Signature-based algorithms to compute Gröbner bases

John Perry
john.perry@usm.edu

Christian Eder
ederc@mathematik.uni-kl.de

The University of Southern Mississippi

Technische Universität Kaiserslautern

Background

- The **Macaulay matrix** is formed by coefficients of monomial multiples of polynomials:

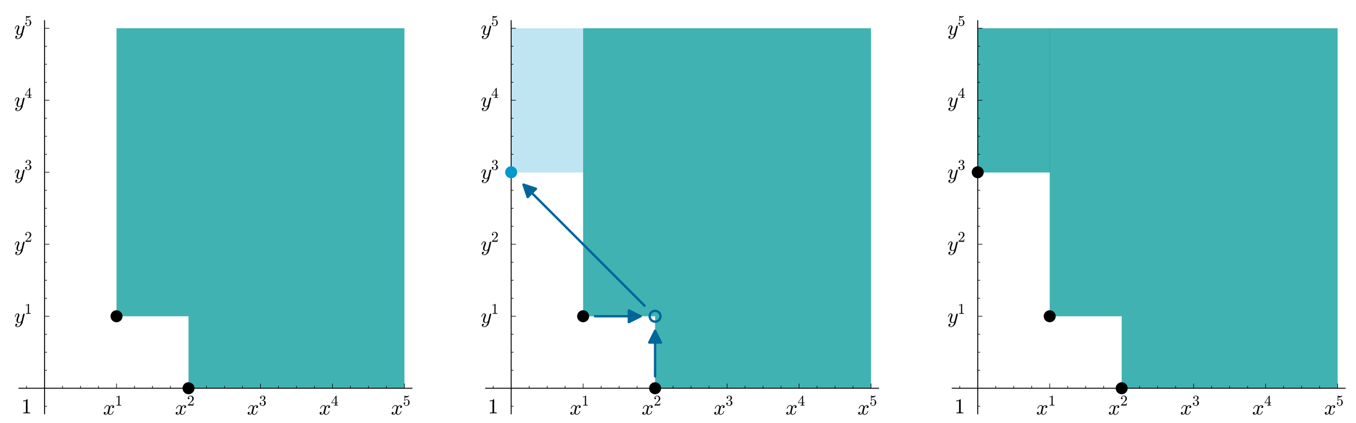
$$F = \{x^2+y^2-4, xy-1\}$$

$$\downarrow$$

$$\begin{array}{l}
\begin{array}{cccccccccc} x^3 & x^2y & xy^2 & y^3 & x^2 & xy & y^2 & x & y & 1 \end{array} \\
\begin{pmatrix}
\ddots & & & & & \ddots & & & & \\
 & 1 & & & & & & -1 & & \\
 & & 1 & & & & & & -1 & \\
 & & & & & 1 & & & & -1 \\
\ddots & & & & & \ddots & & & & \\
1 & & 1 & & & & & -4 & & \\
 & 1 & & 1 & & & & & -4 & \\
 & & & & 1 & & 1 & & & -4
\end{pmatrix}
\begin{array}{c} \vdots \\ x\mathbf{F}_2 \\ y\mathbf{F}_2 \\ \mathbf{F}_2 \\ \vdots \\ x\mathbf{F}_1 \\ y\mathbf{F}_1 \\ \mathbf{F}_1 \end{array}
\end{array}$$

Gaussian reduction (“triangularization”) reveals fundamental polynomials, called a **Gröbner basis**. New polynomials expand $\langle \mathrm{col}(p)\rangle$ in monoid of monomials in n variables, which is Noetherian, so expands only finitely many times.

$$\begin{array}{l} \begin{array}{cccc} x^2y & y^3 & x & y \end{array} \\ \begin{pmatrix} 1 & & -1 & \\ 1 & 1 & & -4 \end{pmatrix} \begin{array}{c} x\mathbf{F}_2 \\ y\mathbf{F}_1 \end{array} \end{array} \longrightarrow \begin{array}{l} \begin{array}{cccc} x^2y & y^3 & x & y \end{array} \\ \begin{pmatrix} & -1 & -1 & 4 \\ 1 & 1 & & -4 \end{pmatrix} \begin{array}{c} x\mathbf{F}_2 - y\mathbf{F}_1 \\ y\mathbf{F}_1 \end{array} \end{array}$$



