Computer Algebra
Lecture 5

James Davenport

University of Bath

7 September 2018

Solving systems of polynomial equations

The obvious method of solving systems of linear equations is

1. Write as a matrix equation $M.\mathbf{x} = \mathbf{a}$
2. Compute M^{-1}
3. $\mathbf{x} = M^{-1}(M.\mathbf{x}) = M^{-1}\mathbf{a}$

Apart from problems of whether M^{-1} exists, the problem with this if we're doing algebra is that M^{-1} might be huge.A better method is

1. Write as a matrix equation $M.\mathbf{x} = \mathbf{a}$
2. Do Gaussian elimination on $M|\mathbf{a}$ (an $n \times n + 1$ matrix) until the M part is triangular
3. Solve by back-substitution

In fact this is really what we do by hand

Gaussian elimination is intelligent subtracting of one equation from another.

Example (Easy)

Sometimes this works for nonlinear equations: given

$$x^2 - y = 0 \qquad x^2 - z = 0 \qquad y + z = 0,$$

we can subtract the first from the second to get $y - z = 0$, this and the third give $y = 0$ and $z = 0$, and we are left with $x^2 = 0$, so $x = 0$.

Example (Hard)

But what about $x^2 - 1 = 0 \qquad xy - 1 = 0$, We can subtract x times the second equation from y times the first, to get $x - y = 0$. Hence the solutions are $x = \pm 1$, $y = x$.

Where's the algorithm?

Polynomial Ideals

Because we can add/subtract equations, the precise set of equations doesn't really matter. And $L = R$ is the same as $L - R = 0$, so we can treat all equations as $P = 0$.

Definition

Let S be a set of polynomials in the variables $x_1, \ldots, x_n$, with coefficients from R. The *ideal generated by* S, denoted (S), is the set of all finite sums $\sum f_i s_i$: $s_i \in S$, $f_i \in R[x_1, \ldots, x_n]$. If S generates I, we say that S is a *basis* for I.

This is the "set of all equivalent equations", what we want is the equivalent of "upper triangular". There are two such
: Gröbner bases (for distributed polynomials) and Regular Chains (for recursive polynomials).
We will do Gröbner bases [CLO15]

Distributed Polynomials

$\alpha_1 x^{a_1} y^{b_1} z^{c_1} \ldots + \alpha_2 x^{a_2} y^{b_2} z^{c_2} + \cdots$, but in which order?
Do we write $7x^2y^2 + 3xy^{10} + \cdots$, or $3xy^{10} + 7x^2y^2 + \cdots$?

Notation

Our variables are $x_1, \ldots, x_n$, which we will abbreviate to $\mathbf{x}$. Similarly $x_1^{a_1} x_2^{a_2} \ldots x_n^{a_n}$ will be abbreviated $\mathbf{x}^{\mathbf{a}}$. $\mathbf{x}^{\mathbf{a}}$ is a monomial. Write $\overleftarrow{\mathbf{a}}$ for $[a_n, a_{n-1}, \ldots, a_1]$.

To answer the question, we need some order $\succ$ on our monomials, so we always write polynomials ordered by $\succ$ on the monomials. We require two properties:

1. $\forall \mathbf{a} \neq \mathbf{0}$, $1 = \mathbf{x}^{\mathbf{0}} \prec \mathbf{x}^{\mathbf{a}}$;
2. if $\mathbf{x}^{\mathbf{a}} \prec \mathbf{x}^{\mathbf{b}}$, then $\forall \mathbf{c} : \mathbf{x}^{\mathbf{a}}\mathbf{x}^{\mathbf{c}} \prec \mathbf{x}^{\mathbf{b}}\mathbf{x}^{\mathbf{c}} = \mathbf{x}^{\mathbf{b}+\mathbf{c}}$.

Possible Orders

$\prec_{\mathrm{lex}}$ "lexicographic": to compare $\mathbf{a}$ with $\mathbf{b}$, compare a_1 with b_1. If that's a tie, compare a_2 with b_2 etc.

$\prec_{\mathrm{gr}}$ "graded lexicographic": to compare $\mathbf{a}$ with $\mathbf{b}$, compare $\sum a_i$ with $\sum b_i$. If that's a tie, use $\prec_{\mathrm{lex}}$.

