A (short) survey on signature-based Gröbner Basis Algorithms

Christian Eder, Jean-Charles Faugère,
John Perry and Bjarke Hammersholt Roune

ACA 2014, New York, US

July 10, 2014

Technische Universität Kaiserslautern

How to detect zero reductions in advance?

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

$$\mathbf{g_1 = xy - z^2, \quad g_2 = y^2 - z^2}$$

How to detect zero reductions in advance?

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

$$\mathbf{g_1} = \mathbf{xy} - \mathbf{z^2}, \quad \mathbf{g_2} = \mathbf{y^2} - \mathbf{z^2}$$

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

$$\Longrightarrow \mathbf{g_3} = \mathbf{xz^2} - \mathbf{yz^2}.$$

How to detect zero reductions in advance?

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

$$\mathbf{g_1} = \mathbf{xy} - \mathbf{z^2}, \quad \mathbf{g_2} = \mathbf{y^2} - \mathbf{z^2}$$

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

$$\Longrightarrow \mathbf{g_3} = \mathbf{xz^2} - \mathbf{yz^2}.$$

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

How to detect zero reductions in advance?

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

$$\mathbf{g_1 = xy - z^2}, \quad \mathbf{g_2 = y^2 - z^2}$$

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

$$\Longrightarrow \mathbf{g_3 = xz^2 - yz^2}.$$

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

We can reduce further using $z^2 g_2$:

$$\boxed{-y^2z^2 + z^4 + y^2z^2 - z^4 = 0.}$$

Signatures

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

Signatures

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

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

Signatures

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

- Let R^m be generated by $e_1, \ldots, e_m$ and let $\prec$ be a compatible monomial order on the monomials of R^m.
- Let $\alpha \mapsto \overline{\alpha} : R^m \to R$ such that $\overline{e}_i = f_i$ for all i.

Signatures

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

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

- Let R^m be generated by $e_1, \ldots, e_m$ and let $\prec$ be a compatible monomial order on the monomials of R^m.
- Let $\alpha \mapsto \overline{\alpha} : R^m \to R$ such that $\overline{e}_i = f_i$ for all i.
- Each $f \in I$ can be represented via some $\alpha \in R^m$: $f = \overline{\alpha}$

Signatures

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

- Let R^m be generated by $e_1, \ldots, e_m$ and let $\prec$ be a compatible monomial order on the monomials of R^m.
- Let $\alpha \mapsto \overline{\alpha} : R^m \to R$ such that $\overline{e}_i = f_i$ for all i.
- Each $f \in I$ can be represented via some $\alpha \in R^m$: $f = \overline{\alpha}$
- **A signature** of f is given by $\mathfrak{s}(f) = \mathrm{lt}_{\prec}(\alpha)$ where $f = \overline{\alpha}$.

Signatures

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

- Let R^m be generated by $e_1, \ldots, e_m$ and let $\prec$ be a compatible monomial order on the monomials of R^m.
- Let $\alpha \mapsto \overline{\alpha} : R^m \to R$ such that $\overline{e}_i = f_i$ for all i.
- Each $f \in I$ can be represented via some $\alpha \in R^m$: $f = \overline{\alpha}$
- **A signature** of f is given by $\mathfrak{s}(f) = \mathrm{lt}_{\prec}(\alpha)$ where $f = \overline{\alpha}$.
- An element $\alpha \in \mathscr{R}^m$ with $\overline{\alpha} = 0$ is called **a syzygy**.

Our example again – with signatures and $\prec_{\textbf{pot}}$

$$g_1 = xy - z^2, \; \mathfrak{s}(g_1) = e_1,$$
$$g_2 = y^2 - z^2, \; \mathfrak{s}(g_2) = e_2.$$

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

$$g_1 = xy - z^2, \; \mathfrak{s}(g_1) = e_1,$$
$$g_2 = y^2 - z^2, \; \mathfrak{s}(g_2) = e_2.$$

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

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

$$g_1 = xy - z^2,\ \mathfrak{s}(g_1) = e_1,$$
$$g_2 = y^2 - z^2,\ \mathfrak{s}(g_2) = e_2.$$

$$g_3 = \mathrm{spol}(g_2, g_1) = xg_2 - yg_1$$
$$\Rightarrow \mathfrak{s}(g_3) = x\,\mathfrak{s}(g_2) = xe_2.$$

$$\mathrm{spol}(g_3, g_1) = yg_3 - z^2 g_1$$
$$\Rightarrow \mathfrak{s}\left(\mathrm{spol}(g_3, g_1)\right) = y\,\mathfrak{s}(g_3) = xye_2.$$