- A **signature-based strategy** reduces a row *only from below*.
  - If p can appear at row $\tau\mathbf{F}_i$, with leftmost nonzero entry in column t, we write $\tau\mathbf{F}_i \in \mathrm{row}(p)$ and $\mathrm{col}(p) = t$. We record only the monomial multiple in $\mathrm{row}(p)$.
  - The **signature** of p, written $\mathcal{S}(p)$, is the lowest row in $\mathrm{row}(p)$. In the example above, $\mathcal{S}(-y^3-x+4y) = x\mathbf{F}_2$.
- A **syzygy** $(h_1,\ldots,h_m)$ corresponds to a dependence among the rows of the matrix, and appears as *empty rows* of the triangularized matrix:

$$\begin{array}{l}
\begin{array}{cccccc} x^3y & xy^3 & x^2 & xy & y^2 & 1 \end{array} \\
\begin{pmatrix}
 & & & & & 0 \\
 & 1 & & & -1 & \\
 & & & 1 & & -1 \\
1 & & & -1 & & \\
 & & 1 & & 1 & -4
\end{pmatrix}
\begin{array}{c} \mathbf{h}_1\mathbf{F}_1 + \mathbf{h}_2\mathbf{F}_2 \\ y^2\mathbf{F}_2 \\ \mathbf{F}_2 \\ xy\mathbf{F}_1 \\ \mathbf{F}_1 \end{array}
\end{array}$$

where $h_1 = -xy+1$ and $h_2 = x^2+y^2-4$.

Challenge

Efficiency: Algorithms F_5 [4], G^2V [5], “F_5 revised” [1] use a signature-based strategy, but select rows using different criteria, use different notation, and are difficult to compare accurately.

Termination: Under observation, signature-based algorithms consider only finitely many polynomials. It has not been clear *why*, since they do not always expand $\langle \mathrm{col}(p)\rangle$, or if there exist systems where they consider infinitely many.

Contributions to the Theory

Main Results ([2, 3]): *In a signature-based strategy,*

1. *triangularizing p in row $\sigma\mathbf{F}_i$ yields a syzygy if and only if $\mathcal{S}(p) < \sigma\mathbf{F}_i$;*
2. *if $\sigma\mathbf{F}_i \in \mathrm{row}(p) \cap \mathrm{row}(q)$, then*
   - *we can use p or q to triangularize — **even if***
   - *this choice automatically triangularizes row $\sigma\mathbf{F}_i$;*
3. *if*
   - *$\sigma\mathbf{F}_i = \mathcal{S}(p)$ and $u = \mathrm{col}(p)$,*
   - *$\tau\mathbf{F}_i = \mathcal{S}(q)$ and $t = \mathrm{col}(q)$, and*
   - *$\tau\mu = \sigma$ and $tv = u$ for some monomials μ, v,*

   *then we need not triangularize p in row $\sigma\mathbf{F}_i$, and we call p **signature redundant**;*
4. *if*
   - *$\sigma\mathbf{F}_i = \mathcal{S}(p) = \mathcal{S}(q)$,*
   - *$t = \mathrm{col}(p) = \mathrm{col}(q)$, and*
   - *we can find a in the ground field such that $\mathrm{col}(p-aq) < t$ but $\sigma\mathbf{F}_i \in \mathrm{row}(p-aq)$,*

   then we can find r such that $\mathcal{S}(r) < \sigma\mathbf{F}_i$ and $t = \mathrm{col}(r)$.

