

Minicourse  
University of Maryland  
Second Lecture  
Applications of Gröbner Bases

William W. Adams

March 9, 2005

## PART I: Review of a Gröbner bases.

Let  $k$  be a field and let  $k[x_1, \dots, x_n]$  be the polynomial ring in  $n$  variables.

We first assume that we have a term order on  $k[x_1, \dots, x_n]$ , that is a *total* order  $<$  on the power products of  $k[x_1, \dots, x_n]$  such that for all power products  $X, X_1, X_2$  we have

1.  $1 \leq X$

2.  $X_1 \leq X_2 \implies XX_1 \leq XX_2$

Given  $f = cX + \text{lower terms}$ , where  $c \in k$ ,  $c \neq 0$  and  $X$  is a power product, we define

$\text{lt}(f) = cX =$  the leading term of  $f$

$\text{lp}(f) = X =$  the leading power product of  $f$

$\text{lc}(f) = c =$  the leading coefficient of  $f$ .

Example.  $f = 7x_1^3x_2 + 5x_1^3x_3 + 8x_1^2x_2^3x_4^5$  with respect to the lexicographic term order

$$\text{lt}(f) = 7x_1^3x_2$$

$$\text{lp}(f) = x_1^3x_2$$

$$\text{lc}(f) = 7.$$

Also for a subset  $\Omega \subseteq k[x_1, \dots, x_n]$  we set

$$\text{Lt}(\Omega) = \langle \text{lt}(f) \mid f \in \Omega \rangle$$

We define division for multivariate polynomials.

Given  $f, g \in k[x_1, \dots, x_n]$  we write

$$f \xrightarrow{g} h$$

provided that  $h = f - cXg$  where  $c \neq 0$  is in  $k$  and  $X$  is a power product and  $cX\text{lt}(g)$  is a non-zero term of  $f$ .

We note that last time we restricted this to the statement  $h = f - \frac{\text{lt}(f)}{\text{lt}(g)}g$  where we used the leading term of  $g$  to cancel the leading term of  $f$  instead of cancelling any term of  $f$ .

Further if  $F = \{f_1, \dots, f_s\}$ , we write

$$f \xrightarrow{F}_+ h$$

provided that

$$\begin{aligned} f &\xrightarrow{f_{i_1}} h_1 \xrightarrow{f_{i_2}} h_2 \cdots \\ &\cdots \xrightarrow{f_{i_{\ell-1}}} h_{\ell-1} \xrightarrow{f_{i_\ell}} h \end{aligned}$$

(We say  $f$  reduces to  $h$ .)

Define for two polynomials  $f_1, f_2 \in k[x_1, \dots, x_n]$  and

$$X = \text{lcm}(\text{lp}(f_1), \text{lp}(f_2))$$

the S-polynomial of  $f_1, f_2$  by

$$S(f_1, f_2) = \frac{X}{\text{lt}(f_1)} f_1 - \frac{X}{\text{lt}(f_2)} f_2.$$

Also define  $r \in k[x_1, \dots, x_n]$  to be *reduced* with respect  $G = \{g_1, \dots, g_t\}$  provided no  $g_i \in G$  can be used to reduce  $r$ .

We now characterize Gröbner bases.

**THEOREM:** Let  $G = \{g_1, \dots, g_t\} \subseteq k[x_1, \dots, x_n]$  be a finite subset and let  $I = \langle G \rangle$ . Call  $G$  a Gröbner basis for  $I$  provided any one of the following conditions hold:

1. For all  $f \in I$  we have  $f \xrightarrow{G}_+ 0$ .
2. For all  $f \in I$  there is an  $i$  such that  $\text{lp}(g_i) | \text{lp}(f)$ .
3.  $\text{Lt}(G) = \text{Lt}(I)$ .
4. For all  $i, j$  we have  $S(g_i, g_j) \xrightarrow{G}_+ 0$ .
5. For all  $f \in k[x_1, \dots, x_n]$  there is a *unique* reduced  $r \in k[x_1, \dots, x_n]$  such that  $f \xrightarrow{G}_+ r$ .
6. For all  $f \in I$  we can write  $f = \sum_{i=1}^t h_i g_i$  where  $h_i \in k[x_1, \dots, x_n]$  and
 
$$\text{lp}(f) = \max(\text{lp}(h_i g_i) | 1 \leq i \leq t).$$

**THEOREM:** (Bruno Buchberger, 1965) Every ideal in  $k[x_1, \dots, x_n]$  has a Gröbner basis and it is effectively computable.

