Signature-based Gröbner Basis Algorithms

Christian Eder, Jean-Charles Faugère and Bjarke Hammersholt Roune

4th annual meeting SPP1489
Bad Boll, Germany

March 04, 2013

Buchberger's algorithm

Input: Ideal $I = \langle f_1, \ldots, f_m \rangle$
Output: Gröbner basis G of I

1. $G = \emptyset$
2. $G := G \cup \{f_i\}$ for all $i \in \{1, \ldots, m\}$
3. Set $P := \{\text{spol}(f_i, f_j) \mid f_i, f_j \in G, i > j\}$

Buchberger's algorithm

Input: Ideal $I = \langle f_1, \ldots, f_m \rangle$
Output: Gröbner basis G of I

1. $G = \emptyset$
2. $G := G \cup \{f_i\}$ for all $i \in \{1, \ldots, m\}$
3. Set $P := \{\text{spol}(f_i, f_j) \mid f_i, f_j \in G, i > j\}$
4. Choose $p \in P$, $P := P \setminus \{p\}$

Buchberger's algorithm

Input: Ideal $I = \langle f_1, \ldots, f_m \rangle$
Output: Gröbner basis G of I

1. $G = \emptyset$
2. $G := G \cup \{f_i\}$ for all $i \in \{1, \ldots, m\}$
3. Set $P := \{\text{spol}(f_i, f_j) \mid f_i, f_j \in G, i > j\}$
4. Choose $p \in P$, $P := P \setminus \{p\}$
   (a) If $p \xrightarrow{G} 0$ ▶▶ **no new information**
   Go on with the next element in P.
   (b) If $p \xrightarrow{G} h \neq 0$ ▶▶ **new information**
   Build new S-pair with h and add them to P.
   Add h to G.
   Go on with the next element in P.
5. When $P = \emptyset$ we are done and G is a Gröbner basis of I.

Buchberger's algorithm

Input: Ideal $I = \langle f_1, \ldots, f_m \rangle$
Output: Gröbner basis G of I

1. $G = \emptyset$
2. $G := G \cup \{f_i\}$ for all $i \in \{1, \ldots, m\}$
3. Set $P := \{\mathrm{spol}(f_i, f_j) \mid f_i, f_j \in G, i > j\}$
4. Choose $p \in P$, $P := P \setminus \{p\}$
   (a) If $p \xrightarrow{G} 0$ ▶▶ **no new information**
   Go on with the next element in P.
   (b) If $p \xrightarrow{G} h \neq 0$ ▶▶ **new information**
   Build new S-pair with h and add them to P.
   Add h to G.
   Go on with the next element in P.
5. When $P = \emptyset$ we are done and G is a Gröbner basis of I.

How to predict zero reductions?

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:

1. 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:

1. 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.

2. 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:

1. 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.

2. Let $\alpha \mapsto \overline{\alpha} : R^m \to R$ such that $\overline{e}_i = f_i$ for all i.

3. 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:

1. 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.

2. Let $\alpha \mapsto \overline{\alpha} : R^m \to R$ such that $\overline{e}_i = f_i$ for all i.

3. Each $f \in I$ can be represented via some $\alpha \in R^m$: $f = \overline{\alpha}$

4. **A signature** of f is given by $\mathfrak{s}(f) = \mathrm{lt}_{\prec}(\alpha)$ where $f = \overline{\alpha}$.

How to use signatures?

General idea: Per signature we only need to compute 1 element for G.

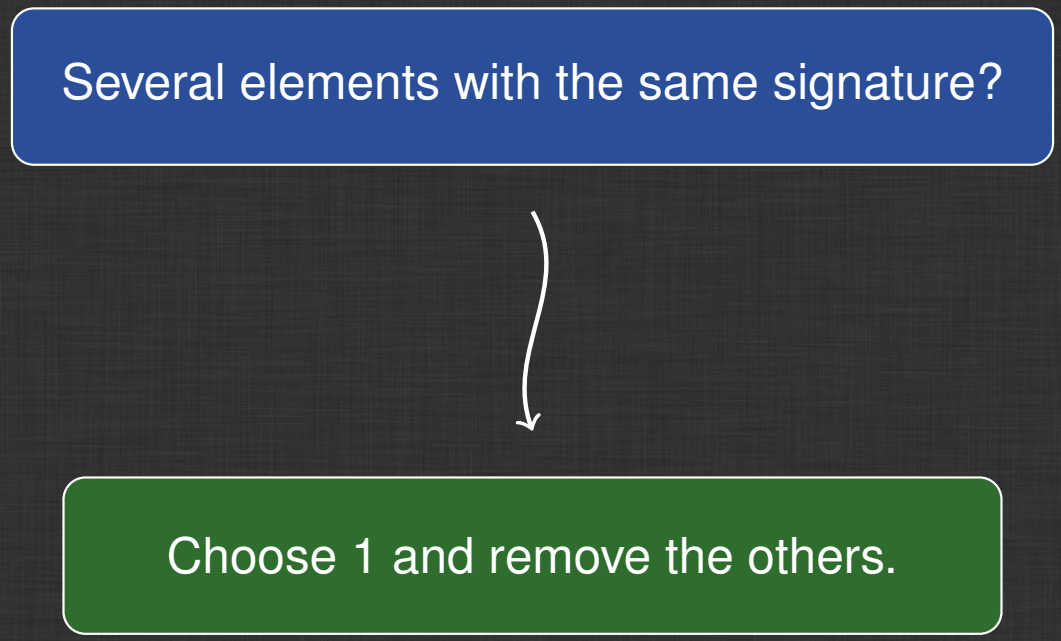
How to use signatures?

