Gröbner Bases: a Tutorial

Mike Stillman

These notes are based on lectures given in Berkeley at M.S.R.I. in August 1998. They are meant to be an elementary introduction to the very useful notion of a Gröbner basis, for non-specialists. The main prerequisite is an understanding of the importance and beauty of systems of polynomial equations. There are exercises for each of the three lectures. I strongly suggest working through them: one must do mathematics to learn it. For further reading, I highly recommend the book by Cox , Little, and O'Shea. The exercises and projects presented in that book are also recommended. It is important to compute Gröbner bases both by hand, and also by computer: I am available to help those wishing to learn *Macaulay* 2 (a computer algebra system developed by Dan Grayson and myself).

Let's get started!

1 Lecture # 1: Gröbner bases.

Motivation.

We start with a typical problem:

Given polynomials $f_1(x_1, \ldots, x_n), f_2(x_1, \ldots, x_n), \ldots, f_r(x_1, \ldots, x_n)$ in the polynomial ring $\mathbf{C}[x_1, \ldots, x_n]$, does the system of equations

$$f_1 = f_2 = \ldots = f_r = 0$$

have a solution? (Here, the base field is $\mathbf{C}$, the complex numbers).

Sometimes one also wants to find the solutions if there are any: we will discuss this problem later.

Let's start with some simple cases.

Example 1.1 [Linear polynomials] Suppose the polynomials equations are linear, say $f_i = \sum_j a_{ij}x_j + b_i = 0$, where the a_{ij} and b_i are scalars in the base field. The most common method to solve these equations is to use Gaussian elimination on the matrix $(A|b)$ to obtain the row echelon form of this matrix. One can then read off the solutions from this matrix. What is happening in terms of the polynomials?

For example, if $f_1 = x_1+x_2-1$ and , $f_2 = x_1-x_2+2$, then Gaussian elimination uses the term x_1 in f_1 as a pivot, and replaces f_2 with $f_2 := f_2 - f_1 = -2x_2+3$, and back substitution uses the term $-2x_2$ in the new f_2 as a pivot to remove the x_2 term from f_1, $f_1 := f_1 + 1/2f_2 = x_1 + 1/2$. Each of these substitutions is reversible: one can obtain the original polynomials as linear combinations of $x_1+1/2$ and $-2x_2+3$.

Before we continue, we need some definitions and notation. Throughout these lectures, we let k be the base field. We let k be any field, but when we consider solutions, we always consider solutions over the algebraic closure $\overline{k}$ of k. We stated the problem above for $k = \mathbf{C}$, but we could have taken any other algebraically closed field. Given k, we denote by R the ring of polynomials in n variables over k:

$$R = k[x_1, \ldots, x_n].$$

We let $I = (f_1, \ldots, f_r) \subset R$ be the *ideal* generated by $f_1, \ldots, f_r$, that is,

$$I = \{\sum_{i=1}^{r} g_i f_i \mid g_i \in R\},$$

is the set of all possible linear combinations (with polynomials as coefficients) of the f_i. Sometimes we call a "nice" generating set of an ideal a "basis" of the ideal. Notice that if $1 \in I$, then for some polynomials $g_1, \ldots, g_r$,

$$1 = g_1 f_1 + \ldots + g_r f_r,$$

so then there can be no common solution to $f_1 = \ldots = f_r = 0$. In the third lecture, we will use Hilbert's Nullstellensatz, which states that the converse is also true: $f_1 = \ldots = f_r = 0$ has no solution (over the algebraic closure $\overline{k}$) if and only if $1 \in I$.

In the case where I is generated by linear polynomials, as in the example above, the Gaussian elimination algorithm replaces our original generating set with a newer, simpler one. This new basis of the ideal I is far superior to the original one: we can easily see that the set of equations is consistent, and it is easy to find all solutions to the system using this basis.

The next simple case is when there is only one variable.

Example 1.2 [One variable] Suppose that $f_1, f_2, \ldots, f_r$ are all polynomials in one variable x with coefficients in a field k. In this case, one can use Euclid's algorithm to determine whether the system

$$f_1(x) = f_2(x) = \ldots = f_r(x) = 0$$

has a solution (in the algebraic closure of k).