$\prec_{\mathrm{tdeg}}$ "total degree": to compare $\mathbf{a}$ with $\mathbf{b}$, compare $\sum a_i$ with $\sum b_i$. If that's a tie, use $\prec_{\mathrm{lex}}$ *backwards*, i.e. $\mathbf{a} \prec_{\mathrm{lex}} \mathbf{b} \Rightarrow \mathbf{b} \prec_{\mathrm{tdeg}} \mathbf{a}$. Many systems actually use $\prec_{\mathrm{lex}}$ on $\overleftarrow{\mathbf{a}}$ and $\overleftarrow{\mathbf{b}}$.

$\prec_{\mathrm{elim}}^{1,2}$ $\prec_1$ on $[a_1, \ldots, a_k]$, with ties broken by $\prec_2$ on $[a_{k+1}, \ldots, a_n]$.

Notation

For a fixed $\prec$, write lm for the leading monomial, and lt for the leading term (i.e. with the coefficient).

But . . .

‘if the order of the variables is reversed, and we then reverse the sense of the answer, what’s the difference?”. Indeed, for two variables, there is no difference. However, with more variables it does indeed make a difference.For three variables, the monomials of degree three are ordered as

$$x^3 > x^2y > x^2z > xy^2 > xyz > xz^2 > y^3 > y^2z > yz^2 > z^3$$

under `grlex`, but as

$$x^3 > x^2y > xy^2 > y^3 > x^2z > xyz > y^2z > xz^2 > yz^2 > z^3$$

under `tdeg`. One way of seeing the difference is to say that `grlex` with $x > y > z$ discriminates *in favour of* x, whereas `tdeg` with $z > y > x$ discriminates *against* z. This metaphor reinforces the fact that there is no difference with two variables.

Reduction

Definition

If $\mathrm{lm}(g)$ divides $\mathrm{lm}(f)$, then we say that g reduces f to $h = \mathrm{lc}(g)f - (\mathrm{lt}(f)/\mathrm{lm}(g))g$, written $f \to^g h$. Otherwise we say that f is *reduced* with respect to g.

If R is a field, division is possible, and so it is more usual to reduce f to $f - (\mathrm{lt}(f)/\mathrm{lt}(g))g.\mathrm{lm}(h) < \mathrm{lm}(f)$

Proposition

Any chain $f_1 \to^g f_2 \to^g f_3 \cdots$ is finite, i.e. terminates in a polynomial h reduced with respect to g. We write $f_1 \overset{*}{\to}^g h$.

These concepts and results extend to reduction by a set G of polynomials, where $f \to^G h$ means $\exists g \in G : f \to^g h$.

Nondeterminacy of $f \to^G h$

But a polynomial can have several reductions with respect to G (one for each element of G whose leading monomial divides the leading monomial of f).
For example, let $G = \{g_1 = x - 1, g_2 = y - 2\}$ and $f = xy$. Then there are two possible reductions of f: $f \to^{g_1} h_1 = f - yg_1 = y$, and $f \to^{g_2} h_2 = f - xg_2 = 2x$. In this case $h_1 \to^{g_2} 2$ and $h_2 \to^{g_1} 2$, so that $f \stackrel{*}{\to}^G 2$ uniquely, but even this need not always be the case.
If we let $G = \{g_1 = x - 1, g_2 = x^2\}$ and $f = x^2 - 1$, then $f \to^{g_2} h_2 = f - g_2 = -1$, whereas $f \to^{g_1} f - xg_1 = x - 1 \to^{g_1} 0$: so $f \stackrel{*}{\to}^G 0$ or -1.

Complete reduction

This definition deals with reduction of the leading monomial of f by g, but it might be that other monomials are reducible. For simplicity we consider the case when R is a field (division is possible).

Definition

If any term cm of f is reducible by g, i.e. the leading monomial of g divides m, we say that g part-reduces f, and write $f \Rightarrow^g f - (cm/\operatorname{lt}(g))g$.

We can continue this process (but only finitely often, by a theorem), until no monomial of f is reducible by g, when we write $f \overset{*}{\Rightarrow}{}^g h$, and say that f is *completely reduced* by g to h.
Again, this extends to reduction by a set of polynomials.
And again, this might not be unique.