General idea: Per signature we only need to compute 1 element for G.

Several elements with the same signature?

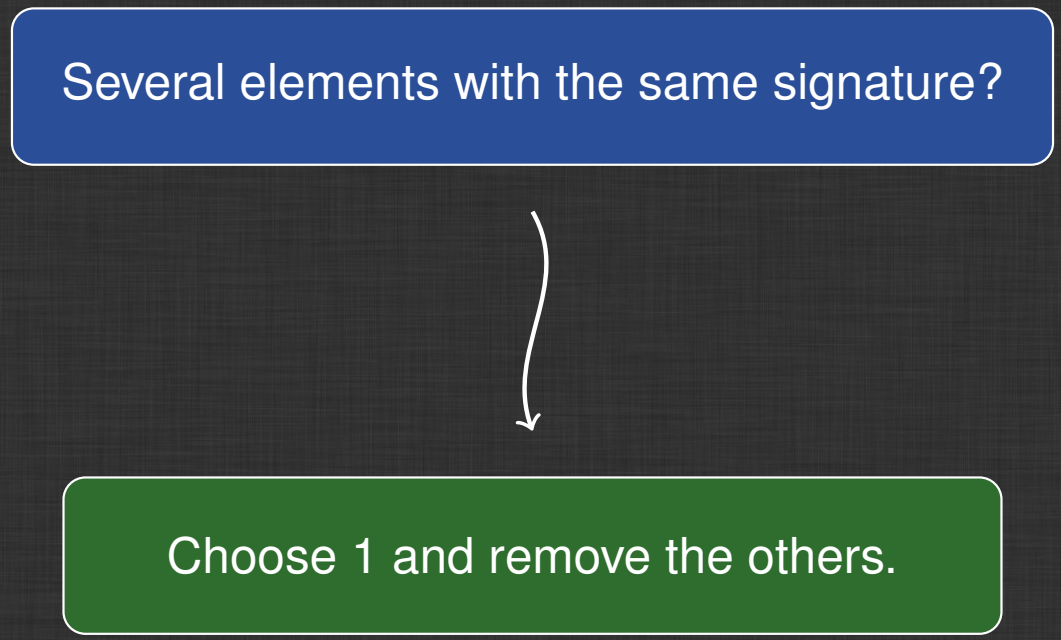
How to use signatures?

General idea: Per signature we only need to compute 1 element for G.



How to use signatures?

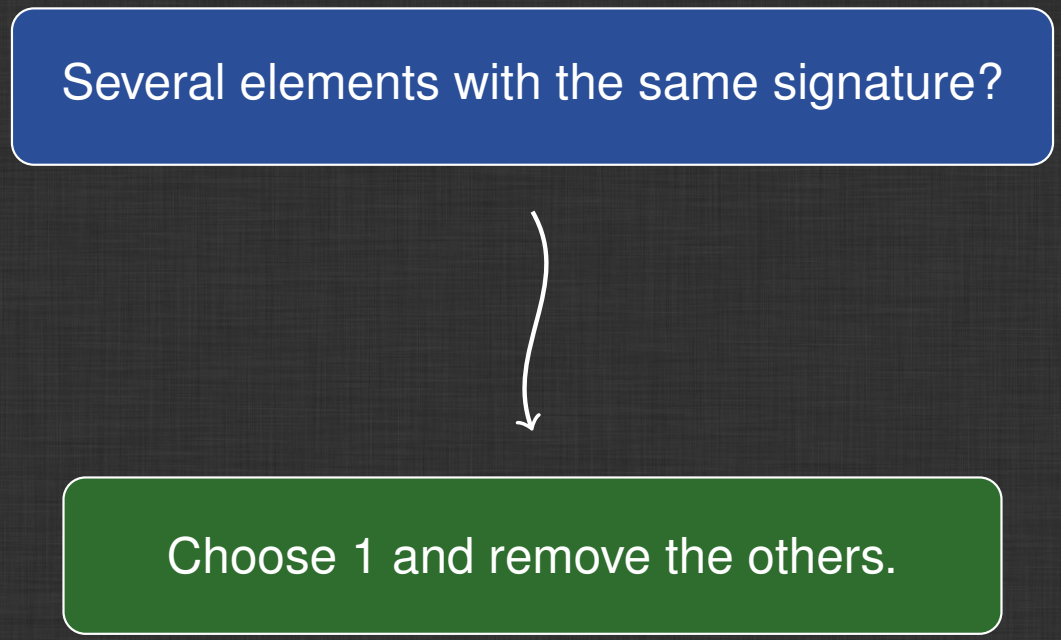
General idea: Per signature we only need to compute 1 element for G.