For example, suppose that $I = (f_1, f_2) \subset k[x]$, where

$$f_1 = x^3 - x^2 - 2x, \quad f_2 = x^2 - 3x + 2.$$

The Euclidean algorithm attempts to uncover new lead terms by cancelling lead terms. Using the lead term of f_2 as a "pivot", the algorithm proceeds by computing

$$f_1 - x f_2 = 2x^2 - 4x.$$

The lead term here is still divisible by the pivot term, so we continue:

$$f_3 = f_1 - x f_2 - 2 f_2 = x - 2.$$

Now we use the lead term x of f_3 as a pivot, and we quickly find that both f_1 and f_2 are divisible by f_3. The conclusion: another (and better) generating set for I is the single polynomial $x - 2$: $I = (x - 2)$. Thus the system $f_1 = f_2 = 0$ has the unique solution $x = 2$.

For $I = (f_1(x), \dots, f_r(x))$, the Euclidean algorithm finds the greatest common divisor $g(x)$ of these polynomials. So the original generating set for I is replaced by the much simpler one $I = (g(x))$. The original system has a solution exactly when $g(x)$ is not a non-zero constant (at least over an algebraically closed field).

We are mostly interested in the case of ideals of nonlinear polynomials in several variables. Our plan is to extract the key features of Gaussian elimination and Euclid's algorithm and apply them to the general case. This leads us to define the notion of a term order, and then to define the notion of a Gröbner basis. Finally, abstracting out what is happening in both algorithms a bit more leads to Buchberger's algorithm for computing a Gröbner basis.

Gröbner bases

The key ingredient to the above algorithms is a consistent choice of pivot terms. In both examples there is a consistent notion of which term in a polynomial should be used as a pivot. In the case of linear polynomials, we chose the pivot to be the term which was greatest using the order $x_1 > x_2 > \ldots > x_n > 1$. (We could easily have chosen a different order on the variables if we had been so inclined). In the case of polynomials in one variable, we chose the pivot term to be the term which is greatest using the order $x^d > x^{d-1} > \ldots > x^2 > x > 1$. If we choose any other term, then the division process would never terminate.

Monomials play an important role here. We will use the following multi-index notation for monomials: If $A = (a_1, \dots, a_n)$ is a vector of non-negative integers, we set $x^A = x_1^{a_1} x_2^{a_2} \dots x_n^{a_n}$. The *degree* of x^A is $\deg x^A = |A| = a_1 + \ldots + a_n$.

In several variables, with non-linear polynomials, there is no "canonical" choice of pivot. Instead, we have more choice. If we wish to order the monomials of a polynomial so that the greatest term in this order is the pivot, what properties should this order have? First: it is important that a monomial $x^A \neq 1$ should be chosen as a pivot before the monomial 1: otherwise the reductions will not terminate. Second: If the pivot term of a polynomial f is x^A (the "lead term" of f), then the pivot term of $x^B f$ should be $x^B x^A$: the terms should not change order upon multiplying by a monomial. These requirements lead to the following

Definition 1.3 *A total order $>$ on the monomials of $R = k[x_1, \dots, x_n]$ is called a term order if*
(a) $x^A > 1$, for every monomial $x^A \neq 1$, and
(b) If $x^A > x^B$, then for every monomial x^C, $x^{A+C} > x^{B+C}$.

There is only one term order on $k[x]$:

$$x^d > x^{d-1} > \ldots > x > 1.$$

Definition 1.4 [Specific orders]
The **lexicographic order** *is the order $>$ such that $x^A > x^B$, exactly when the first non-zero entry of the vector $A - B$ is positive.*
The **graded lexicographic order** *is the order $>$ such that $x^A > x^B$ if $\deg x^A > \deg x^B$, or $\deg x^A = \deg x^B$, and the first non-zero entry of $A - B$ is positive.*
The **graded reverse lexicographic order** *is the order $>$ such that $x^A > x^B$ if $\deg x^A > \deg x^B$, or $\deg x^A = \deg x^B$, and the* last *non-zero entry of $A - B$ is* negative.

