Signature-based algorithms to compute Gröbner bases

John Perry
december@usm.edu

Christian Eder
ederc@mathematik.uni-kl.de

BACKGROUND

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

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

\[
\begin{pmatrix}
1 & 1 & 1 & 1 & -4 & 1 \\
0 & 1 & 1 & 1 & 1 & 1 \\
\end{pmatrix}
\]

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

• A signature-based strategy reduces a row only from below.
  - If \( p \) appears at row \( \tau F, i \) with leftmost nonzero entry in column \( t \), we write \( \tau F, i \in \text{row}(p) \) and \( \text{col}(p) = t \). We record only the monomial multiple in row \( p \).
  - The signature of \( p \), written \( \text{S}(p) \), is the lowest row in row \( p \).

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:

\[
\begin{pmatrix}
1 & 1 & 1 & 1 & -4 & 1 \\
0 & 1 & 1 & 1 & 1 & 1 \\
\end{pmatrix}
\]

Contributions to the Theory

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

1. triangulizing \( p \) in row \( \sigma F \), yields a syzygy \( \text{if} \) and only if \( \text{S}(p) < \sigma F \); 
2. if \( \sigma F \in \text{row}(p) \cap \text{row}(q) \), then we can use \( p \) or \( q \) to triangularize — even if this choice automatically triangularizes row \( \sigma F \); 
3. if \( \sigma F, i = \text{S}(p) \) and \( u = \text{col}(p) \), then we need not triangularize \( \sigma F \) in row \( \sigma F, i \) and we call \( p \) signature redundant;
4. if \( \sigma F, i = \text{S}(p) \) and \( \text{col}(p) = \text{col}(q) \), then we can find \( r \) such that \( \text{S}(r) < \sigma F, i \) and \( \text{col}(r) = \text{col}(p) \).

Why? Signature strategy ⇒ lower rows triangularized. Hence:

1. Triangulizing \( p \) in row \( \sigma F \) yields a syzygy \( H \) in row \( \sigma F \) if and only if \( \text{S}(p) = \text{S}(p - H \cdot F) < \sigma F \); 
2. We can find \( a \) in the ground field such that \( \text{S}(p - aq) < \sigma F \), so \( p - aq \) appears in lower row, triangularizing to \( r \); 
3. \( H \) is a signature of \( p \) itself, \( \tau F, i = \text{S}(p) \) and \( \text{col}(p) = \text{col}(q) \), then we can find \( r \) such that \( \text{S}(r) < \sigma F, i \).

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 \( I + \{ f_{i+1} \} \)

1. Let \( G = \{ (f_1, f_i), \ldots, (f_{i+1}, f_{i+1}) \} \)
2. Let \( P = \{ \text{lowest rows where elements of} \ G \ \text{triangulize} \} \)
3. Let \( \text{Syz} = \{ \tau F, i+1 : \tau = \text{col}(f_j), 1 \leq j \leq i \} \)
4. while \( P \neq \emptyset \)
  a. Prune \( P \) using \( \text{Syz} \) and Result 1
  b. Let \( S \) = \{rows of \( P \) in rows of least degree\}
  c. while \( S \neq \emptyset \)
    i. Prune \( S \) using \( \text{Syz} \), \( G \), and Results 1, 2, 3
    ii. Pop, triangularize \( \sigma F, a \) in \( S \); new poly \( r \)
    iii. if \( \text{Syz} \), add \( \sigma F, a \) to \( \text{Syz} \)
    iv. if not syzygy and not signature redundant Update \( P, S \) with \( \text{multiples of} \ r \)
    v. Append \( \sigma F, i+1 \) to \( G \)

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 \( (\tau F, i+1, \ldots, \tau F, a) \) to \( \text{Syz} \), \( F \) non-signature-redundant iff \( r \) non-signature-redundant \( \text{Syz}(G) \) 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