Gröbner Bases

Victor Adamchik

Carnegie Mellon University

Buchberger's algorithm

Theorem. (*Buchberger's S-pair criterion*)

A finite set $G = \{g_1, \ldots, g_s\}$ for an ideal I is a Gröbner basis if and only if

$$S(g_k, g_n) \xrightarrow{*}_G 0$$

(the remainder of division $S(g_k, g_n)$ by G is zero) for any k and n.

Buchberger's algorithm

Fix a monomial order.

A Gröbner basis G for ideal $I = \langle f_1, \ldots, f_s \rangle$ is obtained by the following procedure:

1. for each i and j execute $S(f_i, f_j) \xrightarrow{*}_G r_{i j}$

2. if all remainders are zero, return $f_1, \ldots, f_s$

3. otherwise add $r_{i j}$ to basis G and goto step 1

This procedure gives us an ascending chain of ideals that must eventually stop growing because $F[x_1, \ldots, x_n]$ is Noetherian. This proves that algorithm terminates.

Unfortunately, there is no bound on the running time.

Input: A polynomial set $F = \{f_1, \ldots, f_s\}$ that generates an ideal I

Output: A Gröbner basis $G = \{g_1, \ldots, g_r\}$ that generates I.

$G := F$

M := set of pairs $\{f_i, f_j\}$ where f_i and f_j are in G.

WHILE (M<>Ø) DO

{p, q} := a pair in M

M := M - {{p, q}}

S := SPolynomial(p, q)

R := NormalForm(S, G)//reduce S wrt to G

IF (R <> 0) THEN

$M := M\ U\ \{f_i,\ R\}$ for all g_i in G

$G := G\ U\ \{R\}$

■ Example 1

Consider the ideal $< x^2 - y,\ x^3 - z >$ and build a Gröbner basis wrt to *lex* order $x > y > z$.

We start with computing

$$S\left(x^2 - y,\ x^3 - z\right) = \frac{x^3}{x^2} * \left(x^2 - y\right) - \frac{x^3}{x^3} * \left(x^3 - z\right) = -x\, y + z$$

Its leading term $x\, y$ is not contained in $< \mathrm{LM}(f_1),\ \mathrm{LM}(f_2) > \ = \ < x^2 >$, therefore we must add it to the basis, which is now is

$$< x^2 - y,\ x^3 - z,\ -x\, y + z >$$

Now we compute

$$S\left(x^2 - y, -x\, y + z\right) = \frac{x^2\, y}{x^2} * \left(x^2 - y\right) - \frac{x^2\, y}{-x\, y} * (-x\, y + z) = x\, z - y^2$$

We add it to the basis, which now is

$$< x^2 - y,\ x^3 - z,\ -x\, y + z,\ x\, z - y^2 >$$

Keep computing

$$S(f_2,\ f_3) = z * f_1$$

$$S(f_1,\ f_4) = y * f_3$$

$$S(f_2,\ f_4) = (x\, y + z) * f_3$$

$$S(f_3,\ f_4) = y^3 - z^2$$

The last has leading term that is not in $< x^2,\ x\, y,\ x\, z >$.Adding the new generator completes the Gröbner basis

$$< x^2 - y,\ x^3 - z,\ -x\, y + z,\ x\, z - y^2,\ y^3 - z^2 >$$

You check this by computing S-polynomials.

```
GroebnerBasis[{x^2 - y, x^3 - z}, {x, y, z},
 MonomialOrder → Lexicographic]
```

```
{y^3 - z^2, -y^2 + x z, x y - z, x^2 - y}
```

■ **Example 2**

Compute a Gröbner basis for the ideal $< x\,y^3 - x^2,\ x^3\,y^2 - y >$ wrt to *graded lex* order $x > y$.

$$S\left(x\,y^3 - x^2,\ x^3\,y^2 - y\right) = \frac{x^3\,y^3}{x\,y^3} * \left(x\,y^3 - x^2\right) - \frac{x^3\,y^3}{x^3\,y^2} * \left(x^3\,y^2 - y\right) = -x^4 + y^2$$