We have defined each of these so that in every case, $x_1 > x_2 > \ldots > x_n$. For $R = k[x_1, x_2, x_3]$, the graded reverse lexicographic order satisfies

$$x_1^2 > x_1x_2 > x_2^2 > x_1x_3 > x_2x_3 > x_3^2,$$

while the graded lexicographic order has

$$x_1^2 > x_1x_2 > x_1x_3 > x_2^2 > x_2x_3 > x_3^2.$$

The only difference between these two orders (at least for these specific monomials) is that the middle two monomials have changed order. This seems like such a small difference, but we will see that the properties of Gröbner bases using these two orders are dramatically different. As a first glimpse of the difference, notice that the last three monomials in the reverse lexicographic case are all divisible by the last variable x_3, whereas the last three monomials in the graded lexicographic order all don't involve x_1. This will imply that the properties (and also the size) of the corresponding Gröbner bases will very different.

The exercises include several other important term orders.

This definition allows us to choose the pivot, or initial, term in a polynomial:

Definition 1.5 [Initial term] *Given a term order $>$ on R, if $f = c_1x^{A_1} + \ldots + c_sx^{A_s}$, where $c_i \neq 0$ are constants, and $x^{A_1} > \ldots > x^{A_s}$, the initial term, or lead term of f is $in_>(f) = c_1x^{A_1}$. For convenience, we also define $in(0) = 0$.*

If the term order is understood, we abbreviate the notation to $in(f)$.

The key idea is that what is important are the possible "pivot", or initial terms that one can obtain by (polynomial) combinations of the original polynomials.

Definition 1.6 [Initial ideal] *Given an ideal $I \subset R$, and a term order $>$ on R, the ideal of initial terms, denoted by $in_>(I)$, is the monomial ideal generated by $\{in(f) \mid f \in I\}$.*

Sometimes we drop the $>$ subscript, and write simply $in(I)$.

Definition 1.7 [Gröbner bases] *Let $I \subset R = k[x_1, \ldots, x_n]$ be an ideal, and let $>$ be a term order on R. A subset $G = \{g_1, \ldots, g_s\}$ of I is called* a Gröbner basis *of I, with respect to $>$, if the monomial ideal $in_>(I)$ is generated by $\{in(g_1), \ldots, in(g_s)\}$.*

This last condition simply means that if $h \in I$ is non-zero, then $in(h)$ is divisible by one of the lead monomials $in(g_i)$.

A Gröbner basis G is called **minimal** if the lead terms of the elements in G minimally generate $in(I)$: that is, $in(g_i)$ never divides $in(g_j)$, as long as $i \neq j$. The Gröbner basis G is called **auto-reduced** if in addition, no term in the polynomial g_i is divisible by $in(g_j)$, whenever $i \neq j$, and that each g_i is monic: the lead monomial $in(g_i)$ has coefficient one.

We can now partly solve our original problem: the solution set of $f_1 = \ldots = f_r = 0$ is empty if $1 \in I = (f_1, \ldots, f_r)$. This is if and only if, by Hilbert's Nullstellensatz, as we will see in the third lecture. Now, using any term order, $1 \in I$ if and only if $1 \in in(G)$ and this last condition may be checked by inspection of the Gröbner basis.

Example 1.8 This example is perhaps the simplest non-trivial Gröbner basis. Let $>$ be the lexicographic order with $x > y$. Let $I = (x^2, xy + y^2) \subset k[x, y]$. From these two polynomials, we see that $in(I)$ contains x^2 and xy. Can we obtain any other lead terms which are not divisible by one of these? We can cancel the lead terms: $y(x^2) - x(xy + y^2) = xy^2$. This is not a new lead term, since it is divisible by xy. We obtain a new lead term by cancelling that: $xy^2 - y(xy + y^2) = y^3$. Thus $y^3 \in I$ and so $y^3 \in in(I)$. Although we haven't yet proved it, the Gröbner basis of I is

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

Soon we will move on to applications. Right now, though, we use the following result to show that Gröbner bases exist, and at the same time, we get a clear proof of Hilbert's basis theorem. We leave the proof of this lemma as a nice exercise (the proof is given in the Cox-Little-O'Shea book).

Lemma 1.9 **[Gordan's Lemma]** *Let S be a set of monomials in $k[x_1, \ldots, x_n]$. Under the partial order $x^A \leq x^B$ if x^A divides x^B, there are only finitely many minimal elements of S. In particular, every monomial ideal in $k[x_1, \ldots, x_n]$ is finitely generated (a special case of Hilbert's basis theorem).*

This lemma is often called "Dickson's lemma." This lemma has some important consequences for term orders and Gröbner bases.

