The F_4 Algorithm

Dylan Peifer

Cornell University

9 May 2017

Gröbner Bases – History

- Gröbner bases were introduced in 1965 in the PhD thesis of Bruno Buchberger under Wolfgang Gröbner.
- Buchberger's algorithm computes Gröbner bases, and is the standard in most computer algebra systems.
- F_4 was introduced in 1999 by Jean-Charles Faugère as an improved Gröbner basis algorithm.
- F_4 is based on Buchberger, but gains efficiency by using fast matrix algorithms to quickly row reduce large sparse matrices that represent many steps of Buchberger's algorithm.

Polynomials

A Gröbner basis is a set of polynomials with a special property.

Definition

Let $R = k[x_1, \ldots, x_n]$ denote the ring of polynomials in variables $x_1, \ldots, x_n$ with coefficients from a field k.

Example

Let $R = \mathbb{Q}[x, y]$. Then $x^2 - x + 2$ and $\frac{1}{2}x^3y + xy^2 + xy - y + 1$ are elements of R. R contains all polynomials in variables x and y with rational coefficients.

Definition

Given a set of polynomials $\{f_1, \ldots, f_k\} \subseteq R$, the ideal $I \subseteq R$ generated by $f_1, \ldots, f_k$ is

$$I = \langle f_1, \ldots, f_k \rangle = \{a_1 f_1 + \cdots + a_k f_k \mid a_i \in R\}.$$

Univariate Division Algorithm

$$
\begin{array}{rrrrrl|rrrrrrrrrrr}
 & & & & & & & x^2 & + & 2x & + & 2 & & & & \\
\hline
x^2 & + & x & - & 2 & & & x^4 & + & 3x^3 & + & 2x^2 & + & 5x & + & 1 \\
 & & & & & & - & (x^4 & + & x^3 & - & 2x^2) & & & & \\
\cline{7-12}
 & & & & & & & & & 2x^3 & + & 4x^2 & + & 5x & + & 1 \\
 & & & & & & & & - & (2x^3 & + & 2x^2 & - & 4x) & & \\
\cline{9-14}
 & & & & & & & & & & & 2x^2 & + & 9x & + & 1 \\
 & & & & & & & & & & - & (2x^2 & + & 2x & - & 4) \\
\cline{11-16}
 & & & & & & & & & & & & & 7x & + & 5
\end{array}
$$

Given input dividend f and divisor a, the division algorithm computes an expression of the form $f = aq + r$. In our example,

$$x^4 + 3x^3 + 2x^2 + 5x + 1 = (x^2 + 2x + 2)(x^2 + x - 2) + (7x + 5).$$

Multivariate Division Algorithm

$$
\begin{array}{ccc|cccccccccccc}
 & & & q_1: & x^3 & - & xy & & & & & & & & \\
 & & & q_2: & x^2y & - & y^2 & + & 1 & & & & & & \\
\hline
x^2 & - & y^3 & & & & & & & & & & & & \\
xy^2 & + & x & & x^5 & + & x & & & & & & & & \\
 & & & - & (x^5 & - & x^3y^3) & & & & & & & & \\
\cline{4-9}
 & & & & & & x^3y^3 & + & x & & & & & & \\
 & & & & & - & (x^3y^3 & + & x^3y) & & & & & & \\
\cline{6-11}
 & & & & & & & & -x^3y & + & x & & & & \\
 & & & & & & & - & (-x^3y & + & xy^4) & & & & \\
\cline{8-13}
 & & & & & & & & & & -xy^4 & + & x & & \\
 & & & & & & & & & - & (-xy^4 & - & xy^2) & & \\
\cline{10-15}
 & & & & & & & & & & & & xy^2 & + & x \\
 & & & & & & & & & & & - & (xy^2 & + & x) \\
\cline{12-15}
 & & & & & & & & & & & & & & 0
\end{array}
$$

Given input dividend f and divisors $a_1, \ldots, a_k$, the multivariate division algorithm computes an expression of the form $f = a_1 q_1 + \cdots + a_k q_k + r$. In our example,

$$x^5 + x = (x^3 - xy)(x^2 - y^3) + (x^2y - y^2 + 1)(xy^2 + x).$$

Gröbner Bases – Definition

A Gröbner basis of an ideal I is a generating set with a nice property.

Definition

Given a monomial order, a Gröbner basis G of a nonzero ideal I is a generating set $\{g_1, g_2, \ldots, g_k\} \subseteq I$ such that for all $f \in R$, f leaves remainder 0 when divided by G if and only if $f \in I$.

Many questions about an ideal are easy to answer with a Gröbner basis, so a key question in computational algebra is how to compute a Gröbner basis for a given ideal.

Analogy to Linear Algebra

polynomials	$\Longleftrightarrow$	vectors
ring $R = k[x_1, \ldots, x_n]$	$\Longleftrightarrow$	vector space V
ideal $I \subseteq R$	$\Longleftrightarrow$	subspace $W \subseteq V$
generating set $\{f_1, \ldots, f_k\}$ of I	$\Longleftrightarrow$	basis $\{v_1, \ldots, v_k\}$ of W
Gröbner basis $\{g_1, \ldots, g_m\} \subseteq I$	$\Longleftrightarrow$	orthonormal basis $\{u_1, \ldots, u_k\} \subseteq W$
useful for computing: ideal membership, ideal intersections, solutions of systems, implicitizations, $\ldots$	$\Longleftrightarrow$	useful for computing: projections, decompositions, norms, adjoints, $\ldots$

Buchberger's Criterion

It is very difficult to show that a generating set is a Gröbner basis by definition. Buchberger proved that we can instead check that a certain property holds for each pair of generators.