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

$$g_1 = xy - z^2,\ \mathfrak{s}(g_1) = e_1,$$
$$g_2 = y^2 - z^2,\ \mathfrak{s}(g_2) = e_2.$$

$$g_3 = \operatorname{spol}(g_2, g_1) = xg_2 - yg_1$$
$$\Rightarrow \mathfrak{s}(g_3) = x\,\mathfrak{s}(g_2) = xe_2.$$

$$\operatorname{spol}(g_3, g_1) = yg_3 - z^2 g_1$$
$$\Rightarrow \mathfrak{s}(\operatorname{spol}(g_3, g_1)) = y\,\mathfrak{s}(g_3) = xye_2.$$

Note that $\mathfrak{s}(\operatorname{spol}(g_3, g_1)) = xy\,e_2$ and $\operatorname{lm}(g_1) = xy$.

Think in the module

$\alpha \in R^m \implies$ polynomial $\overline{\alpha}$ with $\mathrm{lt}\left(\overline{\alpha}\right)$, signature $\mathfrak{s}(\alpha) = \mathrm{lt}\left(\alpha\right)$

Think in the module

$\alpha \in R^m \implies$ polynomial $\overline{\alpha}$ with $\operatorname{lt}(\overline{\alpha})$, signature $\mathfrak{s}(\alpha) = \operatorname{lt}(\alpha)$

S-pairs/S-polynomials:

$$\operatorname{spol}\left(\overline{\alpha}, \overline{\beta}\right) = a\overline{\alpha} - b\overline{\beta} \implies \operatorname{spair}(\alpha, \beta) = a\alpha - b\beta$$

Think in the module

$\alpha \in R^m \implies$ polynomial $\overline{\alpha}$ with $\operatorname{lt}(\overline{\alpha})$, signature $\mathfrak{s}(\alpha) = \operatorname{lt}(\alpha)$

S-pairs/S-polynomials:

$$\operatorname{spol}\left(\overline{\alpha}, \overline{\beta}\right) = a\overline{\alpha} - b\overline{\beta} \implies \operatorname{spair}(\alpha, \beta) = a\alpha - b\beta$$

$\mathfrak{s}$-reductions:

$$\overline{\gamma} - d\overline{\delta} \implies \gamma - d\delta$$

Think in the module

$\alpha \in R^m \implies$ polynomial $\overline{\alpha}$ with $\operatorname{lt}(\overline{\alpha})$, signature $\mathfrak{s}(\alpha) = \operatorname{lt}(\alpha)$

S-pairs/S-polynomials:

$$\operatorname{spol}\left(\overline{\alpha}, \overline{\beta}\right) = a\overline{\alpha} - b\overline{\beta} \implies \operatorname{spair}(\alpha, \beta) = a\alpha - b\beta$$

$\mathfrak{s}$-reductions:

$$\overline{\gamma} - d\overline{\delta} \implies \gamma - d\delta$$

Remark

In the following we need one detail from signature-based Gröbner Basis computations:

We pick from P by increasing signature.

Signature-based criteria

$\mathfrak{s}(\alpha) = \mathfrak{s}(\beta) \implies$ Compute 1, remove 1.

Signature-based criteria

$$\mathfrak{s}(\alpha) = \mathfrak{s}(\beta) \implies \text{Compute 1, remove 1.}$$

Sketch of proof

1. $\mathfrak{s}(\alpha - \beta) \prec \mathfrak{s}(\alpha), \mathfrak{s}(\beta)$.
2. All S-pairs are handled by increasing signature.
   $\Rightarrow$ All relatons $\prec \mathfrak{s}(\alpha)$ are known:

$$\alpha = \beta + \text{ elements of smaller signature}$$

$\square$

Signature-based criteria

S-pairs in signature T

Signature-based criteria

S-pairs in signature T

What are all possible configurations to reach signature T?

Signature-based criteria

S-pairs in signature T

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

What are all possible configurations to reach signature T?

Signature-based criteria

S-pairs in signature T

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

What are all possible configurations to reach signature T?

Define an order $\trianglelefteq$ on $\mathfrak{R}_T$ and choose the maximal element.