**Definition** A Gröbner basis  $G = \{g_1, \dots, g_t\}$  is called *reduced* provided for each  $i = 1, \dots, t$ ,  $g_i$  is monic and reduced with respect to the remaining  $g_j$ 's.

**THEOREM:** Given an ideal  $I$  in  $k[x_1, \dots, x_n]$  and a term order  $<$  on  $k[x_1, \dots, x_n]$ , then  $I$  has a *unique* reduced Gröbner basis with respect to  $<$ .

We mention a couple of difficulties that arise during the computation of Gröbner bases, namely, the possible rapid growth of the degrees and coefficients of the S-polynomials. Even though the degree and/or size of the coefficients of the original polynomials and the Gröbner basis may be of modest size, the intermediary polynomials generated by the S-polynomial computations and reductions can become quite large. This can dramatically slow down the computation. Doing computations with large coefficients can be very costly because of the large amount of arithmetic that becomes necessary.

As an example of this situation, the reduced Gröbner basis for the ideal

$$\langle 4x^2y^2 + 3x, y^3 + 2xy, 7x^3 + 6y \rangle$$

with respect to the lex order with  $x > y$  is  $\{x, y\}$ , while the coefficients during the computation grow as large as  $10^8$ . This can be seen by expressing  $x$  as a linear combination of the three original polynomials  $f_1 = 4x^2y^2 + 3x$ ,  $f_2 = y^3 + 2xy$ , and  $f_3 = 7x^3 + 6y$ :

$$\begin{aligned}
x = & \left( \frac{7}{54}x^2y^5 - \frac{401408}{56428623}y^{10} - \frac{1835008}{56428623}y^9 \right. \\
& - \frac{9604}{18809541}y^8 - \frac{43904}{18809541}y^7 - \frac{200704}{18809541}y^6 + \frac{1}{3} \left. \right) f_1 \\
& + \left( -\frac{7}{27}x^3y^6 + \frac{1605632}{56428623}x^2y^9 + \frac{7340032}{56428623}x^2y^8 \right. \\
& + \frac{38416}{18809541}x^2y^7 + \frac{175616}{18809541}x^2y^6 + \frac{401408}{18809541}xy^7 \\
& \left. - \frac{2}{3}xy + \frac{917504}{18809541}y^8 \right. \\
& + \frac{4802}{6269847}y^7 + \frac{21952}{6269847}y^6 + \frac{100352}{6269847}y^5 + \frac{1}{3}y^3 \left. \right) f_2 \\
& - \frac{1}{112857246}y^5(917504y^5 + 14406y^4 + 65856y^3 \\
& \left. + 301056y^2 + 6269847)f_3.
\end{aligned}$$

Total degree can become very large. For example consider the ideal

$$I = \langle x^7 + xy + y, y^5 + yz + z, z^2 + z + 1 \rangle \subseteq \mathbb{Q}[x, y, z].$$

The generators of this ideal have maximum total degree 7. However the reduced Gröbner basis for  $I$  with respect to lex with  $z > y > x$  contains a polynomial of degree 70. The problem with polynomials with large total degree is the fact that they can have a very large number of terms. For example, the reduced Gröbner basis for the ideal  $I$  above has 3 polynomials with 58, 70, and 35 terms respectively.

You can see that this kind of thing *must* occur. In LEX with  $x$  as the smallest variable we will get as solutions to the polynomial in  $x$  alone all of the  $x$  coordinates of all of the solutions. Looking at the degrees of the original polynomials we see we might expect 70 different solutions.

## **PART II: Elementary Applications of Gröbner bases.**

### Ideal Equality.

Problem: Given two ideals  $I, J$  in  $k[x_1, \dots, x_n]$  determine if they are equal.

Solution: All computer algebra systems compute *reduced* Gröbner bases (maybe with a special command). Since these are unique we can compare them for the answer.

## Existence of Solutions.

Problem: Given an ideals  $I$  in  $k[x_1, \dots, x_n]$  determine whether or not  $V(I)$  has solutions in  $\bar{k}^n$ .