Its leading term x^4 is not contained in $< \mathrm{LM}(f_1),\ \mathrm{LM}(f_2) >$, therefore we must add it to the basis, which is now is

$$< x\,y^3 - x^2,\ x^3\,y^2 - y,\ -x^4 + y^2 >$$

Now we compute

$$S\left(x^3\,y^2 - y, -x^4 + y^2\right) = \frac{x^4\,y^2}{x^3\,y^2} * \left(x^3\,y^2 - y\right) - \frac{x^4\,y^2}{-x^4} * \left(-x^4 + y^2\right) = y^4 - x\,y$$

It's leading term $y^4$is not contained in $< \mathrm{LM}(f_1),\ \mathrm{LM}(f_2),\ \mathrm{LM}(f_3) >$, therefore we must add it to the basis.

$$S\left(x\,y^3 - x^2, -x^4 + y^2\right) = \frac{x^4\,y^3}{x\,y^3} * \left(x\,y^3 - x^2\right) - \frac{x^4\,y^3}{-x^4} * \left(-x^4 + y^2\right) = -x^5 + y^5$$

$$-x^5 + y^5 \rightarrow_{-x^4+y^2} = y^5 - x\,y^2 \rightarrow_{y^4 - x\,y} = 0$$

The basis now is

$$< x\,y^3 - x^2,\ x^3\,y^2 - y,\ -x^4 + y^2,\ y^4 - x\,y >$$

Next we compute

$$S\left(x\,y^3 - x^2,\ y^4 - x\,y\right) = \frac{x\,y^4}{x\,y^3} * \left(x\,y^3 - x^2\right) - \frac{x\,y^4}{y^4} * \left(y^4 - x\,y\right) = 0$$

$$S\left(-x^4 + y^2,\ y^4 - x\,y\right) = \frac{x^4\,y^4}{-x^4} * \left(-x^4 + y^2\right) - \frac{x^4\,y^4}{y^4} * \left(y^4 - x\,y\right) = -y^6 + x^5\,y$$

$$-y^6 + x^5\,y \rightarrow_{y^4 - x\,y} = x^5\,y - x\,y^3 \rightarrow_{-x^4+y^2} = 0$$

```
GroebnerBasis[{x y^3 - x^2, x^3 y^2 - y}, {x, y},
 MonomialOrder → DegreeLexicographic]
```

$\{x\,y - y^4,\ -x^2 + x\,y^3,\ -x^4 + y^2,\ -y + x^3\,y^2\}$

■ Timings

```
Clear[x, y, z]; polys = {x^6 + y^4 + z^3 - 1, x^5 + y^3 + z^2 - 1};
gb = Timing[GroebnerBasis[polys, {y, z, x}]];
{First[gb], Length[gb[[2]]]}
```

```
{0.063, 7}
```

```
gb = Timing[GroebnerBasis[polys, {z, y, x}]];
{First[gb], Length[gb[[2]]]}
```

$\{1.33357\times 10^{-17},\ 5\}$

```
gb = Timing[GroebnerBasis[polys, {x, y, z}]];
{First[gb], Length[gb[[2]]]}
```

```
{1.422, 11}
```

```
gb = Timing[GroebnerBasis[polys, {y, z, x},
    MonomialOrder → DegreeLexicographic]];
{First[gb], Length[gb[[2]]]}
```

$\{1.661\times 10^{-16},\ 2\}$

```
gb = Timing[GroebnerBasis[polys, {x, y, z},
    MonomialOrder → DegreeReverseLexicographic]];
{First[gb], Length[gb[[2]]]}
```

```
{0., 3}
```

■ Monomial orders

```
GroebnerBasis[{x + y + z, x - 2 y + z^3, x^2 - 2 y^3 + z},
 {x, y, z}]
```

Reverting the order of the variables gives now one univariate polynomial in x.

```
GroebnerBasis[{x + y + z, x - 2 y + z^3, x^2 - 2 y^3 + z},
 {z, y, x}]
```

