

Elementary Gröbner Basis Theory

Jeffrey Clark
Elon University
e-mail: clarkj@elon.edu
web: <http://frodo.elon.edu>

Saturday, March 9, 2002

Contents

1	Introduction	1
2	History	2
3	Computation	2
3.1	Order	2
3.2	Rewriting	3
3.3	Algorithm	4
4	Examples	5
4.1	Solving a System of Polynomial Equations	5
4.2	Eliminating a Parameter from Parametric Equations	6
5	References	7

1 Introduction

In finite dimensional linear algebra, we often use bases to answer questions about operators and subspaces. Depending upon the context, some bases work better than others. For example, an orthonormal basis can easily be used to test whether a given vector is in a given subspace, or to express a vector uniquely in terms of the basis.

It is possible to perform analogous operations with the algebra of polynomials over a finite number of variables. Gröbner bases have been around for over three decades and serve as convenient tools for answering questions about polynomials and systems of polynomial equations.

2 History

Bruno Buchberger wrote his dissertation in 1965 at the University of Innsbruck on the creation of what is now known as Gröbner bases. (Wolfgang Gröbner supervised his dissertation.)

Buchberger's work did not really attract notice until the 1970's, at which time Buchberger coined the term "Gröbner basis."

The main algorithm for computing Gröbner bases is known as the Buchberger algorithm.

3 Computation

3.1 Order

We will be working with long division with multivariable polynomials. With one variable, it is clear what we mean by quotient and remainder: if we divide $x^3 + 1$ by $x^2 + 1$, we have $x^3 + 1 = (x^2 + 1)(x) + (-x + 1)$, where the quotient is x and the remainder $-x + 1$ is required to be "smaller" than $x^2 + 1$, in the sense that its degree is smaller than that of $x^2 + 1$.

What if we have two variables x and y ? What does it mean to divide $x^3 + y^3$ by $x^2 + y^2$? Do we want $x^3 + y^3 = (x^2 + y^2)(x) + (-xy^2 + y^3)$ or $x^3 + y^3 = (x^2 + y^2)(y) + (x^3 - x^2y)$?

The key is deciding how we want the remainder to be "smaller" than the divisor. This implies some sort of ordering of the polynomials. We will start by ordering the terms, so that each polynomial will have a leading term. We can then define $p < q$ to mean that the leading coefficient of $q - p$ is positive.

Ordering the terms really comes down to ordering the monomials $x_1^{e_1} x_2^{e_2} \dots x_n^{e_n}$; once we have done so, then we can worry as to whether or not the coefficient of the term is positive or negative.

Since we are dealing with polynomials, we need an order that respects not only addition but also multiplication. Therefore we define a *monomial ordering* on the monomials to be a well-ordering $<$ such that if m_1, m_2 , and m_3 are any monomials, $m_1 < m_2$ implies that $m_1 m_3 < m_2 m_3$.

One of the simplest monomial orderings is lexicographic: $x_1^{e_1} \dots x_n^{e_n} > x_1^{f_1} \dots x_n^{f_n}$ if and

only if there is a j between 1 and n such that $e_i = f_i$ for $i < j$ and $e_j > f_j$. This ordering is completely determined by how we order the variables themselves.

Once we have a monomial order defined, we have a well-ordering on the set of polynomials. In performing long division, we will always require that the remainder be smaller than the divisor in the sense of this order. Thus, if we use a lexicographic ordering on our variables, we have that $x^3 + y^3 = (x^2 + y^2)(x) + (-xy^2 + y^3)$. The remainder $-xy^2 + y^3$ is smaller than our divisor $x^2 + y^2$ since the leading term of $-xy^2 + y^3 - (x^2 + y^2)$ is $-x^2$, and the leading coefficient is negative.

3.2 Rewriting

We can think of going from a polynomial to its remainder as a form of rewriting. For example, if we know that $x^2 + 1 = 0$, then we can replace the leading term x^2 everywhere that it appears by -1 . We will write this substitution as a rewriting rule $x^2 \rightarrow -1$; we will also use an arrow wherever we employ it, i.e., $x^3 \rightarrow -x$. In the area of solving systems of polynomial equations, we would like to be able to use one equation to simplify another in this fashion. The process of applying rewriting rules to polynomials is known as reduction since we are replacing the leading term by a combination of smaller terms.

In this setting, we would like to reduce a given equation by all of the other equations, and therein lies the rub. It is possible that reducing a polynomial by different equations will yield different results.

For example: Suppose we know that $x^2 - y = 0$ and that $x^3 - y = 0$, where we order the terms lexicographically with $x > y$. Then how can we use these equations to reduce x^3 ? If we divide out by the first polynomial, we have $x^3 = (x^2 - y)(x) + xy$, which we can write as $x^3 \rightarrow xy$. If we divide out by the second polynomial we have $x^3 = (x^3 - y) + y$, which we can write as $x^3 \rightarrow y$. Note that the results xy and y differ and themselves can not be reduced any further.

This problem will only occur when we try and reduce a term that is divisible by both of the leading terms.

Therefore if we want to make sure that reduction by a set of polynomials leads to consistent results, we will need to make sure that the result of applying two rules to any common multiples of their leading terms will yield the same result.