Recall, that  $V(I)$  is defined to be all  $\alpha \in \bar{k}^n$  such that  $f(\alpha) = 0$  for all  $f \in I$ .

Solution: The Weak Hilbert

NullstellenSatz says that  $V(I)$  is non-empty for *all* proper ideals of  $k[x_1, \dots, x_n]$ . So the questions amounts to deciding when an ideal  $I = k[x_1, \dots, x_n]$ .

If  $G$  is a Gröbner basis of  $I$  then  $1 \in I$  if and only if  $1 \xrightarrow{G} + 0$  and so we see we must have  $1 \in G$  (or any unit) and so if  $G$  is reduced we get  $G = \{1\}$ .

## Ideal Membership.

Problem: Given an ideal  $I \subseteq k[x_1, \dots, x_n]$  say,  $I = \langle f_1, \dots, f_s \rangle$ , and given  $f \in k[x_1, \dots, x_n]$  determine whether  $f \in I$  and if so compute  $h_1, \dots, h_s \in k[x_1, \dots, x_n]$  such that  $f = h_1 f_1 + \dots + h_s f_s$ .

Problem:

1. Determine a Gröbner basis  $G = \{g_1, \dots, g_t\}$  for  $I$
2. See if  $f \xrightarrow{G} + 0$  and if so use this computation to find  $a_1, \dots, a_t$  such that  $f = a_1 g_1 + \dots + a_t g_t$ .
3. Do the bookkeeping in the Buchberger algorithm to get the  $g_i$ 's in terms of the  $f_i$ 's to get  $f = h_1 f_1 + \dots + h_s f_s$ .

Example: Let  $I = \langle f_1, f_2 \rangle$  where  $f_1 = xy - x$  and  $f_2 = x^2 - y$  are in  $k[x, y]$ . We use DegLex with  $x < y$ . We then compute

$$S(f_1, f_2) = xf_1 - yf_2 = y^2 - x^2 := f_3.$$

Then one readily checks that  $G = \{f_1, f_2, f_3\}$  is a Gröbner basis for  $I$ . Let us take

$$f = 3x^2y^2 - x^4 - y^3 - x^2y + y^2 - xy - x^2 + x.$$

Then

$$\begin{aligned} f &\xrightarrow{3xy, f_1} -x^4 - y^3 + 2x^2y + y^2 - xy - x^2 + x \\ &\xrightarrow{-x^2, f_2} -y^3 + x^2y + y^2 - xy - x^2 + x \\ &\xrightarrow{-y, f_3} y^2 - xy - x^2 + x \\ &\xrightarrow{-1, f_3} -xy + x \xrightarrow{-1, f_1} 0. \end{aligned}$$

Following the reductions above we see that

$$f = (3xy - 1)f_1 - x^2f_2 - (y - 1)f_3.$$

Then using the expression for  $f_3 = xf_1 - yf_2$  used above, we get

$$f = (2xy + x - 1)f_1 + (y^2 - x^2 - y)f_2.$$

## Radical Membership.

Problem: Given an ideal  $I \subseteq k[x_1, \dots, x_n]$  determine whether  $f \in \sqrt{I}$ . Recall that

$$\sqrt{I} = \{h \in k[x_1, \dots, x_n] \mid h^m \in I \text{ with } m \in \mathbf{N}\}.$$

So the problem, by the Hilbert Nullstellensatz, is to decide whether  $f$  vanishes on  $V(I)$ .

Solution: Take a new variable  $y$ . It is not hard to show that  $f \in \sqrt{I}$  if and only if

$$J := \langle I, 1 - yf \rangle$$

is the unit ideal in  $k[x_1, \dots, x_n, y]$ . So compute a Gröbner basis of  $J$  with respect to any order and see if it contains an element of  $k^*$  (i.e. if the reduced Gröbner basis contains  $\{1\}$ ).

Note: Actually determining a Gröbner basis for  $\sqrt{I}$  can be done, but requires a much more sophisticated procedure.

## Basis of $k[x_1, \dots, x_n]/I$ .

Problem: Given an ideal  $I \subseteq k[x_1, \dots, x_n]$  find a  $k$ -basis of  $k[x_1, \dots, x_n]/I$  that allows us to compute in this ring.