More general

Reduction deals with the Easy example, but for Hard we need a new concept.

Definition

Let $f, g \in R[x_1, \ldots, x_n]$. The S-polynomial of f and g, written $S(f, g)$ is defined as

$$S(f,g) = \frac{\mathrm{lt}(g)}{\gcd(\mathrm{lm}(f), \mathrm{lm}(g))} f - \frac{\mathrm{lt}(f)}{\gcd(\mathrm{lm}(f), \mathrm{lm}(g))} g. \qquad (1)$$

These divisions concerned are exact. This generalises reduction in the sense that, if $\mathrm{lm}(g)$ divides $\mathrm{lm}(f)$, then $f \rightarrow^{g} S(f, g)$. As with reduction, the leading monomials in the two components on the righthand side of equation (1) cancel.

Another way of thinking of the S-polynomial is that it is the difference between what you get by reducing $\mathrm{lcm}(\mathrm{lm}(f), \mathrm{lm}(g))$ by f and by g.

The Gröbner Base Theorem [BW93, Proposition 5.38, Theorem 5.48]

Theorem

The following conditions on a set $G \subset R[x_1, \ldots, x_n]$, with a fixed ordering $\prec$ on monomials, are equivalent.

1. $\forall f, g \in G, S(f,g) \overset{*}{\rightarrow}^{G} 0$. *This is known as the S-Criterion.*
2. *If $f \overset{*}{\rightarrow}^{G} g_1$ and $f \overset{*}{\rightarrow}^{G} g_2$, then g_1 and g_2 differ at most by a multiple in R, i.e. $\overset{*}{\rightarrow}^{G}$ is essentially well-defined.*
3. $\forall f \in (G), f \overset{*}{\rightarrow}^{G} 0$.
4. $(\mathrm{lm}(G)) = (\mathrm{lm}((G)))$, *i.e. the leading monomials of G generate the same ideal as the leading monomials of the whole of (G).*

If G satisfies these conditions, G is called a Gröbner base .

Condition 1 is testable, condition 3 says we can check whether any polynomial is in the ideal or not. Condition 4 is vital for proofs.

Completely reduced Gröbner Bases

A particularly useful Gröbner base is a *completely reduced Gröbner base* (abbreviated *crGb*) G, i.e. one where every element is completely reduced with respect to all the others: in symbols

$$\forall g \in G \qquad g \overset{*}{\Rightarrow}^{G\setminus\{g\}} g. \tag{2}$$

For a consistent set of linear polynomials, the crGb would be a set of linear polynomials in one variable each, e.g. $\{x-1, y-2, z-3\}$, effectively the solution.
In general, a monic crGb is a locally canonical form for an ideal: two ideals are equal if, and only if, they have the same crGb (with respect to the same ordering, of course).

Buchberger's Theorem

Theorem (Buchberger)

Every polynomial ideal has a Gröbner base: we will show this constructively for finite sets defining the ideal.

There are typical halting-problem paradoxes with infinite sets of generators.

Algorithm

```
procedure $\textsc{Buchberger}(G_0 \subset R[x_1, \ldots, x_n], \prec)$
    $G := G_0$; $n := |G|$;                $\triangleright$ we consider $G$ as $\{g_1, \ldots, g_n\}$
    $P := \{(i,j) : 1 \le i < j \le n\}$
    while $P \ne \emptyset$ do
        Pick $(i,j) \in P$;
        $P := P \setminus \{(i,j)\}$;
        Let $S(g_i, g_j) \stackrel{*}{\rightarrow}^{G} h$                $\triangleright$ This is where $\prec$ matters
        if $h \ne 0$ then                $\triangleright$ $\mathrm{lm}(h) \notin (\mathrm{lm}(G))$
            $g_{n+1} := h$;                $\triangleright$ $G := G \cup \{h\}$;
            $P := P \cup \{(i, n+1) : 1 \le i \le n\}$;
            $n := n + 1$;
        end if
    end while
    Optionally $G :=$Interreduce$(G)$
end procedure
```

But we wanted to solve equations!