Special cases

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

Special cases

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

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

Special cases

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

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

1. If $b\beta$ is a syzygy $\Longrightarrow$ Go on to next signature.

Special cases

$$\mathfrak{R}_T = \left\{ a\alpha \;\middle|\; \alpha \text{ handled by the algorithm and } \mathfrak{s}(a\alpha) = T \right\}$$

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

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

Special cases

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

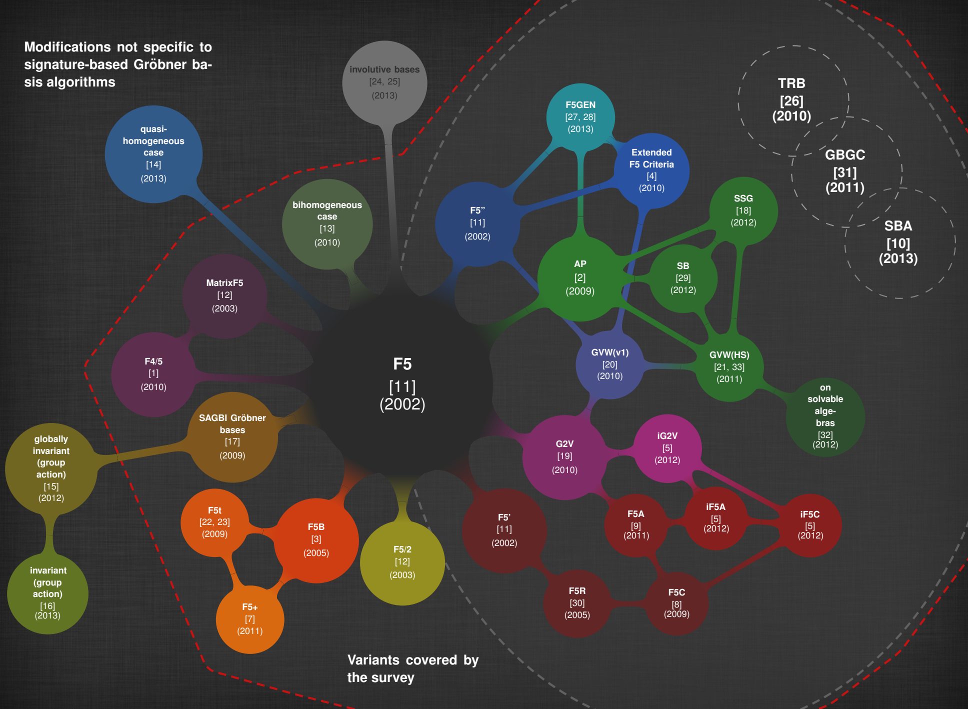
Choose $b\beta$ to be an element of $\mathfrak{R}_T$ maximal w.r.t. an order $\trianglelefteq$.

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

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

$$\mathfrak{s}\left(\text{spol}(g_3, g_1)\right) = xye_2$$

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


Modifications not specific to signature-based Gröbner basis algorithms
involutive bases [24, 25] (2013)
quasi-homogeneous case [14] (2013)
bihomogeneous case [13] (2010)
MatrixF5 [12] (2003)
F4/5 [1] (2010)
SAGBI Gröbner bases [17] (2009)
globally invariant (group action) [15] (2012)
invariant (group action) [16] (2013)
F5t [22, 23] (2009)
F5B [3] (2005)
F5+ [7] (2011)
F5/2 [12] (2003)
F5 [11] (2002)
F5GEN [27, 28] (2013)
Extended F5 Criteria [4] (2010)
F5” [11] (2002)
AP [2] (2009)
SSG [18] (2012)
SB [29] (2012)
GVW(v1) [20] (2010)
GVW(HS) [21, 33] (2011)
on solvable algebras [32] (2012)
G2V [19] (2010)
iG2V [5] (2012)
F5’ [11] (2002)
F5A [9] (2011)
iF5A [5] (2012)
iF5C [5] (2012)
F5R [30] (2005)
F5C [8] (2009)
TRB [26] (2010)
GBGC [31] (2011)
SBA [10] (2013)
Variants covered by the survey

Where are the differences?

There are three different choices you can make:

Where are the differences?

There are three different choices you can make:

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

Where are the differences?

There are three different choices you can make:

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

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

Where are the differences?