For every pair of polynomials p and q we define their syzygy to be

$$S(p, q) = (\text{lcm}(p_L, q_L) / p_L)p - (\text{lcm}(p_L, q_L) / q_L)q$$

where p_L and q_L are the respective leading terms. (The difference will always result in the leading terms of the products cancelling out.) The syzygy is a measurement of how far apart the reduction of $\text{lcm}(p_L, q_L)$ by p or q is. If we now set the syzygy to 0, we force the results of reductions by p and by q to be equal.

For example, $S(x^2 - y, x^3 - y) = (x^3/x^2)(x^2 - y) - (x^3/x^3)(x^3 - y) = y - xy$.

3.3 Algorithm

When we look at all the possible combinations of a given set of polynomials, we are looking at an *ideal* generated by them.

A reduced Gröbner basis for a given polynomial ideal is a set of polynomials that will always produce the same result when applied as rewrite rules to any polynomial. By the above, one of the problems in constructing such a basis lies in making sure that all syzygies are accounted for.

The following algorithm, due to Buchberger, will take a set of polynomials and produce a reduced Gröbner basis for the ideal that they generate.

1. Let G be the set of polynomials, with a monomial ordering on them.
2. Let B be the reduced Gröbner basis. Start with $B = \{\}$.
3. While G is nonempty, let g be an element, and remove it from G .
4. Reduce g by all of the elements of B .
5. If $g = 0$, return to Step 3.
6. Otherwise, see if any of the elements b of B can be reduced by g . If so, remove b from B and add it to G .
7. Add $S(g, b)$ to G for all of the remaining elements of B .
8. Add g to B .
9. Return to 3.

It can be shown that this algorithm will always terminate in a finite number of steps. At any point we may remove any constant factors.

For example: let $x > y > z$ with a lexicographic ordering on polynomials in those three variables. We will find a Gröbner basis for the polynomials $x^2 - 2$, $y^2 - 3$, and $x + y - z$. The leading term will always be written at the front of the polynomial.

We start with:

$$B = \{\}$$

$$G = \{x^2 - 2, y^2 - 3, x + y - z\}$$

Take $g = x^2 - 2$ from G . Since B is empty, it can not be reduced any further by division by elements of B , and likewise none of the elements of B can be reduced. There are no syzygies to compute, and we add g to B .

$$B = \{x^2 - 2\}$$

$$G = \{y^2 - 3, x + y - z\}$$

Take $g = y^2 - 3$ from G . It cannot be reduced nor reduce the only element of B . We add the syzygy $S(y^2 - 3, x^2 - 2) = -3x^2 + 2y^2$ to G and g to B .

$$B = \{x^2 - 2, y^2 - 3\}$$

$$G = \{x + y - z, -3x^2 + 2y^2\}$$

Take $g = x + y - z$ from G . The first generator in B can be reduced by g to $y^2 - 2yz + z^2 - 2$, and is removed from B , with its reduced form added to G . We add the syzygy $S(x + y - z, y^2 - 3) = y^3 - y^2z + 3x$ to G and g to B .

$$B = \{y^2 - 3, x + y - z\}$$

$$G = \{-3x^2 + 2y^2, y^2 - 2yz + z^2 - 2, y^3 - y^2z + 3x\}$$

We take $g = -3x^2 + 2y^2$ from G . The first element of B reduces g to $-3x^2 + 6$, which the second element of B reduces to $-3y^2 + 6yz - 3z^2 + 6$, which now the first element reduces to $6yz - 3z^2 - 3 = 3(2yz - z^2 - 1)$. None of the elements of B can be reduced by $2yz - z^2 - 1$, so we add its syzygies $S(2yz - z^2 - 1, y^2 - 3) = -yz^2 - y + 6z$, and $S(2yz - z^2 - 1, x + y - z) = -xz^2 - x - 2y^2z + 2yz^2$ to G , and add $2yz - z^2 - 1$ to B .

$$B = \{y^2 - 3, x + y - z, 2yz - z^2 - 1\}$$

$$G = \{y^2 - 2yz + z^2 - 2, y^3 - y^2z + 3x, -yz^2 - y + 6z, -xz^2 - 2y^2z + 2yz^2\}$$

After a few more (lengthy) iterations, we end up with G empty and $B = \{-1 + 10z^2 - z^4, -2y + 11z - z^3, -2x - 9z + z^3\}$ as our Gröbner basis.

This process is too lengthy to be done by hand; fortunately both *Maple* and *Mathematica* have commands for it. In *Maple* the command is `groebner[gbasis]`, and in *Mathematica* it is `GroebnerBasis[listofpolys, variableorder]`.

4 Examples

4.1 Solving a System of Polynomial Equations

If it is possible to eliminate a variable from a system of polynomial equations, then a properly chosen Gröbner basis for that system will contain a polynomial free of that variable.

The same is true for eliminating several variables, so if it is possible to solve a system for a finite number of solutions, then it is possible to find a Gröbner basis for the system that eliminates all but one of the variables. The roots of that univariate polynomial can be substituted back in to recursively solve for the values of the other variables.