Definition

The set of solutions over K of an ideal I is called the *variety* of I, written $V(I)$. If S is a set of polynomials which generates I, so $I = \langle S \rangle$, we will write $V(S)$ as shorthand for $V(\langle S \rangle)$.

We should note that two different ideals can have the same variety, e.g. (x) and (x^2) both have the variety $x = 0$, but the solution has different multiplicity.
However, the two ideals $(x^2 + y^2)$ and (x, y) both have only the solution $x = y = 0$ *over the reals*, but over the complexes the first has the solutions $x = \pm iy$, and hence the varieties are different.

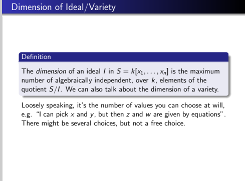
Dimension of Ideal/Variety

Definition

The *dimension* of an ideal I in $S = k[x_1, \ldots, x_n]$ is the maximum number of algebraically independent, over k, elements of the quotient S/I. We can also talk about the dimension of a variety.

Loosely speaking, it's the number of values you can choose at will, e.g. "I can pick x and y, but then z and w are given by equations". There might be several choices, but not a free choice.

└Dimension of Ideal/Variety



Dimension of Ideal/Variety

Definition

The *dimension* of an ideal I in $S = k[x_1, \ldots, x_n]$ is the maximum number of algebraically independent, over k, elements of the quotient S/I. We can also talk about the dimension of a variety.

Loosely speaking, it's the number of values you can choose at will, e.g. "I can pick x and y, but then z and w are given by equations". There might be several choices, but not a free choice.

For linear equations, dimension is easy: in upper triangular form it's the number of x_i without values. $\begin{pmatrix} 2 & 1 & 1 \\ 0 & 2 & 4 \\ 0 & 0 & 0 \end{pmatrix}$ doesn't determine the last variable. The solution is a 1-dimensional set, i.e.a line.

In the non-linear it's similar: it's the maximum number of undetermined variables. $\left\{ \begin{array}{c} x^2 + 2 * x * y - z \\ 2y - z \end{array} \right.$ doesn't determine z at all, but given z determines $y = z/2$ and then x, so it's a curve.

No solutions in K

Here the crGb will be $\{1\}$, or more generally $\{c\}$ for some non-zero constant c.
The existence of a solution would imply that this constant was zero, so there are no solutions.
The dimension is undefined, but normally written as -1.

A finite number of solutions in K

There is a neat generalisation of the result that a polynomial of degree n has n roots.

Proposition

If it's finite, the number (counted with multiplicity) of solutions of a system with Gröbner basis G is equal to the number of monomials which are not reducible by G.

It follows from this that, if (and only if) there are finitely many solutions, every variable x_i must appear alone, to some power, as the leading monomial of some element of G.
In this case, the dimension is zero.

An infinite number of solutions in K

Then some variables do not occur alone, to some power, as the leading monomial of any element of G.

In this case, the dimension is greater than zero.

While 'dimension' is a convenient generalisation of the linear case, many more things can happen in the non-linear case.

If the dimension of the ideal is d, there must be at least d variables which do not occur alone, to some power, as the leading monomial of any element of G.

However, if $d > 0$, there may be more.

Consider the ideal $(xy - 1) \subset k[x, y]$. $\{xy - 1\}$ is already a Gröbner base, and neither x nor y occur alone, to any power, in a leading term (the only leading term is xy).

However, the dimension is 1, not 2, because fixing x determines y, and *vice versa*, so there is only one independent variable.

It's pretty weird

There are other phenomena that occur with nonlinear equations that cannot occur with linear equations.
Consider the ideal

$$\langle (x+1-y)(x-6+y), (x+1-y)(y-3) \rangle$$

(where the generators we have quoted do in fact form a Gröbner base, at least for `plex(x,y)` and `tdeg(x,y)`, and the leading monomials are x^2 and xy).
x occurs alone, but y does not, so in fact this ideal has dimension greater than 0 but at most 1, i.e. dimension 1.
But the solutions are $x = y - 1$ (a straight line) *and* the point $(3, 3)$. Such ideals are said to be of *mixed* dimension, and are often quite messy to work with.