Corollary 1.10 *A term order $>$ is a well ordering on the set of monomials. i.e. every set S of monomials has a minimal element with respect to $>$.*

Corollary 1.11 *For every ideal $I \subset R$ and every term order $>$, the ideal $in_>(I)$ is finitely generated. In particular, every ideal has a (finite) Gröbner basis.*

Corollary 1.12 *If $J \subset I \subset R$ are ideals, and $>$ is a term order, and if $in(I) = in(J)$, then $I = J$.*

Proof. If not, there exists an $f \in I$, but not in J. Choose an element f satisfying this, such that $in(f)$ is minimal with respect to this property. Since $in(I) = in(J)$, there exists $g \in J$ with $in(g) = in(f)$. Then $f - g$ is in I, not in J, and has lower lead term than f, a contradiction. ∎

This next result is crucial for applications. Often it is easier to show that a set G is a Gröbner basis of I, than to show directly that G generates I.

Corollary 1.13 *If $G = \{g_1, \ldots, g_s\}$ is a Gröbner basis of the ideal I, then G generates I.*

Proof. Apply the previous corollary with J being the ideal generated by G. ∎

Corollary 1.14 **[Hilbert basis theorem]** *Let $I \subset R = k[x_1, \ldots, x_n]$ be an ideal. Then I is finitely generated.*

Proof. Choose a term order, and let G be a Gröbner basis of I. Then G generates I (previous corollary) and is a finite set (by definition). ∎

This method of proving Hilbert's basis theorem is essentially due to Gordan.

2 Lecture #2: Buchberger's algorithm and basic applications

Division Algorithm

One of the first questions that arises when discussing ideals is whether a specific polynomial $h \in R$ is in the ideal I. This was one of the first applications of Gröbner bases, and was one of Buchberger's original motivations for defining Gröbner bases.

Problem 2.1 **[Ideal membership]** Given generators for an ideal $I \subset R = k[x_1, \ldots, x_n]$, and given a polynomial $h \in R$, determine whether $h \in I$.

Gröbner bases provide a solution: First compute a Gröbner basis of I, say $G = \{g_1, \ldots, g_s\}$. Since $h \in I$, its lead term is divisible by the lead term of one of the g_i. Subtract off an appropriate multiple of g_i to h to cancel the lead term. The new polynomial h is in I exactly when the previous h is. Continue until one obtains that $h = 0$ (and so the original h is in I), or until $in(h)$ is not divisible by a $in(g_i)$. (and so the original h is not in I). This process must terminate since there are no infinite descending chains of monomials under a term order.

This method leads to the division algorithm to find the remainder of h:

Definition 2.2 **[Remainder]** *Let $G = \{g_1, \ldots, g_s\}$ be a set of non-zero polynomials. Define the remainder, $R_G(h)$, of $h \in R$ by G by the formula:*

$$R_G(h) = \begin{cases} R_G(h - \alpha g_i), & \textit{if } i \textit{ is least such that } \alpha g_i = in(h); \\ R_G(h - in(h)), & \textit{otherwise, if } h \neq 0; \\ 0, & \textit{if } h = 0. \end{cases}$$

In the first case, we choose the least i such that $in(g_i)$ divides $in(h)$ (if there are several).

If G is a Gröbner basis, then the choice of i does not affect the final answer (an exercise!).

Example 2.3 In Example1.8, we computed that $R_G(xy^2) = y^3$, where $G = \{x^2, xy + y^2\}$.

If $G = \{x_1 - x_2^d, x_2 - x_3^d, \ldots, x_{n-1} - x_n^d\}$, for some $d > 0$, and the term order is the lexicographic order with $x_1 > \ldots > x_n$, then $R_G(x_1^d) = x_n^{d^2}$. Notice that G is a minimal Gröbner basis, but is not auto-reduced.

The remainder also gives us a way of determining whether two polynomials are equal modulo I:

Proposition 2.4 **[Ideal membership]** *Let $I \subset R$ be an ideal, and let G be a subset of I. Then*

(a) G is a Gröbner basis of I if and only if for every $h \in I$, $R_G(h) = 0$.