There are three different choices you can make:

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

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

3. Choose a rewrite order $\trianglelefteq$ on $\mathfrak{R}_T$ such that $\alpha \trianglelefteq \beta$:
Common choices:

- $\alpha \in \mathscr{G} \trianglelefteq \beta$ syzygy
- β added to $\mathscr{G}$ after α or $\mathfrak{s}(\alpha)\,\mathrm{lt}\left(\overline{\beta}\right) \prec \mathfrak{s}(\beta)\,\mathrm{lt}(\overline{\alpha})$.

Buchberger's criteria?

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

Buchberger's criteria?

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

Chain criterion is a special case of the Rewrite criterion
$\Rightarrow$ already included.

Buchberger's criteria?

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

Chain criterion is a special case of the Rewrite criterion
$\Rightarrow$ already included.

Product criterion is not always (but mostly) included.

Buchberger's criteria?

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

Chain criterion is a special case of the Rewrite criterion
$\Rightarrow$ already included.

Product criterion is not always (but mostly) included.

α added to $\mathscr{G}$

▼

Generate all possible principal syzygies with α.
(e.g. **GVW**)

Buchberger's criteria?

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

Chain criterion is a special case of the Rewrite criterion
$\Rightarrow$ already included.

Product criterion is not always (but mostly) included.

α added to $\mathscr{G}$

▼

Generate all possible principal syzygies with α.
(e.g. **GVW**)

S-pair fulfilling Product criterion not detected by Rewrite criterion

▼

Add one corresponding syzygy.
(e.g. **SB** in **Singular**)

References I

[1] Albrecht, M. and Perry, J. F4/5. `http://arxiv.org/abs/1006.4933`, 2010.

[2] Arri, A. and Perry, J. The F5 Criterion revised. *Journal of Symbolic Computation*, 46(2):1017–1029, June 2011. Preprint online at `arxiv.org/abs/1012.3664`.

[3] Ars, G. *Applications des bases de Gröbner à la cryptographie*. PhD thesis, Université de Rennes I, 2005.

[4] Ars, G. and Hashemi, A. Extended F5 Criteria. *Journal of Symbolic Computation, MEGA 2009 special issue*, 45(12):1330–1340, 2010.

[5] Eder, C. Improving incremental signature-based Groebner bases algorithms. *ACM SIGSAM Communications in Computer Algebra*, 47(1):1–13, 2013. `http://arxiv.org/abs/1201.6472`.

[6] Eder, C. and Faugère, J.-C. A survey on signature-based Groebner basis algorithms, 2014. `http://arxiv.org/abs/1404.1774`

[7] Eder, C., Gash, J., and Perry, J. Modifying Faugère's F5 Algorithm to ensure termination. *ACM SIGSAM Communications in Computer Algebra*, 45(2):70–89, 2011. `http://arxiv.org/abs/1006.0318`.

[8] Eder, C. and Perry, J. F5C: A Variant of Faugère's F5 Algorithm with reduced Gröbner bases. *Journal of Symbolic Computation, MEGA 2009 special issue*, 45(12):1442–1458, 2010. `dx.doi.org/10.1016/j.jsc.2010.06.019`.

References II

[9] Eder, C. and Perry, J. Signature-based Algorithms to Compute Gröbner Bases. In *ISSAC 2011: Proceedings of the 2011 international symposium on Symbolic and algebraic computation*, pages 99–106, 2011.

[10] Eder, C. and Roune, B. H. Signature Rewriting in Gröbner Basis Computation. In *ISSAC 2013: Proceedings of the 2013 international symposium on Symbolic and algebraic computation*, pages 331–338, 2013.

[11] Faugère, J.-C. A new efficient algorithm for computing Gröbner bases without reduction to zero F5. In *ISSAC'02, Villeneuve d'Ascq, France*, pages 75–82, July 2002. Revised version from `http://fgbrs.lip6.fr/jcf/Publications/index.html`.

[12] Faugère, J.-C. and Joux, A. Algebraic Cryptanalysis of Hidden Field Equation (HFE) Cryptosystems Using Gröbner Bases. 2729:44–60, 2003.

[13] Faugère, J.-C., Safey El Din, M., and Spaenlehauer, P.-J. Gröbner Bases of Bihomogeneous Ideals Generated by Polynomials of Bidegree (1,1): Algorithms and Complexity. *Journal of Symbolic Computation*, 46(4):406–437, 2011. Available online 4 November 2010.