Why? Signature strategy $\Rightarrow$ lower rows triangularized. Hence:

1. Triangularizing p in row $\sigma\mathbf{F}_i$ yields a syzygy H in row $\sigma\mathbf{F}_i$ if and only if $\mathcal{S}(p) = \mathcal{S}(p - H\cdot F) < \sigma\mathbf{F}_i$.
2. We can find a in the ground field such that $\mathcal{S}(p-aq) < \sigma\mathbf{F}_i$, so $p-aq$ appears in lower row, triangularizing to r; $p = aq + r$.
3. Choose $\mu\cdot\tau = \sigma$, $tv = u$. If $\mu > v$, then p, q triangularize. If $\mu \le v$, find a such that $\mathcal{S}(p - a\mu q) < \sigma\mathbf{F}_i$, so $p - a\mu q$ appears in lower row, triangularizing to r; $p = a\mu q + r$.
4. If we can find such a, we can also find b where $r = p - bq$, $\mathrm{col}(r) = t$, and $\mathcal{S}(r) < \sigma\mathbf{F}_i$.

Common Algorithm

The following generalized algorithm allows accurate comparison.

inputs generators $(f_1,\ldots,f_i)$ of ideal I; $f_{i+1} \notin I$
outputs Gröbner basis G of $I + \langle f_{i+1}\rangle$

1. Let $G = ((\mathbf{F}_1, f_1), \ldots, (\mathbf{F}_{i+1}, f_{i+1}))$
2. Let $P = \{\text{lowest rows where elements of } G \text{ triangularize}\}$
3. Let $Syz = \{\tau\mathbf{F}_{i+1} : \tau = \mathrm{col}(f_j), 1 \le j \le i\}$
4. **while** $P \ne \emptyset$
   (a) Prune P using Syz and Result 1
   (b) Let $S = \{\text{rows of } P \text{ in rows of least degree}\}$
   (c) while $S \ne \emptyset$
      i. Prune S using Syz, G, and Results 1, 2, 3
      ii. Pop, triangularize min $\sigma\mathbf{F}_{i+1}$ in S: new poly r
      iii. **if** syzygy, add $\sigma\mathbf{F}_{i+1}$ to Syz
      iv. **if** not syzygy **and** not signature redundant
      Update P, S w/multiples of r
      v. Append $(\sigma\mathbf{F}_{i+1}, r)$ to G
5. **return** $\{g : (\sigma\mathbf{F}_{i+1}, g) \in G\}$

Efficiency: The most significant difference lies in how algorithms implement Result 2. Usually, [4] was most efficient, though [1] sometimes bested it. We never found [5] to be fastest.

Termination: Map $(\tau\mathbf{F}_i, x_1^{\beta_1}\cdots x_n^{\beta_n} + \cdots) \xrightarrow{\varphi} (\tau\cdot x_{n+1}^{\beta_1}\cdots x_{n+n}^{\beta_n})$; new rows considered iff r non-signature-redundant iff $\langle\varphi(G)\rangle$ expands in monoid of monomials in $2n$ variables; monoid is Noetherian, so finitely many expansions, so finitely many new rows.

Acknowledgments and References

Joint work with Alberto Arri (Univ. Pisa, now Google Corp.) and Justin Gash (Franklin College). The Centre for Computer Algebra at TU Kaiserslautern graciously provided hospitality and advice.

References

[1] Alberto Arri and John Perry, *The F5 Criterion revised*, Journal of Symbolic Computation **46** (2011), no. 2, 1017–1029.

[2] Christian Eder, Justin Gash, and John Perry, *Modifying Faugère's F5 algorithm for termination*, ACM Communications in Computer Algebra **45** (2011), no. 2, 70–89.

[3] Christian Eder and John Perry, *Signature-based algorithms to compute Gröbner bases*, ISSAC Proceedings, ACM Press, 2011, revised version at `arxiv.org/abs/1101.3589`.

[4] Jean-Charles Faugère, *A new efficient algorithm for computing Gröbner bases without reduction to zero F5*, ISSAC Proceedings, ACM Press, 2002, revised version at `fgbrs.lip6.fr/jcf/Publications/index.html`, pp. 75–82.

[5] Shuhong Gao, Yinhua Guan, and Frank Volny, *A new incremental algorithm for computing Groebner bases*, ISSAC Proceedings, ACM Press, 2010.