Solution: Let  $G = \{g_1, \dots, g_t\}$  be a Gröbner basis for  $I$  with respect to any term order. Then we know that for all  $f \in k[x_1, \dots, x_n]$  we can reduce  $f$  until it is “reduced” that is there is a unique polynomial  $r \in k[x_1, \dots, x_n]$  such that  $f \xrightarrow{G} r$  such that no  $\text{lp}(g_i)$  divides *any* term of  $r$ . Denote this element by  $n(f)$  (with the term order and ideal understood). This statement implies the power products occurring in such a reduced polynomial are linear independent in  $k[x_1, \dots, x_n]/I$ .

Hence The power products not divisible by any  $\text{lp}(g_i)$  ( $1 \leq i \leq t$ ) form a  $k$  basis of  $k[x_1, \dots, x_n]/I$ . Also the multiplication in  $k[x_1, \dots, x_n]/I$  is obtained by multiplying the two power products and reducing with  $G$ .

Example:  $I = \langle xy - x, x^2 - y \rangle$  We saw before that a Gröbner basis for this ideal (actually interreducing the one given there) is  $G = \{xy - x, x^2 - y, y^2 - y\}$ . The set of power products not divisible by these leading terms ( $\{xy, x^2, y^2\}$ ) would be simply  $1, x, y$ .

We get the multiplication table by  $x^2 \longrightarrow y$ ,  $xy \longrightarrow x$ , and  $y^2 \longrightarrow y$ .

So we get:

$$\begin{array}{c}
 \mathbf{1} \\
 \mathbf{x} \\
 \mathbf{y}
 \end{array}
 \left\| \begin{array}{c}
 \mathbf{1} \\
 \mathbf{x} \\
 \mathbf{y}
 \end{array} \right\|
 \begin{array}{c}
 \mathbf{x} \\
 \mathbf{y} \\
 \mathbf{x}
 \end{array}
 \left\| \begin{array}{c}
 \mathbf{y} \\
 \mathbf{x} \\
 \mathbf{y}
 \end{array} \right.$$

Example above: Invert  $y + x + 1 + I$  if you can.  
I.e. find  $a, b, c \in k$  with

$$(ay + bx + c)(y + x + 1) \equiv 1 \pmod{I}$$

Use the multiplication table above and solve the linear equations for  $a, b, c$  if there is a solution. In this case we get the inverse to be  $-\frac{1}{3}y - \frac{1}{3}x + 1$ .

OR:  $f$  has an inverse in  $k[x_1, \dots, x_n]/I$  if and only if  $\langle I, f \rangle = \langle 1 \rangle$ . So find a reduced Gröbner basis  $G$  for  $\langle I, f \rangle$  and then  $f$  has an inverse if and only if  $G = \{1\}$ . In this case write 1 in terms of  $f$  and the generating set of  $I$ , as we did in the previous example and you have the inverse.

### 3-Color a Graph.

Problem: Given a graph  $K$ , find an assignment of 3 colors to the vertices of  $K$  such that two vertices connected by an edge have different colors.

Solution: Let  $\zeta = e^{\frac{2\pi i}{3}}$  and assign to each vertex one of  $1, \zeta, \zeta^2$  (representating the 3 colors). For the  $n$  vertices of  $K$  labeled by the variables  $x_1, \dots, x_n$  So the condition that we assign a vertex a cube root of unity means we must have  $x_i^3 - 1 = 0$  for  $i = 1, \dots, n$ . Now the condition that adjacent vertices  $i, j$  have assigned a different root of unity is characterized by the equation  $x_i^2 + x_i x_j + x_j^2 = 0$ . Let  $I$  be the ideal in  $k[x_1, \dots, x_n]$  generated by these polynomials. So  $K$  is 3-colorable if and only if  $V(I) \neq \emptyset$  if and only if  $I \neq \langle 1 \rangle$  if and only if the reduced Gröbner basis of  $I$  is not  $\{1\}$ . In this case we can solve the equations to get a specific coloring.

Example:

A GRAPH WITH 8 VERTICES WAS  
DRAWN IN HERE

You can determine the graph from the  
equations below.