Calculating a Gröbner basis is typically a very time consuming process for larger polynomial systems. In most cases the calculation using the term order MonomialOrder -> DegreeReverseLexicographic is the fastest.

```
GroebnerBasis[{x^7 + y^5 + z^2, x - 2 y^3 + 5 z^3,
x^2 - 7 y^3 + z^4}, {z, y, x},
MonomialOrder -> Lexicographic]; // Timing
```

```
GroebnerBasis[{x^7 + y^5 + z^2, x - 2 y^3 + 5 z^3,
x^2 - 7 y^3 + z^4}, {z, y, x},
MonomialOrder -> DegreeReverseLexicographic]; // Timing
```

The DegreeReverseLexicographic is not directly useful for equation solving. But it is very useful for detecting an inconsistent system of equations.

For eliminating variables the term order MonomialOrder -> EliminationOrder is often the most appropriate one.

```
GroebnerBasis[{x - s t^2 + s, y - s^2 + t^2, z - s^3 + t},
 {z, y, x}, {s, t},
MonomialOrder -> EliminationOrder]
```

Coefficients Growth

In[4]:=
```
eqs = {2 x^4 y + x^3 y^3 - x z^2 + 1, x^2 + y^2 z^3 - 1, x^2 y - 7 y^3 z^2 + y^2 z^3};
```

In[5]:=
```
gb = GroebnerBasis[eqs, {x, y, z}];
```

In[6]:=
```
Exponent[#, {x, y, z}] & /@ gb
```

Out[6]=
```
{{0, 0, 44}, {0, 1, 43}, {1, 0, 43}}
```

In[7]:=
```
Max[Abs[Cases[gb, _Integer, 3]]]
```

Out[7]=
```
660 315 050 284 902 405 127 753 569 085 965 903 934 655 262 562 978 197 853 379 515
 017 909 418 018 128 358 017 411 114 728 904 394 324 209 494 316 198 167 365 922
 715 648 404 225 906 493 353 093 640 012 381 786 701 916 234 271 606 424 340 544
 687 009 397 545 950 038 307 082 551 077 348 818 498 311 022 761 249 117 137 174
 194 545 028
```

Minimal Gröbner basis

Buchberger's algorithm does not guarantee that obtained basis will be unique. There are two places in the algorithm where we make choices:

a) the order of polynomials in the basis

b) in the while loop: {p, q} := a pair in M - we choose two polynomials at random.

Definition. *A Gröbner basis is called* ***minimal*** *if all* $LC(g_k) = 1$ *and for all* $i \neq j$ $LM(g_i)$ *does not divide* $LM(g_j)$.

How to obtain a minimal basis? We must eliminate all g_i for which there exists $j \neq i$ such that $\mathrm{LM}(g_j)$ divides $\mathrm{LM}(g_i)$.The minimal basis is not unique as well.

Example. Consider a basis (*lex* order $y > x$).

$$< y^2 + y x + x^2,\ y + x,\ y,\ x^2,\ x >$$

which is not minimal.

We can remove the first, second and fourth polynomials to get $< y,\ x >$

We could also remove the first, third and fourth to get $< y + x,\ x >$

Definition. *A Gröbner basis is called* ***reduced*** *if all* $LC(g_k) = 1$ *and each* g_i *is reduced with respect* *to* $G - \{g_i\}$

Lemma. Let $G = \{g_1, \ ..., \ g_s\}$ be a minimal Gröbner basis. Consider the following reduction process

$$g_1 \to_{H_1} h_1 \,, \ \text{where } H_1 = \{g_2, \ \ ..., \ g_s\}$$

$$g_2 \to_{H_2} h_2 \,, \ \text{where } H_2 = \{h_1, \, g_3, \ \ ..., \ g_s\}$$

$$g_3 \to_{H_3} h_3 \,, \ \text{where } H_3 = \{h_1, \, h_2, \, g_4, \ \ ..., \ g_s\}$$

and so on

$$g_s \to_{H_s} h_s \,, \ \text{where } H_s = \{h_1, \, h_2, \ \ ..., \ h_{s-1}\}$$