Definition

Let $S(f,g) = \frac{\mathrm{lcm}(\mathrm{LM}(f),\mathrm{LM}(g))}{\mathrm{LT}(f)} f - \frac{\mathrm{lcm}(\mathrm{LM}(f),\mathrm{LM}(g))}{\mathrm{LT}(g)} g$ *where* lcm *is the least common multiple,* LT *is the leading term, and* LM *is the leading monomial. This is the S-polynomial of f and g, where S stands for subtraction or syzygy.*

Theorem (Buchberger's Criterion)

Let $G = \{g_1, g_2, \ldots, g_k\} \subseteq I$ for some ideal I. If $S(g_i, g_j)$ leaves remainder 0 when divided by G for all pairs $g_i, g_j \in G$ then G is a Gröbner basis of I.

Buchberger's Algorithm

1. Start with any generating set $F = \{f_1, \ldots, f_k\}$ of I.
2. Select a pair of generators f_i, f_j from F.
3. Compute the remainder r when $S(f_i, f_j)$ is divided by F.
4. If $r = 0$ then continue, otherwise add r to the generating set F.
5. Repeat from step 2 until all possible pairs from F have been processed. Note that any time we add generators to F we suddenly have many more pairs to consider.

Outline of F_4

1. Start with any generating set $F = \{f_1, \ldots, f_k\}$ of I.
2. Select a set of pairs $P = \{(f_{i_1}, f_{j_1}), \ldots, (f_{i_m}, f_{j_m})\}$ from F.
3. Produce a matrix M with rows corresponding to polynomials associated to the pairs in P. Compute the reduced row echelon form of M.
4. If any rows in $\mathrm{rref}(M)$ have a leading term that does not appear as a leading term in rows of M, add the polynomials corresponding to these rows to F.
5. Repeat from step 2 until all possible pairs from F have been processed. Note that any time we add generators to F we suddenly have many more pairs to consider.

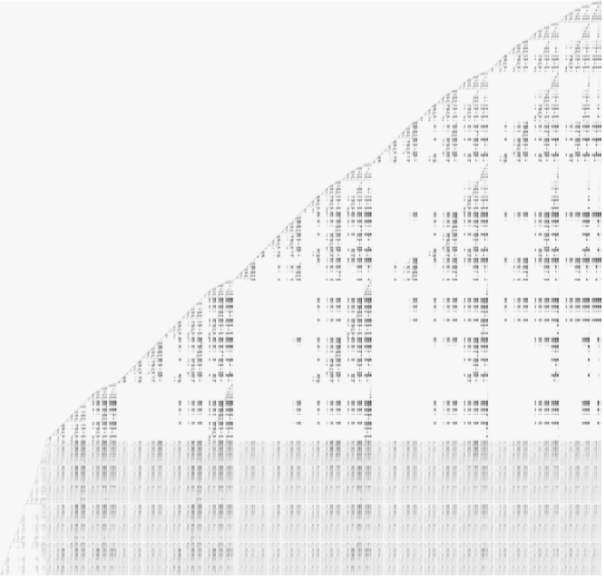
Reduction and Symbolic Preprocessing

The goal of F_4 is to mimic multivariate division with row reduction.

$$
\begin{array}{rrrrrrrrrrr}
 & & & q_1: & x^3 & & & & & & \\
 & & & q_2: & x^2y & & & & & & \\ \cline{4-11}
x^2 & - & y^3 & \multicolumn{1}{|r}{} & & & & & & & \\
xy^2 & + & x & \multicolumn{1}{|r}{} & x^5 & + & x & & & & \\
 & & & - & (x^5 & - & x^3y^3) & & & & \\ \cline{4-9}
 & & & & & & x^3y^3 & + & x & & \\
 & & & & & - & (x^3y^3 & + & x^3y) & & \\ \cline{6-11}
 & & & & & & & & -x^3y & + & x \\
 & & & & & & & & & \dots &
\end{array}
$$

1. Start set L with both halves of the S-polynomial for each pair in P.
2. For every term in L that is divisible by a lead term of some generator f_i, add a multiple of f_i with that lead term to L.
3. Repeat 2 until every term in L has been considered.
4. Make a matrix with columns corresponding to the terms in L in decreasing order, and rows the coefficients of the polynomials in L.
5. Put the matrix in reduced row echelon form.

Matrices from F_4



Results

Timings in seconds for several examples.

example	Macaulay2 Buchberger	Macaulay2 F4	Magma Buchberger	Magma F4
hcyclic8	320	4	111.6	1.12
jason210	16	6	5.65	2.79
katsura10	68	1	21.46	0.13
katsura11	955	4	272.01	0.64
mayr42	71	66	165.14	28.61
yang1	28	503	92.27	13.22

References

[1] Brice Boyer, Christian Eder, Jean-Charles Faugère, Sylvain Lachartre, and Fayssal Martani. GBLA: Gröbner basis linear algebra package. In *Proceedings of the ACM on International Symposium on Symbolic and Algebraic Computation*, ISSAC '16, pages 135-142, New York, NY, USA, 2016. ACM

[2] Jean-Charles Faugère. A new efficient algorithm for computing Gröbner bases (F4). *Journal of Pure and Applied Algebra*, 139(1-3):61-88, 1999.

[3] Jean-Charles Faugère and Sylvain Lachartre. Parallel Gaussian Elimination for Gröbner bases computations in finite fields. In *Proceedings of the 4th International Workshop on Parallel and Symbolic Computations*, PASCO '10, pages 89-97, New York, NY, USA, 2010. ACM.