Our goal: Make good choices.

How to use signatures?

General idea: Per signature we only need to compute 1 element for G.



Our goal: Make good choices.

Our task: Keep signatures correct.

Think in the module

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

Think in the module

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

S-pairs/S-polynomials:

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

Think in the module

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

S-pairs/S-polynomials:

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

$\mathfrak{s}$-reductions:

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

Think in the module

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

S-pairs/S-polynomials:

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

$\mathfrak{s}$-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:

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

□

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 on $\mathfrak{R}_T$ and choose the maximal element.

Special cases

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

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 $\trianglelefteq$.

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 $\trianglelefteq$.

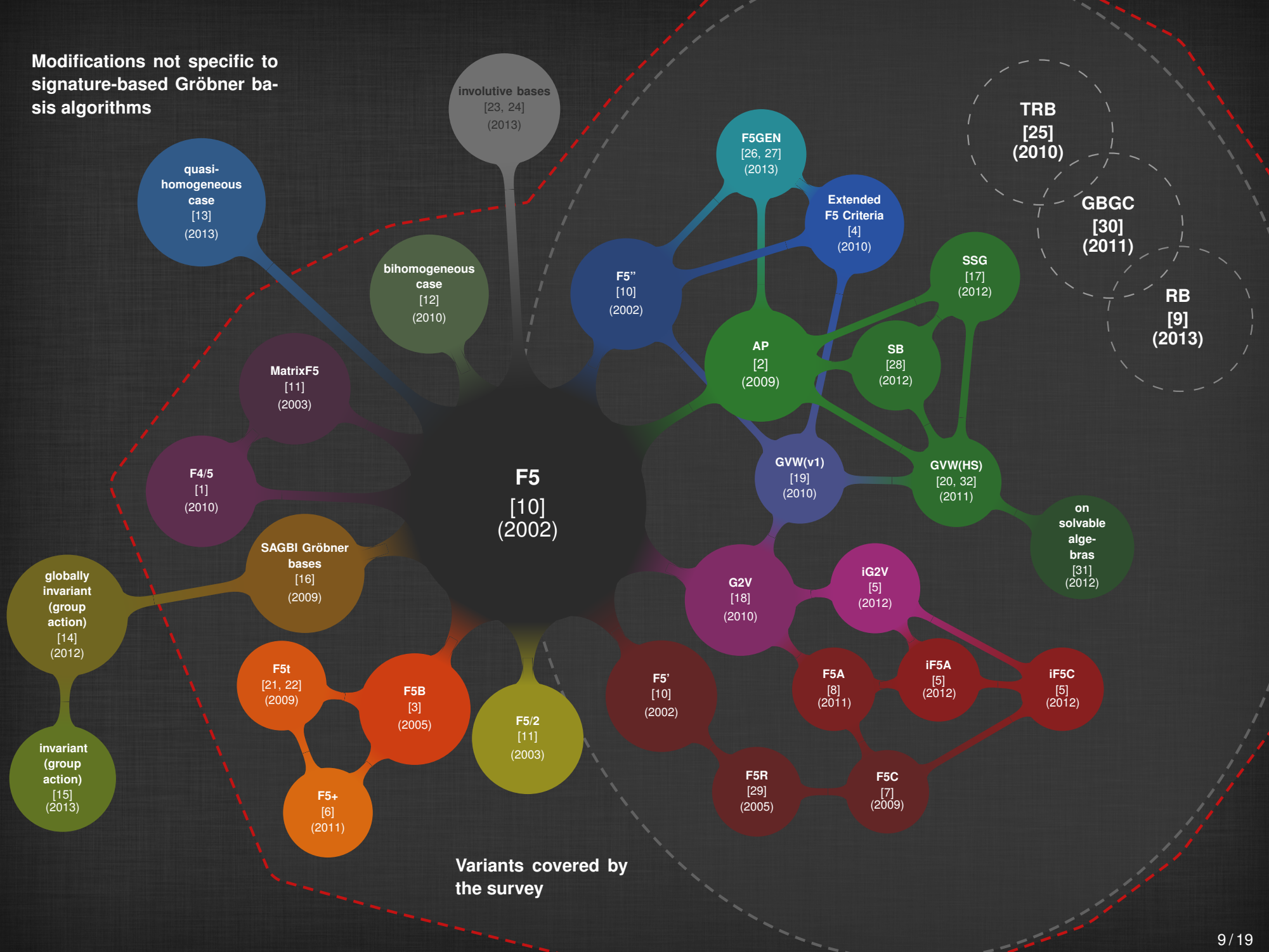
1. If $b\beta$ is a syzygy $\Longrightarrow$ Go on to next signature.