[14] Faugère, J.-C., Safey El Din, M., and Verron, T. On the complexity of Computing Gröbner Bases for Quasi-homogeneous Systems. In *Proceedings of the 38th international symposium on International symposium on symbolic and algebraic computation*, ISSAC '13, pages 189–196, New York, NY, USA, 2013. ACM.

References III

[15] Faugère, J.-C. and Svartz, J. Solving polynomial systems globally invariant under an action of the symmetric group and application to the equilibria of n vertices in the plane. In *Proceedings of the 37th international symposium on International symposium on symbolic and algebraic computation*, ISSAC '12, pages 170–178, New York, NY, USA, 2012. ACM.

[16] Faugère, J.-C. and Svartz, J. Gröbner Bases of ideals invariant under a Commutative group : the Non-modular Case. In *Proceedings of the 38th international symposium on International symposium on symbolic and algebraic computation*, ISSAC '13, pages 347–354, New York, NY, USA, 2013. ACM.

[17] Faugère, J.-C. and Rahmany, S. Solving systems of polynomial equations with symmetries using SAGBI-Gröbner bases. In *ISSAC '09: Proceedings of the 2009 international symposium on Symbolic and algebraic computation*, ISSAC '09, pages 151–158, New York, NY, USA, 2009. ACM.

[18] Galkin, V. Simple signature-based Groebner basis algorithm. `http://arxiv.org/abs/1205.6050`, 2012.

[19] Gao, S., Guan, Y., and Volny IV, F. A new incremental algorithm for computing Gröbner bases. In *ISSAC '10: Proceedings of the 2010 international symposium on Symbolic and algebraic computation*, pages 13–19. ACM, 2010.

[20] Gao, S., Volny IV, F., and Wang, D. A new algorithm for computing Groebner bases. `http://eprint.iacr.org/2010/641`, 2010.

References IV

[21] Gao, S., Volny IV, F., and Wang, D. A new algorithm for computing Groebner bases (rev. 2011). `http://www.math.clemson.edu/~sgao/papers/gvw.pdf`, 2011.

[22] Gash, J. M. *On efficient computation of Gröbner bases*. PhD thesis, University of Indiana, Bloomington, IN, 2008.

[23] Gash, J. M. A provably terminating and speed-competitive variant of F5 – F5t. *submitted to the Journal of Symbolic Computation*, 2009.

[24] Gerdt, V. P. and Hashemi, A. On the use of Buchberger criteria in G2V algorithm for calculating Gröbner bases. *Program. Comput. Softw.*, 39(2):81–90, March 2013.

[25] Gerdt, V. P., Hashemi, A., and M.-Alizadeh, B. Involutive Bases Algorithm Incorporating F5 Criterion. *J. Symb. Comput.*, 59:1–20, 2013.

[26] Huang, L. A new conception for computing Gröbner basis and its applications. `http://arxiv.org/abs/1012.5425`, 2010.

[27] Pan, S., Hu, Y., and Wang, B. The Termination of Algorithms for Computing Gröbner Bases. `http://arxiv.org/abs/1202.3524`, 2012.

[28] Pan, S., Hu, Y., and Wang, B. The Termination of the F5 Algorithm Revisited. In *ISSAC 2013: Proceedings of the 2013 international symposium on Symbolic and algebraic computation*, pages 291–298, 2013.

References V

[29] Roune, B. H. and Stillman, M. Practical Gröbner Basis Computation. In *ISSAC 2012: Proceedings of the 2012 international symposium on Symbolic and algebraic computation*, 2012.

[30] Stegers, T. Faugère's F5 Algorithm revisited. Master's thesis, Technische Univeritat Darmstadt, revised version 2007.

[31] Sun, Y. and Wang, D. K. A generalized criterion for signature related Gröbner basis algorithms. In *ISSAC 2011: Proceedings of the 2011 international symposium on Symbolic and algebraic computation*, pages 337–344, 2011.

[32] Sun, Y., Wang, D. K., Ma, D. X., and Zhang, Y. A signature-based algorithm for computing Gröbner bases in solvable polynomial algebras. In *ISSAC 2012: Proceedings of the 2011 international symposium on Symbolic and algebraic computation*, pages 351–358, 2012.

[33] Volny, F. *New algorithms for computing Gröbner bases*. PhD thesis, Clemson University, 2011.