases: review

Rough idea

Signatures

Predicting zero
reductions

The algorithm

Implementation

Why?

Where?

Two variants

Termination (?)

The difficulty

Faugère's original
argument

Non-terminating
example... terminates!

Variants that guarantee
termination

Faugère's original argument

Theorem

*If reduction stage concludes without zero reductions,
then ideal of L_t 's has increased.*

This theorem is wrong.

Example (Gash, 2008)

- Uses Faugère's example (2002 paper)
- Consider S -polynomials in different order
- \rightsquigarrow no reduction to zero
and ideal of L_t 's does not increase.
- “redundant polynomials”

Redundant polynomials: necessary?

Why does F5 compute redundant polynomials?

- Some top-reductions forbidden
- Redundant polynomials restore necessary top-reductions

Example

- p_1 top-reducible by p_2 , but forbidden
- p_1 added to GB \rightsquigarrow new rewrite rule
- p_3 top-reducible by p_1 ? *now allowed*
- equivalent to top-reduction by p_2

Redundant polynomials: necessary?

Why does F5 compute redundant polynomials?

- Some top-reductions forbidden
- Redundant polynomials restore necessary top-reductions

Example

- p_1 top-reducible by p_2 , but forbidden
- p_1 added to GB \rightsquigarrow new rewrite rule
- p_3 top-reducible by p_1 ? *now allowed*
- equivalent to top-reduction by p_2

F5

Gröbner bases: review

Rough idea

Signatures

Predicting zero
reductions

The algorithm

Implementation

Why?

Where?

Two variants

Termination (?)

The difficulty

Faugère's original
argument

Non-terminating
example... terminates!

Variants that guarantee
termination

Possible resolution...?

An idea:

- Suppose reduction stage returns redundant polynomials
 - d -Gröbner basis!
- keep polys, but...
- not their S -polys
 - multiples of reducers' S -polynomials
- **Guaranteed termination!** *but...*
- No longer guaranteed correct!
 - Non-trivial concern: **Cyclic-7 oops!**
 - Rewrite rules \implies non-computed S -polys!

F5

Gröbner bases: review

Rough idea

Signatures

Predicting zero
reductions

The algorithm

Implementation

Why?

Where?

Two variants

Termination (?)

The difficulty

Faugère's original
argument

Non-terminating
example... terminates!

Variants that guarantee
termination

Possible resolution...?

An idea:

- Suppose reduction stage returns redundant polynomials
 - d -Gröbner basis!
- keep polys, but...
- not their S -polys
 - multiples of reducers' S -polynomials
- **Guaranteed termination!** *but...*
- No longer guaranteed correct!
 - Non-trivial concern: **Cyclic-7 oops!**
 - Rewrite rules \implies non-computed S -polys!

F5

Gröbner bases: review

Rough idea

Signatures

Predicting zero
reductions

The algorithm

Implementation

Why?

Where?

Two variants

Termination (?)

The difficulty

Faugère's original
argument

Non-terminating
example... terminates!

Variants that guarantee
termination

F5

Gröbner bases: review

Rough idea

Signatures

Predicting zero
reductions

The algorithm

Implementation

Why?

Where?

Two variants

Termination (?)

The difficulty

**Faugère's original
argument**

Non-terminating
example... terminates!

Variants that guarantee
termination

Regular case

- General agreement: termination
- Proof in Faugère's HDR? (2007)
- Another idea (J Gash, 2009)
 - Non-termination? chain of divisible lt's
 - Subchain of divisible signatures (ACC)
 - Cannot occur in regular case
 - Still working on this...

① F5

Gröbner bases: review

Rough idea

Signatures

Predicting zero reductions

The algorithm

② Implementation

Why?

Where?

Two variants

③ Termination (?)

The difficulty

Faugère's original argument

Non-terminating example... terminates!

Variants that guarantee termination

F5

Gröbner bases: review

Rough idea

Signatures

Predicting zero
reductions

The algorithm

Implementation

Why?

Where?

Two variants

Termination (?)

The difficulty

Faugère's original
argument

**Non-terminating
example... terminates!**

Variants that guarantee
termination

Non-terminating examples

- Widespread belief: F5 does not always terminate
- Proposals for non-terminating systems
 - Stegers' `nonTerminatingExample.mag`
 - Brickenstein's example
(private communication, exploit iterative computation)
- However...
 - Singular and Sage: *both* systems terminate

nonTerminatingExample.mag

Termination in Singular and Sage, not in Magma?!?

- Error in implementation
 - Rewrite rules sometimes not assigned
 - Some top-reductions not completed
- Correction \rightsquigarrow termination!

(R Dellaca-J Gash-J Perry, 2009)

F5

Gröbner bases: review

Rough idea

Signatures

Predicting zero
reductions

The algorithm

Implementation

Why?

Where?

Two variants

Termination (?)

The difficulty

Faugère's original
argument

**Non-terminating
example... terminates!**

Variants that guarantee
termination

1 F5

Gröbner bases: review

Rough idea

Signatures

Predicting zero reductions

The algorithm

2 Implementation

Why?

Where?

Two variants

3 Termination (?)

The difficulty

Faugère's original argument

Non-terminating example... terminates!

Variants that guarantee termination

F5

Gröbner bases: review

Rough idea

Signatures

Predicting zero
reductions

The algorithm

Implementation

Why?

Where?

Two variants

Termination (?)

The difficulty

Faugère's original
argument

Non-terminating
example... terminates!

Variants that guarantee
termination

Private communications

- Faugère, 2007 HDR: proof fixed
 - Regular sequences only?
 - Find me a copy?
- Zobnin, 2008: Restructured algorithm
 - Proceeds by increasing signature, other changes
 - Implementation?

F5

Gröbner bases: review

Rough idea

Signatures

Predicting zero
reductions

The algorithm

Implementation

Why?

Where?

Two variants

Termination (?)

The difficulty

Faugère's original
argument

Non-terminating
example... terminates!

**Variants that guarantee
termination**

Gash (2008 PhD Dissertation)

- Redundant polynomials \rightsquigarrow special bin D
- Test for GB: force carefully-chosen zero reductions
- If failure, add D to GB and proceed
- Loss of efficiency via zero reductions vs. guaranteed termination and correctness

F5

Gröbner bases: review

Rough idea

Signatures

Predicting zero
reductions

The algorithm

Implementation

Why?

Where?

Two variants

Termination (?)

The difficulty

Faugère's original
argument

Non-terminating
example... terminates!

**Variants that guarantee
termination**

Another solution?

Another idea: modified F5C

- Suppose reduction stage returns redundant polynomials
 - d -Gröbner basis!
- Immediately interreduce, discard *all* redundant polynomials
- Re-examine all pairs
 - S -polynomials of degree $\leq d$: good! new rewrite rule
 - S -polynomials of degree $> d$: bad! compute S -poly
- **WARNING:**

The above has not (yet) been proved or implemented.

F5

Gröbner bases: review

Rough idea

Signatures

Predicting zero
reductions

The algorithm

Implementation

Why?

Where?

Two variants

Termination (?)

The difficulty

Faugère's original
argument

Non-terminating
example... terminates!

**Variants that guarantee
termination**

Finis

Thank you!