Reduce [HS18, Section 16.28]

```
load_package groebner;
```

`torder(vl,m);` `vl` list of variables
with $m \in \{\texttt{lex}, \texttt{gradlex}, \texttt{revgradlex}\} = \{\prec_{\rm lex}, \prec_{\rm gr}, \prec_{\rm tdeg}\}$

An example

$$
\begin{aligned}
x^2 - 1 &= 0 && (3)\\
y^2 - 1 &= 0 && (4)\\
(x-1)(y-1) &= 0 && (5)
\end{aligned}
$$

Solutions:
$(-1,1), (1,-1), (1,1)$
These equations *are* the simplest description of this variety.
Solve equation (3).

- $x = 1$ (5) disappears, and we are left with (4): $y = \pm 1$.
- $x = -1$ (5) becomes $-2(y-1) = 0$, so $y = 1$, which also satisfies (4).

A bigger example

$$\begin{aligned} x^{2000}-1 &= 0 \qquad (6)\\ y^{2000}-1 &= 0 \qquad (7)\\ (x^{1000}-1)(y^{1000}-1) &= 0 \qquad (8)\end{aligned}$$

We could consider each solution of (6) separately, but this is boring.

Instead consider

$\gcd(x^{2000}-1, \mathrm{lc}_y((x^{1000}-1)(y^{1000}-1))) = x^{1000}-1$.

Then we have the same case analysis as before.

Can we generalise?

For zero-dimensional ideals, with a `lex` ordering a Gröbner base has to look like.

$$\begin{gathered}
p_n(x_n) \\
p_{n-1,1}(x_{n-1},x_n),\ldots,p_{n-1,k_{n-1}}(x_{n-1},x_n), \\
p_{n-2,1}(x_{n-2},x_{n-1},x_n),\ldots,p_{n-2,k_{n-2}}(x_{n-2},x_{n-1},x_n), \\
\ldots \\
p_{1,1}(x_1,\cdots,x_{n-1},x_n),\ldots,p_{1,k_1}(x_1,\cdots,x_{n-1},x_n),
\end{gathered}$$

where k_i is the number of polynomials involving x_i but not any x_j for $j<i$ and

$$\deg_{x_i}(p_{i,j}) \le \deg_{x_i}(p_{i,j+1}) \tag{9}$$

and p_{i,k_i} is monic in x_i.

Criteria

There are two criteria which make Buchberger's algorithm faster.

Proposition (Buchberger's gcd (or First) Criterion [Buc79])

If

$$\gcd(\mathrm{lm}(f), \mathrm{lm}(g)) = 1, \tag{10}$$

then $S(f,g) \overset{*}{\rightarrow}^{\{f,g\}} 0$ *(so needn't be computed).*

Proposition (Buchberger's lcm (or Third) Criterion [Buc79])

If $I = (B)$ *contains* f, g, h *and the reductions under* $\overset{*}{\rightarrow}^{B}$ *of* $S(f,g)$ *and* $S(f,h)$, *(i.e. we've already computed* $S(f,g)$ *and* $S(f,h)$*) and if both* $\mathrm{lcm}(\mathrm{lm}(f), \mathrm{lm}(g))$ *and* $\mathrm{lcm}(\mathrm{lm}(f), \mathrm{lm}(h))$ *divide* $\mathrm{lcm}(\mathrm{lm}(g), \mathrm{lm}(h))$, *then* $S(g,h) \overset{*}{\rightarrow}^{B} 0$, *and hence need not be computed.*

Bibliography I

B. Buchberger.
A Criterion for Detecting Unnecessary Reductions in the Construction of Groebner Bases.
In *Proceedings EUROSAM 79*, pages 3–21, 1979.

T. Becker and V. (with H. Kredel) Weispfenning.
Groebner Bases. A Computational Approach to Commutative Algebra.
Springer Verlag, 1993.

D.A. Cox, J. Little, and D. O'Shea.
Ideals, Varieties, and Algorithms.
Undergraduate Texts in Mathematics. Springer, Heidelberg, 2015.

Bibliography II

A.C. Hearn and R. Schöpf.
REDUCE User's Manual (Free Version; June 8, 2018).
http://reduce-algebra.sourceforge.net/, 2018.