(b) If G is a Gröbner basis of I, then two polynomials $h_1, h_2 \in R$ are equal modulo I if and only if $R_G(h_1) = R_G(h_2)$.

The proof is left as an exercise.

Computing a Gröbner basis

How do we find a Gröbner basis of an ideal? Let's consider the simple example again.

Example 2.5 One way to uncover new lead terms is to take two polynomials in the ideal, and multiply each by just enough to be able to cancel their lead term by subtraction. For example in Example1.8, we found a new lead term by taking x^2 and $xy + y^2$, multiplying them by y and x respectively, and then subtracting, we end up with xy^2. After reducing this element, we obtained a new lead term y^3.

This construction is important enough to deserve some notation:

Definition 2.6 *Given two non-zero polynomials $g = ax^A + \cdots$, and $h = bx^B + \cdots$, where $in(g) = ax^A$ and $in(h) = bx^B$, define the s-polynomial $spair(g, h)$ by*

$$spair(g, h) = bx^C g - ax^D h,$$

where $x^C x^A = x^D x^B$, and the g.c.d. $(x^C, x^D) = 1$.

The key observation is that this way of uncovering new lead terms is sufficient to find all the possible new lead terms, and hence a Gröbner basis. This result of Buchberger leads to his algorithm for computing a Gröbner basis.

Proposition 2.7 **[Buchberger]** *Let $I \subset R$ be an ideal, and let $G \subset I$ be a finite subset, consisting of non-zero polynomials. Then G is a Gröbner basis if and only if for every pair of elements $g, h \in G$, $R_G(spair(g,h)) = 0$.*

The proof is one of the exercises for this section.

The strategy to compute a Gröbner basis is this: Start with an initial approximation to a Gröbner basis: let G be the set consisting of the original generators. Try to uncover new lead terms by taking two polynomials in this set, forming this s-polynomial and finding the remainder. If we get zero, then we continue. On the other hand, if we get a non-zero remainder, then we have a new lead term. So we add this element to our growing Gröbner basis G. This process must end because the initial ideal is finitely generated (more precisely, because the polynomial ring is Noetherian).

Here is the boiled down version of Buchberger's algorithm for computing a Gröbner basis of an ideal.

Algorithm 2.8 **[Buchberger's algorithm]**

```
input:  A set ${f_1, \ldots, f_r} \subset R$.
output: A Gröbner basis $G$ of the ideal generated by ${f_1, \ldots, f_r}$.
begin
    $G := \{f_1, \ldots, f_r\}$
    Pairs := $\{(f_i, f_j) \mid 1 \leq i < j \leq r\}$
    while $Pairs \neq \emptyset$ do
        $(g_i, g_j)$ := remove an element from Pairs
        $s := spair(g_i, g_j)$
        $h := R_G(s)$
        if $h \neq 0$ then
            $Pairs := Pairs \cup \{(h, g) \mid g \in G\}$.
            $G := G \cup \{h\}$.
    return $G$
end.
```

In practice, there are several improvements that one should make: the result should be auto-reduced, usually as the algorithm proceeds. It is possible to know that certain pairs will reduce to zero, so that they can be discarded immediately. Finally, the order that one processes the pairs is very important to the performance of the algorithm.

Example 2.9 In Example1.8, $G = \{x^2, xy + y^2, y^3\}$ is a Gröbner basis. We can check this by reducing the three s-polynomials. The first, $spair(x^2, xy + y^2)$, is $-xy^2$, and reduces to $-y^3$, and then to zero. $spair(x^2, y^3) = 0$ already, and $spair(xy + y^2, y^3) = y^4$, which reduces to zero in one step. We have therefore verified that G is a Gröbner basis of the ideal $(x^2, xy + y^2)$.

Example 2.10 To give you a feel of the rough size of some Gröbner bases, let $R = k[a, b, c, d]$ be the polynomial ring in four variables. Let $I = \{f_1, f_2, f_3\}$ be the ideal generated by four random forms of degree three. The minimal Gröbner basis of I, using the graded reverse lexicographic order has 11 elements, with (total) degrees 3,3,3,4,4,5,5,5,6,6,7. The minimal Gröbner basis of I, using the lexicographic order, has 55 elements ranging in degrees from 3 to 27. If we use the elimination order eliminating the first two variables (defined in the exercises), then there are 39 Gröbner basis elements, ranging in degrees from 3 to 27. If we use the elimination order eliminating one variable, there are 23 Gröbner basis elements, ranging in degrees 3 to 7.