Special cases

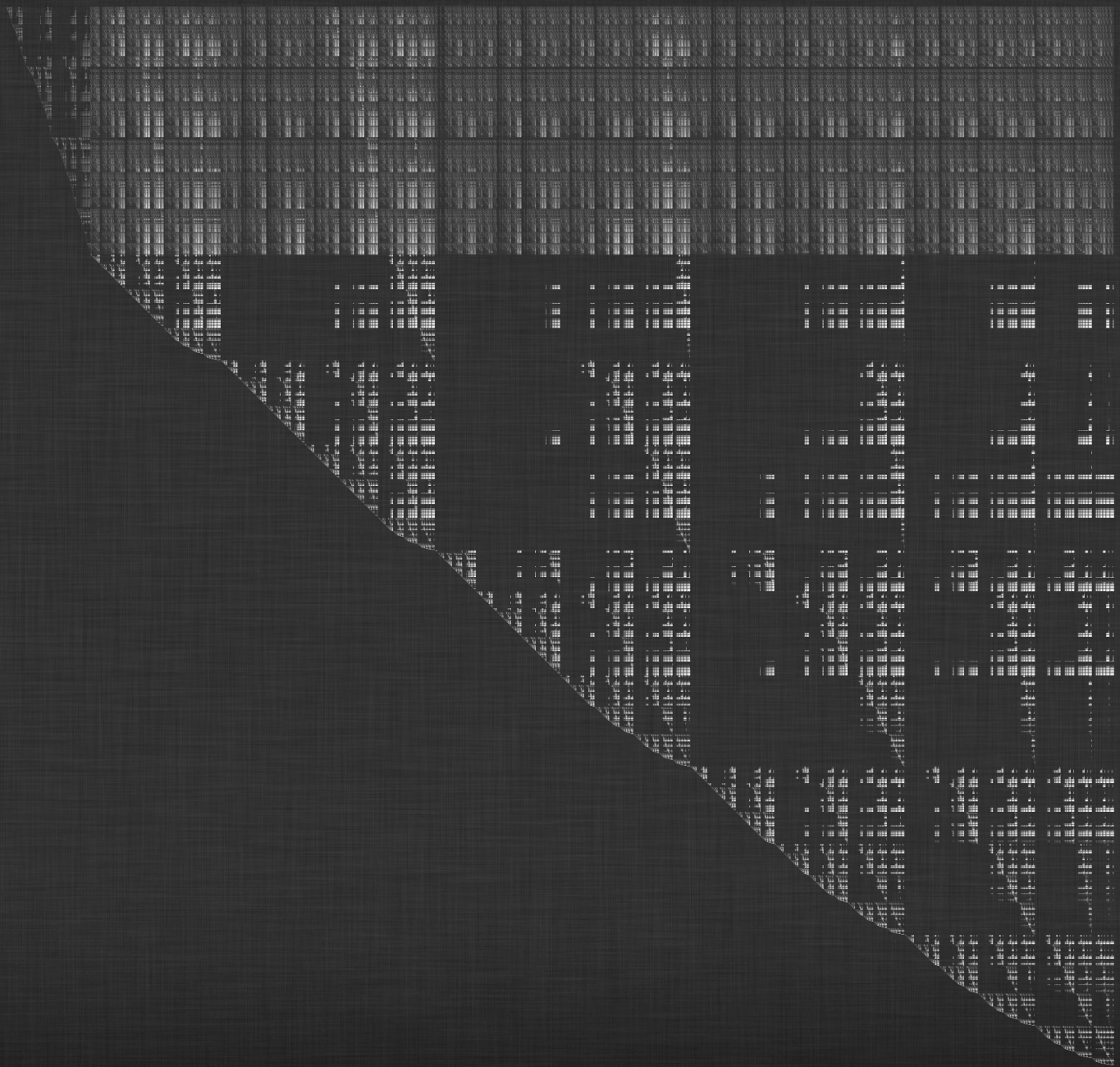
$$\mathfrak{R}_T = \left\{ a\alpha \mid \alpha \text{ handled by the algorithm and } \mathfrak{s}(a\alpha) = T \right\}$$