Then $H = \{h_1, \, h_2, \ \ ..., \ h_s\}$ is a reduced Gröbner basis

Theorem (Buchberger) *Fix a monomial order. Then every non-zero ideal has a* ***unique reduced*** *Gröbner basis*

Example.Consider a basis $< y^2 + y\,x + x^2, \ y + x, \ y, \ x^2, \ x >$ We constructed two minimal bases $< y, \ \ x >$ and $< \ y + x, \ x >$. The last one is not reduced, we can reduce $y + x$ to y using x.

Buchberger's Refined Algorithm

Here we will discuss some improvements on the Buchberger algorithm. The most expensive operation in the algorithm is the reduction of the S-polynomials modulo G. Buchberger developed two criterias for detecting 0-reductions a priori. He also developed other strategies that significantly speed up the calculations.

Buchberger's First Criteria.

If

$$\text{LCM}(\text{LM}(p), \ \text{LM}(q)) \ = \ \text{LM}(p) * \text{LM}(q)$$

then

$$S(p, \ q) \xrightarrow{*}_G 0$$

This means that we can ignore those pairs whose leading monomials are relatively prime.

Buchberger's Second Criteria.

If, when considering the pair $\{f_i, \ f_j\}$, there exist an element f_k such that

$$LCM(\text{LM}(f_i), \text{LM}(f_j)) \text{ is a multiple of } \text{LM}(f_k)$$

$$\text{and } S(f_i, \ f_k) \text{ and } S(f_j, \ f_k) \text{ have already been computed}$$

then

$$S(f_i,\ f_j) \xrightarrow{*}_G 0$$

Another strategy.

Always select pairs $\{f_i,\ f_j\}$ such that $\mathrm{LCM}(\mathrm{LM}(f_i),\ \mathrm{LM}(f_j))$ is as small as possible.

■ Example: Buchberger's Refined Algorithm

Consider the ideal $< x^2 + 2\,x\,y,\ x\,y + 2\,y^2 - 1 >$ and compute its Gröbner basis wrt to *lex* order $x > y$.

$$S(x^2 + 2\,x\,y,\ x\,y + 2\,y^2 - 1) = \frac{x^2\,y}{x^2} * (x^2 + 2\,x\,y) - \frac{x^2\,y}{x\,y} * (x\,y + 2\,y^2 - 1) = x$$

Adjust the basis:

$$< x^2 + 2\,x\,y,\ x\,y + 2\,y^2 - 1,\ x >$$

Look at LCMs:

$$\mathrm{LCM}(\mathrm{LM}(f_1),\ \mathrm{LM}(f_3)) = \mathrm{LCM}(x^2,\ x) = x^2$$

$$\mathrm{LCM}(\mathrm{LM}(f_2),\ \mathrm{LM}(f_3)) = \mathrm{LCM}(x\,y,\ x) = x\,y$$

and choose $\{f_2,\ f_3\}$.

$$S(f_2,\ f_3) = \frac{x\,y}{x\,y} * (x\,y + 2\,y^2 - 1) - \frac{x\,y}{x} * (x) = 2\,y^2 - 1$$

Adjust the basis:

$$< x^2 + 2\,x\,y,\ x\,y + 2\,y^2 - 1,\ x,\ 2\,y^2 - 1 >$$

Look at LCMs:

$$\mathrm{LCM}(\mathrm{LM}(f_1),\ \mathrm{LM}(f_3)) = \mathrm{LCM}(x^2,\ x) = x^2$$

$$\mathrm{LCM}(\mathrm{LM}(f_1),\ \mathrm{LM}(f_4)) = \mathrm{LCM}(x^2,\ y^2) = x^2\,y^2$$

$$\mathrm{LCM}(\mathrm{LM}(f_2),\ \mathrm{LM}(f_4)) = \mathrm{LCM}(x\,y,\ y^2) = x\,y^2$$

$$\mathrm{LCM}(\mathrm{LM}(f_3),\ \mathrm{LM}(f_4)) = \mathrm{LCM}(x,\ y^2) = x\,y^2$$

We can choose $\{f_2,\ f_4\}$ or $\{f_3,\ f_4\}$ - the lowest in x.