Elimination of variables

One of the mot important applications of Gröbner bases is to eliminate variables. The simplest form of the problem is:

Problem 2.11 [Elimination of variables] Given generators for an ideal $I \subset R = k[x_1, \ldots, x_n]$, and an integer $2 \leq i \leq n$, find generators for the ideal

$$I \cap k[x_i, x_{i+1}, \ldots, x_n]$$

in the ring $k[x_i, x_{i+1}, \ldots, x_n]$.

This ideal is called an *elimination* ideal.

Example 2.12 If $I = (ax + b, cx + d) \subset k[x, a, b, c, d]$, then $I \cap k[a, b, c, d] = (ad - bc)$ (clearly the elimination ideal contains this element, and in this case it isn't too hard to check that we have equality.) This is called elimination, since we are "eliminating" the variable x.

Many constructions in algebraic geometry are based on computing elimination ideals. We will see examples in the next lecture, and more examples appear in the exercises.

For now, let's see how we can compute elimination ideals using Gröbner bases. If we could enumerate all of the elements of I (tough, since this is an infinite, usually uncountable set!), then we could simply choose those elements which are in the subring $k[x_i, \ldots, x_n]$. Gröbner bases allow us to mimick this process, by restricting our attention to a finite set: the Gröbner basis itself.

Proposition 2.13 *Let G be a Gröbner basis of I with respect to the lexicographic order $>$. Then $G' := G \cap k[x_i, x_{i+1}, \ldots, x_n]$ is a Gröbner basis of $J := I \cap k[x_i, \ldots, x_n]$ with respect to the term order induced by $>$. In particular, G' generates the ideal J.*

Proof. Write the Gröbner basis G as

$$G = \{g_1, \ldots, g_s, \quad g_{s+1}, \ldots, g_t\},$$

where some monomial of $g_1, \ldots, g_s$ involve at least one of the variables $x_1, \ldots, x_{i-1}$, and $g_{s+1}, \ldots, g_t$ do not involve these variables. Notice that each monomial

$in(g_1), \ldots, in(g_s)$ is divisible by one of $x_1, \ldots, x_{i-1}$, since the term order is the lexicographic order.

We wish to show that $G' = \{g_{s+1}, \ldots, g_t\}$ is a Gröbner basis of J. The set G' is contained in J, so we must show that if $h \in J$, then $in(h)$ is divisible by one of $in(g_{s+1}), \ldots, in(g_t)$. Given an $h \in J$, h is also a member of I, so $in(h)$ is divisible by one of $in(g_1), \ldots, in(g_t)$. Suppose that in fact, $in(h)$ is divisible by one of $in(g_1), \ldots, in(g_s)$. Then $in(h)$ is divisible by one of the variables $x_1, \ldots, x_{i-1}$, and then $h \notin k[x_i, \ldots, x_n]$, a contradiction. Therefore, $in(h)$ must be divisible by a lead term of G', as desired. ∎

Examing the proof, we see that the only property of the term order that we have used is that for $g \in R$, and any $1 \le i \le n$,

$$g \in k[x_i, \ldots, x_n] \iff in(g) \in k[x_i, \ldots, x_n].$$

Many other term orders have this property, at least for a specific i. Let's give this property a name:

Definition 2.14 *A term order is called an elimination order, eliminating $x_1, \ldots, x_{i-1}$, (for a specific i) if for every $g \in R$,*

$$g \in k[x_i, \ldots, x_n] \iff in(g) \in k[x_i, \ldots, x_n].$$

We leave the proof of the generalization of the last Proposition as an exercise.

Proposition 2.15 *Let G be a Gröbner basis of I with respect to an elimination order $>$ which eliminates the variables $x_1, \ldots, x_{i-1}$. Then $G' = G \cap k[x_i, x_{i+1}, \ldots, x_n]$ is a Gröbner basis of $J := I \cap k[x_i, \ldots, x_n]$ with respect to the term order induced by $>$. In particular, G' generates the ideal J.*

Since the lexicographic order can be used to eliminate variables, for each i, one might ask: why ever use any other elimination order? This is addressed in the exercises, but basically, lexicographic Gröbner bases are often prohibitively expensive to compute.