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

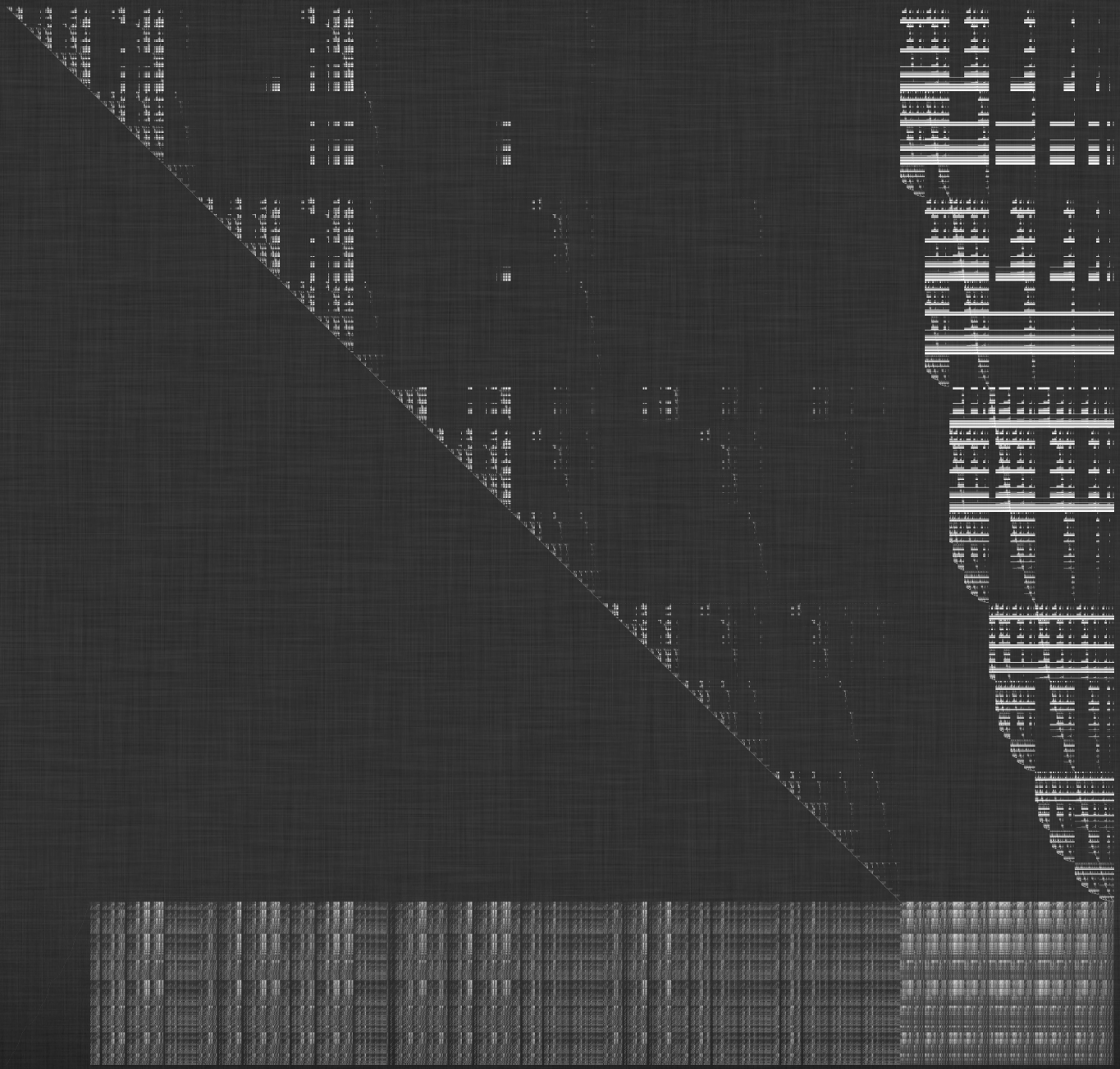
1. If $b\beta$ is a syzygy $\Longrightarrow$ Go on to next signature.
2. If $b\beta$ is not part of an S-pair $\Longrightarrow$ Go on to next signature.