Suppose we start with the following system of equations:

$$\begin{aligned} x^3 + xy + y^3 &= 4 \\ xy^2 + x^3 - y^4 &= 5 \end{aligned}$$

If we use these equations to generate a Gröbner basis with a lexicographic order, then if it is possible to combine these equations to eliminate a variable, it will show up as the largest generator in the basis. The smaller of the two variables will be the one eliminated.

Using *Mathematica*, we write the equations as polynomials in a list, and the lexicographic order as a second list of variables.

With $x > y$:

```
In[1]:= GroebnerBasis[
      {x^3 + x*y + y^3 - 4,
       x*y^2 + x^3 - y^4 - 5}, {x, y}]
```

With $y > x$

```
Out[1]= {-1 - 8 y^3 + 11 y^4 - 13 y^5 + y^6 -
          8 y^7 + y^8 - 3 y^9 - 3 y^10 - 3 y^11 - y^12,
          -8 - 9 x - 8 y + 55 y^2 - 117 y^3 + 88 y^4 - 25 y^5 +
          55 y^6 - 18 y^7 + 17 y^8 + 20 y^9 + 23 y^10 + 8 y^11}
```

```
In[2]:= GroebnerBasis[
      {x^3 + x*y + y^3 - 4,
       x*y^2 + x^3 - y^4 - 5}, {y, x}]
Out[2]= {-381 - 560 x - 100 x^2 + 395 x^3 + 372 x^4 + 40 x^5 -
          143 x^6 - 87 x^7 - 4 x^8 + 21 x^9 + 7 x^10 - x^12,
          118423266 - 3938750 x - 86476014 x^2 -
          50817625 x^3 - 2517535 x^4 +
          28636842 x^5 + 2790073 x^6 +
          2844613 x^7 - 2148924 x^8 + 482607 x^9 -
          428450 x^10 + 97642 x^11 + 69569829 y}
```

In both cases, the first generator is a twelfth-degree polynomial in a single variable. Generally such an equation will not be solvable in terms of radicals, etc., but the system can then be “solved” in terms of the root.

For example, given that y is a root of the first generator in the first case, the second generator expresses x in terms of y . Similarly, the second case allows us to express y in terms of x , given that x is a root for the given twelfth-degree polynomial.

4.2 Eliminating a Parameter from Parametric Equations

If we are given polynomial or even rational parametric equations, we can use them to solve for a Gröbner basis that contains at least one generator that does not contain the parameter(s), i.e., an implicit equation connecting other variables.

Let $x = t/(t^2 - 1)$ and $y = t^2/(t^3 + 1)$. We will try to eliminate t and produce an equation connecting x and y .

As written, x and y are not polynomial functions, but we can introduce two auxiliary variables u and v to be the reciprocals of the denominators:

$$\begin{aligned}x - tu &= 0 \\y - t^2v &= 0 \\u(t^2 - 1) - 1 &= 0 \\v(t^3 + 1) - 1 &= 0\end{aligned}$$

If we order the variables $u > v > t > x > y$, then the greatest polynomial in the Gröbner basis will eliminate u , v , and t if at all possible.

Using *Mathematica* on this system, we find:

```
In[3]:= GroebnerBasis[
  {x - t*u, y - t^2*v, u*(t^2 - 1) - 1,
   v*(t^3 + 1) - 1}, {u, v, t, x, y}]
Out[3]= {x^3 - x*y - x^2*y - 2*x^3*y + y^2 + 3*x^2*y^2,
  x^2 - y - 3*x^2*y + y^2 + t*y^2 + 2*x*y^2 + 2*x^2*y^2 +
  y^3 - 2*t*y^3 - 3*x*y^3, -t*x + x^2 - 2*y +
  t*y + x*y - 2*x^2*y - y^2 + 2*t*y^2 + 3*x*y^2,
  -t - x + x^2 - y + t^2*y + x*y - 2*x^2*y - y^2 +
  2*t*y^2 + 3*x*y^2, 1 - v - t*y, -1 - u + x^2 -
  2*y + t*y + x*y - 2*x^2*y - y^2 + 2*t*y^2 + 3*x*y^2}
```

We can see that the first generator listed gives us our polynomial equation in terms of x and y :

$$x^3 - xy - x^2y - 2x^3y + y^2 + 3x^2y^2 = 0$$

5 References

This paper is available electronically at

<http://frodo.elon.edu/presentations/grobner.pdf>

- Baader, Franz and Nipkow, Tobias. *Term Rewriting and All That*. Cambridge University Press, 1998.
- Becker, Thomas and Weispfenning, Volker. *Gröbner Bases*. Springer-Verlag, 1993.
- Cox, David, Little, John, and O’Shea, Donal. *Ideals, Varieties, and Algorithms*. Springer-Verlag, 1992.

- Cox, David, Little, John, and O'Shea, Donal. *Using Algebraic Geometry*. Springer-Verlag, 1998.
- Davenport, J. H., Siret, Y., and Tournier, E. *Computer Algebra*. Academic Press, 1988.
- Eisenbud, David. *Commutative Algebra with a View Toward Algebraic Geometry*. Springer-Verlag, 1995.