We skip the last one, since the first criteria

$$S(f_2,\ f_4) = \frac{x\,y^2}{x\,y} * (x\,y + 2\,y^2 - 1) - \frac{x\,y^2}{2\,y^2} * (2\,y^2 - 1) = \frac{x}{2} + 2\,y^3 - y$$

$$\frac{x}{2} + 2\,y^3 \; - y \to_x = 2\,y^3 - y \;\to_{2\,y^2-1} \; = 0$$

Two pairs left $\{f_1, \; f_3\}$ and $\{f_1, \; f_4\}$ - the lowest in x. We skip $\{f_1, \; f_4\}$, since the first criteria

$$S(f_1, \; f_3) \; = \; \frac{x^2}{x^2} * \left(x^2 + 2\,x\,y\right) \; - \; \frac{x^2}{x} * (x) \; = 2\,x\,y$$

$$2\,x\,y \;\to_x \; = 0$$

Therefore, here is the basis

$$< x^2 + 2\,x\,y, \;\; x\,y \; + \; 2\,y^2 - 1, \;\; x, \;\; 2\,y^2 - 1 >$$

We can cancel first two polynomials, since they are reduced wrt f_3. Hence

$$< x, \;\; y^2 - \frac{1}{2} >$$

Hilbert's Nullstellensatz

If the ideal is ⟨1⟩ then the polynomials have no common zeros.

Gröbner bases are very useful for solving systems of polynomial equations. Let F be a finite set of polynomials in $K(x_1, \;\; ..., \;\; x_n)$. The variety of F is a set of all common complex zeros:

$$V(F) = \{(z_1, \;\; ..., \; z_n) \;|\; f_k(z_1, \;\; ..., \; z_n) = 0 \text{ for all } f_k \in \; F\}$$

The variety does not change if we replace F by another set of polynomials that generates the same ideal, in particular, by the reduced Gröbner basis. The advantage of G is that it reveals geometric properties of the variety that are not visible from F. What is the size of the variety? Hilbert' s Nullstellensatz implies

The variety V(F) is empty if and only if G = ⟨1⟩

Example.

$$\begin{cases} x + y^2 = 0 \\ -x + y + 1 \; = \; 0 \\ y^3 - y \; = \; 0 \end{cases}$$

```
GroebnerBasis[{x + y^2 == 0, -x + y + 1 == 0, y^3 - y == 0},
  {x, y}]
```

```
{1}
```

```
Solve[{x + y^2 == 0, -x + y + 1 == 0, y^3 - y == 0}, {x, y}]
```

```
{}
```

To count the number of zeros of a given system of equations we need to define a standard monomial.

Definition. Given a fixed ideal $I \subseteq K(x_1, \ldots, x_n)$ and a monomial order, then a monomial $x^\alpha = x_1^{\alpha_1} \ldots x_n^{\alpha_n}$ is called standard if it is not in the leading ideal $\langle LT(I)\rangle$.

Example. Consider $\langle \mathrm{LT}(I)\rangle = < x_1^5 x_2^4 x_3^2 >$, then there are sixty standard monomials.

The variety $V(I)$ is finite if and only if the set of standard monomials is finite, In a univariate case this is the Fundamental Theorem of Algebra, which states that the variety of a univariate polynomial of degree n consists of n complex numbers.

References

[1] D. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Springer-Verlag, 1991.

[2] B. Buchberger, Theoretical Basis for the Reduction of Polynomials to Canonical Forms. *SIGSAM Bull*. **39**(1976), 19-24,

[3] B. Buchberger, A Life Devoted to Symbolic Computation. *Journal of Symbolic Computation*, **41**(2006), 255-258.

[4] Bruno Buchberger's PhD thesis 1965: An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal. *Journal of Symbolic Computation*, **41**(2006), 475-511.