Modifications not specific to signature-based Gröbner basis algorithms
involutive bases [23, 24] (2013)
quasi-homogeneous case [13] (2013)
bihomogeneous case [12] (2010)
F5GEN [26, 27] (2013)
Extended F5 Criteria [4] (2010)
F5" [10] (2002)
SSG [17] (2012)
AP [2] (2009)
SB [28] (2012)
TRB [25] (2010)
GBGC [30] (2011)
RB [9] (2013)
MatrixF5 [11] (2003)
F4/5 [1] (2010)
F5 [10] (2002)
GVW(v1) [19] (2010)
GVW(HS) [20, 32] (2011)
on solvable algebras [31] (2012)
SAGBI Gröbner bases [16] (2009)
globally invariant (group action) [14] (2012)
G2V [18] (2010)
iG2V [5] (2012)
F5t [21, 22] (2009)
F5B [3] (2005)
F5/2 [11] (2003)
F5' [10] (2002)
F5A [8] (2011)
iF5A [5] (2012)
iF5C [5] (2012)
invariant (group action) [15] (2013)
F5+ [6] (2011)
F5R [29] (2005)
F5C [7] (2009)
Variants covered by the survey

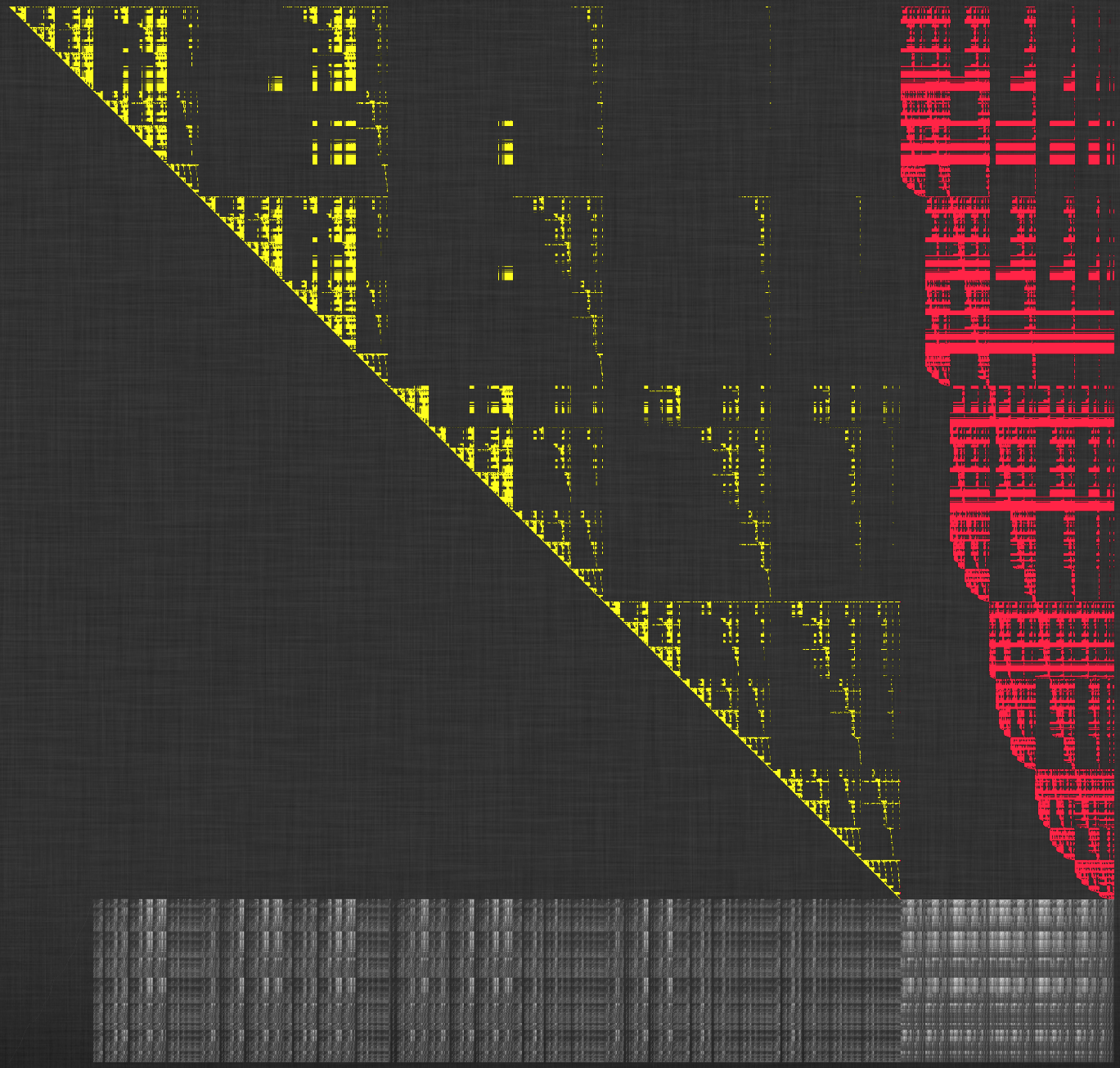
How our matrices look like



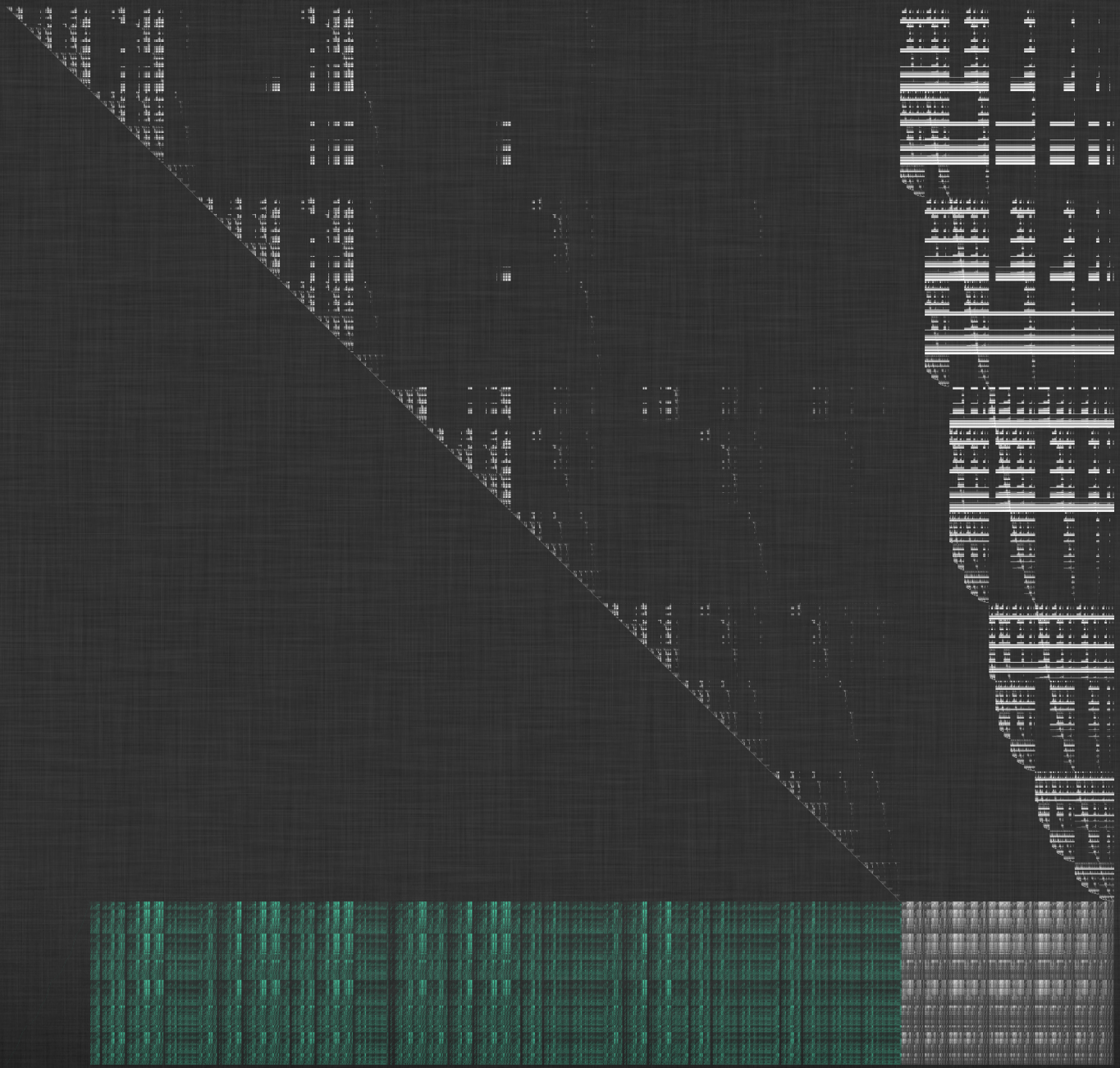
How our matrices look like



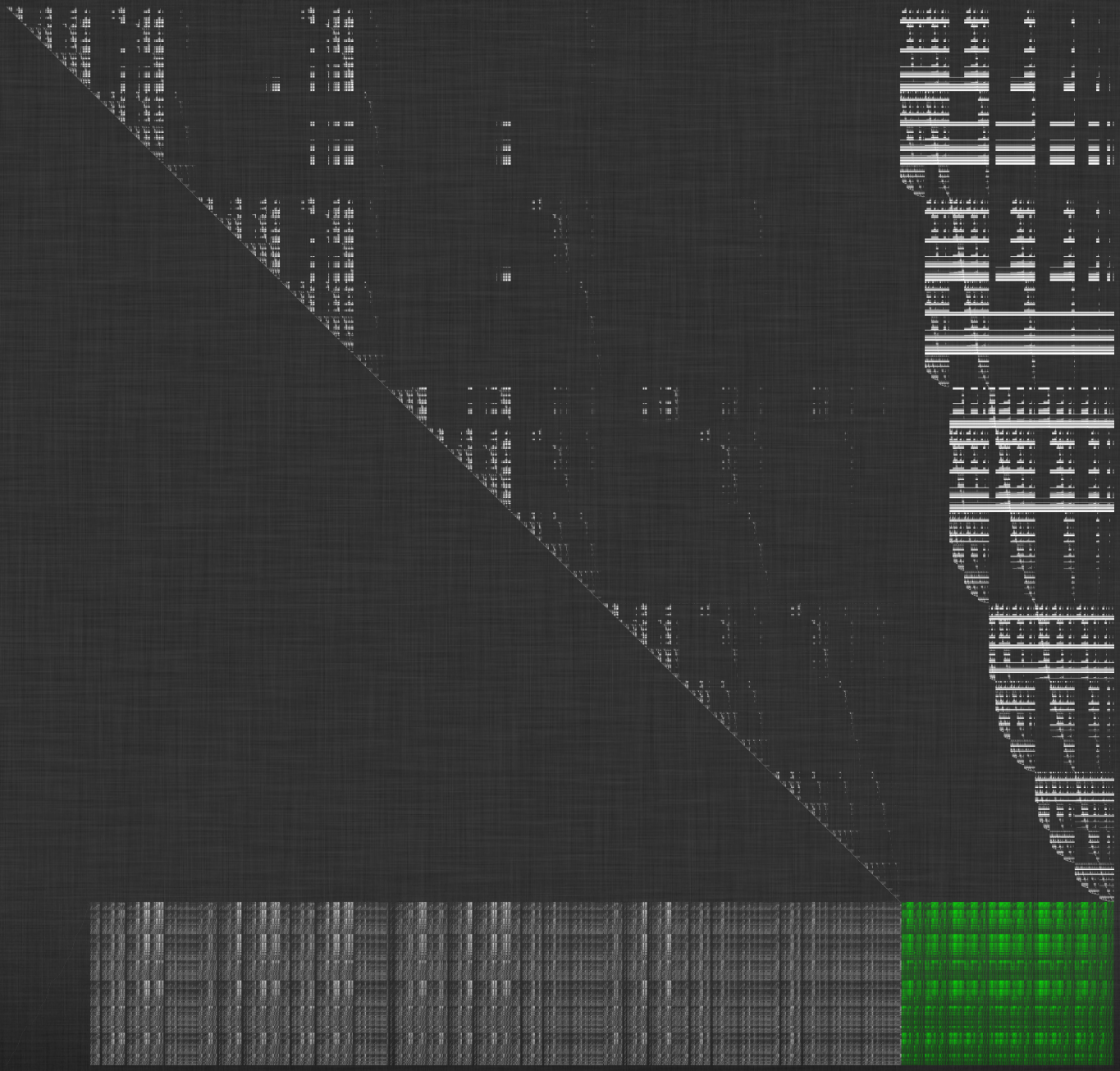
Hybrid Matrix Multiplication



Reduce to zero



New information



First attempts

2011 – University of Kaiserslautern
Bradford Hovinen – LELA
`https://github.com/Singular/LELA`

2012 – UPMC Paris 6, INRIA PolSys Team
Fayssal Martani – new implementation in LELA
`https://github.com/martani/LELA`

2012-2013 – University of Kaiserslautern
Bjarke Hammersholt Roune – MathicGB
`https://github.com/broune/mathicgb`

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., 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.

[7] 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.

[8] 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.

References II

[9] 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.

[10] 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`.

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

[12] 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.

[13] 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.

[14] 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.

References III

[15] 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.

[16] 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.

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

[18] 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.

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

[20] 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.

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

References IV

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

[23] 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.

[24] Gerdt, V. P., Hashemi, A., and M.-Alizadeh, B. Involutive Bases Algorithm Incorporating F5 Criterion. *CoRR*, abs/1306.6811, 2013.

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

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

[27] 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.

[28] 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.

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

References V

[30] 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.

[31] 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.

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