So

$$I = \langle a^3 - 1, b^3 - 1, c^3 - 1, d^3 - 1, e^3 - 1, f^3 - 1, g^3 - 1, h^3 - 1, a^2 + ab + b^2, a^2 + ah + h^2, b^2 + bh + h^2, b^2 + bg + g^2, b^2 + bf + f^2, c^2 + cf + f^2, c^2 + cd + d^2, d^2 + de + e^2, d^2 + df + f^2, e^2 + eg + g^2 \rangle$$

Then a Gröbner basis  $G$  for  $I$ , using CoCoA with Lex and  $a > b > c > d > e > f > g > h$  is given by

$$G = \{h^3 - 1, g^2 + gh + h^2, a - g, b + g + h, f^2 - fg - fh + gh, e^2 + eg - gh - h^2, d^2 + dh - ef + eh + fh, c + d + f, de - dh + ef - eg - eh - fh + gh + h^2, df - dh + ef - eh + fg - gh\}.$$

So a solution exists.

## Hilbert Polynomial.

Let  $I \subseteq A = k[x_0, x_1, \dots, x_n]$  be a homogeneous ideal (i.e. generated by homogeneous polynomials). Then  $I$  defines a projective variety,  $V$ , in projective space  $\mathbf{P}^n$ . Let  $A_d$  be the  $k$ -space of homogeneous polynomials of degree  $d$  and let  $I_d = A_d \cap I$ . Then  $I = \bigoplus_{d \geq 0} I_d$  and  $A/I = \bigoplus_{d \geq 0} A_d/I_d$ . Set  $h_I(d) = \dim_k A_d/I_d$ . It can be proved that for all  $d$  large,  $h_I(d)$  is a polynomial (called the Hilbert Polynomial of  $V$ ). It contains important information about  $V$ . Say, for  $d$  large that

$$h_I(d) = a_m d^m + \dots + a_0.$$

- $m = \dim V$
- $m!a_m = \deg V$
- $(-1)^m(a_0 - 1) = \text{arithmetic genus of } V$

So the question would be how to compute  $h_I(d)$ .

1. Theorem(Macaulay):  $h_I(d) = h_{\text{Lt}(I)}(d)$
2. Compute a Gröbner basis  $g_1, \dots, g_t$  of  $I$ .  
So  $\text{Lt}(I) = \langle \text{lt}(g_1), \dots, \text{lt}(g_t) \rangle$ .
3. Now we have a fairly straight forward combinatorial problem (Mora).

## Singular Locus.

Let  $I = \langle f_1, \dots, f_s \rangle$  and let  $p \in V(I) \subseteq \bar{k}^n$ . Let  $T_p =$  tangent space at  $p =$  space of vectors  $\perp$  to  $\nabla f_1(p), \dots, \nabla f_s(p)$ . Call  $p$  a singular point of  $V$  provided  $\dim T_p > \dim_p V$ . This is true if and only if  $\text{rank} \left[ \frac{\partial f_i}{\partial x_j}(p) \right] < n - \dim_p V$ , which is equivalent to  $p$  is in the variety of  $\text{Jac}(V) := \langle f_1, \dots, f_s, \text{all } n - d \text{ sized minors of } \left[ \frac{\partial f_i}{\partial x_j}(p) \right] \rangle$ . Call the variety of  $\text{Jac}(V)$  the singular locus of  $V$ .

Example: Consider  $I = \langle w^3 - x^4, y^4 - wx^3 \rangle$ .

$$\text{Jacobian Matrix} = \begin{bmatrix} 3w^3 & -4x^3 & 0 & 0 \\ -z^3 & 0 & 4y^3 & -3wz^2 \end{bmatrix}.$$

We get the Gröbner basis of  $\text{Jac}(V)$ :

$$w^3 - x^4, y^4 - wz^3, w^2y^3, x^4z^2, x^3z^3, x^3y^3, wx^3z^2$$

We get that the singular locus is

$$V(w, x, y) \cup V(y, z, w^3 - x^4).$$

## PART III: Elimination.

For Elimination we consider only LEX (more generally we could use an “Elimination Order”)

Basic Theorem: Given an ideal  $I \subseteq k[x_1, \dots, x_n]$  let  $G$  be a Gröbner basis with respect to LEX with  $x_1 < x_2 < \dots < x_n$ . Then for  $1 \leq m \leq n$  we have  $G \cap k[x_1, \dots, x_m]$  is a Gröbner basis for  $I \cap k[x_1, \dots, x_m]$ .

Proof: If  $f \in I \cap k[x_1, \dots, x_m]$  then  $f \in I$  implies  $f \xrightarrow{G}_+ 0$ . But any  $g_j$  with any term containing an  $x_i$  with  $i > m$  must have an  $x_i$  with  $i > m$  in  $\text{lp}(g_j)$  and so could not help in  $f \xrightarrow{G}_+ 0$ . Q.E.D.

This property has many applications, as we shall see. But I recall that LEX tends to be expensive to compute.

NOTE: This procedure corresponds to the *projection*  $V(I) \longrightarrow \bar{k}^m$ .

## Minimal Polynomials.

Problem: Given a field extension  $\mathbf{Q}(\alpha)$  of  $\mathbf{Q}$  let  $\beta \in \mathbf{Q}(\alpha)$ . Find the minimal polynomial of  $\beta$ .

Example: Suppose the minimal polynomial of  $\alpha$  is  $x^5 - x - 2$  and let  $\beta = \frac{1}{\alpha}(1 - \alpha - 2\alpha^3)$ . We see that  $(\alpha, \beta)$  is a zero of the ideal  $I = \langle x^5 - x - 2, xy + 2x^3 + x - 1 \rangle$ .

So any polynomial in  $y$  alone in  $I$  has  $\beta$  as a root. We will obtain such a polynomial by computing the Gröbner basis of  $I$  with respect to a LEX ordering with  $x > y$ . We do this and get  $G = \{g_1, g_2\}$  where

$$g_1 = x - \frac{1438}{45887}y^4 - \frac{2183}{45887}y^3 + \frac{10599}{45887}y^2 - \frac{8465}{45887}y - \frac{101499}{45887}$$

and

$$g_2 = y^5 + \frac{11}{2}y^4 + 4y^3 - 5y^2 + 95y + 259.$$

The latter is clearly the minimal polynomial of  $\beta$  since it has degree 5, the degree of  $\beta$  (it is 1 or 5 and it is not 1).

If we wanted only  $g_2$  there appears to be a lot of wasted computation in computing  $g_1$ . This is a common problem in using Gröbner bases.

## Ideal Intersections and Quotients.

Let  $I, J \subseteq k[x_1, \dots, x_n]$  be two ideals. We would like to compute  $I \cap J$ . This corresponds to  $V(I) \cup V(J)$ . It is not hard to prove that for a new variable  $y$

$$I \cap J = \langle yI, (1 - y)J \rangle \cap k[x_1, \dots, x_n].$$

This can be computed using LEX with  $x_1 < \dots < x_n < y$ .

So also if  $f, g \in k[x_1, \dots, x_n]$  we can compute  $\gcd(f, g)$  since  $\langle f \rangle \cap \langle g \rangle = \langle \text{lcm}(f, g) \rangle$ .

Now set  $J : I = \{g \in k[x_1, \dots, x_n] \mid gI \subseteq J\}$ . This procedure corresponds to considering the set theoretic difference of  $V(I)$  and  $V(J)$ . We have for  $I = \langle f_1, \dots, f_s \rangle$ ,  $J : I = \bigcap J : f_i$  and that  $J : f = \frac{1}{f}(J \cap \langle f \rangle)$ . So this may be computed as well.

## Image of a Polynomial Map.

Problem: Given  $\phi : \bar{k}^n \longrightarrow \bar{k}^m$ , a polynomial map, say

$$\phi(x_1, \dots, x_n) = (f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n))$$

with  $f_1, \dots, f_m \in k[x_1, \dots, x_n]$ , find the image of  $\phi$ . That is, viewing  $\phi$  as parameterizing the variety in  $\bar{k}^m$  find the equations of this variety. This amounts to finding the ideal in  $k[x_1, \dots, x_n]$  of relations among the  $f_1, \dots, f_m$ . Or find the kernel of the  $k$ -algebra homomorphism  $\Phi : k[y_1, \dots, y_m] \longrightarrow k[x_1, \dots, x_n]$  defined by  $y_j \mapsto f_j$  ( $1 \leq j \leq m$ ).

Solution: We consider the graph of  $\phi$  in  $\bar{k}^{m+n}$  defined by the ideal

$$I = \langle y_1 - f_1(x_1, \dots, x_n), \dots, y_m - f_m(x_1, \dots, x_n) \rangle.$$

Considering the projection map  $\pi : \bar{k}^{m+n} \longrightarrow \bar{k}^m$  given by  $(x_1, \dots, x_n, y_1, \dots, y_m) \mapsto (y_1, \dots, y_m)$ . We see that the image of  $\phi$  is just  $\pi(V(I))$ . We can compute this by elimination, i.e. by computing  $I \cap k[y_1, \dots, y_m]$ .

## Tangent Surface to the Twisted Cubic.

This will also be an illustration of the previous slide.

Consider the variety  $V = V(y - x^2, y - x^3)$ . We parameterize  $V : x = t, y = t^2, z = t^3$ . Then the tangent line to  $V$  at  $(t, t^2, t^3)$  is  $(t, t^2, t^3) + (1, 2t, 3t^2)u$  and so is parametrized by

$$x = t + u, y = t^2 + 2tu, z = t^3 + 3t^2u.$$

This is the same problem we had on the previous slide and we find the equation of this tangent surface by eliminating  $t, u$ , that is by computing

$$\langle x - t - u, y - t^2 - 2tu, z - t^3 - 3t^2u \rangle \cap k[x, y, z].$$

We obtain the equation

$$-\frac{4}{3}x^3z + x^2y^2 - \frac{4}{3}y^3 + 2xyz - \frac{1}{3}z^2 = 0.$$

## Image of a Variety.

Problem: Given  $\phi : \bar{k}^n \longrightarrow \bar{k}^m$ , a polynomial map as above assume that  $Y \subseteq \bar{k}^n$  is a variety. Find the ideal  $I$  of  $\phi(Y)$ .

Solution: Say  $Y = V(J)$  where  $J = \langle h_1, \dots, h_r \rangle$ . Let  $Z = V(y_1 - f_1, \dots, y_m - f_m, h_1, \dots, h_r)$ , and one can check that  $\phi(Y) = \pi(Z)$  where  $\pi$  is the corresponding projection. So we need to compute

$$I = \langle y_1 - f_1, \dots, y_m - f_m, h_1, \dots, h_r \rangle \cap k[y_1, \dots, y_m].$$

Example: This is from the instructions in Macaulay.

Let  $Y = V(x_2^2 x_3 - x_1^3 - x_1 x_3^2)$  and  $\phi(x_1, x_2, x_3) = (x_1^2, x_1 x_2, x_1 x_3, x_2^2, x_2 x_3, x_3^2)$ . Then

$$\begin{aligned} & \langle y_1 - x_1^2, y_2 - x_1 x_2, y_3 - x_1 x_3, y_4 - x_2^2, y_5 - x_2 x_3, \\ & y_6 - x_3^2, x_2^2 x_3 - x_1^3 - x_1 x_3^2 \rangle \cap k[y_1, \dots, y_6] = \\ & \langle y_4 y_6 - y_5^2, y_2 y_6 - y_3 y_5, y_1 y_6 - y_3^2, y_2 y_5 - y_3 y_4, \\ & y_1 y_5 - y_2 y_3, y_1 y_4 - y_2^2, y_1 y_3 + y_3 y_6 - y_4 y_6, \\ & y_1 y_2 + y_2 y_6 - y_4 y_5, y_1^2 + y_1 y_6 - y_2 y_5 \rangle. \end{aligned}$$

## Secant Variety.

As another example of the above, say  $V \subseteq \bar{k}^n$  is a variety. Then a secant line of  $V$  is a line  $\overline{pq}$  where  $p, q \in V$  (or a limit of such lines). Set  $\text{Sec } V$  equal the union of all such lines.

We have  $\phi : \bar{k}^n \times \bar{k}^n \times \bar{k} \longrightarrow \bar{k}^n$  given by  $\phi(p, q, t) = (tp + (1 - t)q)$  and  $\phi(V \times V \times \bar{k}) = \text{Sec } V$ . So if  $V = V(h_1, \dots, h_r)$  then

$$\begin{aligned} I_{\text{Sec } V} = & \langle tx_1 + (1 - t)y_1 - z_1, \dots, tx_n + (1 - t)y_n - z_n, \\ & h_1(x_1, \dots, x_n), \dots, h_r(x_1, \dots, x_n), \\ & h_1(y_1, \dots, y_n), \dots, h_r(y_1, \dots, y_n) \rangle \\ & \cap k[z_1, \dots, z_n]. \end{aligned}$$