Example 2.16 This example gives an idea as to how one may use Gröbner bases to solves systems of polynomial equations. As a specific example, let

$$I = (x, y-1, z-2)(x-2, y+1, z-1)(x-2, y-1, z-3)$$

be the product of the given ideals in $\mathbf{C}[x, y, z]$. I is given by 27 generators (all the possible products). We wish to solve the system of equations where all of these are zero. Of course, the solution consists of $(x, y, z) = (0, 1, 2), (2, -1, 1)$ and $(2, 1, 3)$.

How would one see this via Gröbner bases? The Gröbner basis of I, with respect to the lexicographic order $x > y > z$ is (I computed this using *Macaulay* 2):

$$\begin{pmatrix} z^3 - 6z^2 + 11z - 6 \\ y + z^2 - 5z + 5 \\ x - 2z^2 + 8z - 8 \end{pmatrix}.$$

Using the lexicographic order allows us to compute $I \cap k[z]$, which is generated by $z^3 - 6z^2 + 11z - 6 = (z-1)(z-2)(z-3)$. Thus $z = 1, 2$, or 3. The second equation involves just y and z. Plug in the various values of z and this immediately gives the corresponding values for y. Similarly, x is solved using the third equation.

The Gröbner bases don't always come out as nice as this. For example, let

$$J = (x, y-1, z-2)(x-2, y+1, z-1)(x-2, y-1, z-3)^2,$$

where the only difference from the above ideal is that the last ideal is squared. The solution set to the corresponding system of equations is the same as above. The Gröbner basis using the lexicographic order is somewhat more complicated:

$$\begin{pmatrix} z^4 - 9z^3 + 29z^2 - 39z + 18 \\ yz - 3y + z^3 - 8z^2 + 20z - 15 \\ y^2 - 2y + z^3 - 8z^2 + 21z - 17 \\ xz - 3x - 2z^3 + 14z^2 - 32z + 24 \\ xy - x - 2y + 2 \\ x^2 - 4x - 4z^3 + 28z^2 - 60z + 40 \end{pmatrix}.$$

The first equation factors as $(z-1)(z-2)(z-3)^2$, and so $z = 1, 2$, or 3, as above. The second equation allows us to solve for y, as long as $z \neq 3$. If $z = 3$, then the third Gröbner basis element gives $(y-1)^2 = 0$. The next two equations will determine x if $z \neq 3$ or $y \neq 1$. In this event, x is determined by the last equation, by first plugging in $y = 1$ and $z = 3$. Thus, we have found all of the solutions.

For general problems, using the lexicographic order will always allow us to solve the system of equations, using not much more than this method used here. The main problem with this method is that on many larger problems, it is essentially impossible to compute the lexicographic Gröbner basis. In this case, other methods need to be considered. For more information, see Teresa Crick's lectures in this same series.

We will have a little more to say about solving equations in the next lecture.

3 Lecture # 3: Geometry.

Throughout this lecture, we assume that k is algebraically closed. One can relax this assumption at the cost of more complicated statements of results, but we won't bother with that in this lecture.

The Algebra – Geometry Dictionary, Hilbert's Nullstellensatz

Definition 3.1 **[Varieties and ideals]** *Given any set S of polynomials in R, we denote by $V(S)$ the zero set, or variety of S:*

$$V(S) = \{(p_1, \ldots, p_n) \in k^n \mid f(p_1, \ldots, p_n) = 0 \text{ for all } f \in S\}.$$

For example, if $I = (x_1 + x_2 - 1, x_1 - x_2 + 2) \subset \mathbf{C}[x_1, x_2]$, then

$$V(I) = V(\{x_1 + x_2 - 1, x_1 - x_2 + 2\}) = \{(-1/2, 3/2)\} \in \mathbf{C}^2.$$

Notice that if I is the ideal generated by S, then $V(S) = V(I)$. It is customary in algebraic geometry to refer to k^n as $\mathbf{A}^n_k$, *affine n-space* over k. If the field k is understood, then we abbreviate this as $\mathbf{A}^n$. We call subsets of $\mathbf{A}^n$ of the form $V(I)$ *algebraic* sets.

An often used variant is the case of homogeneous polynomials. If f is homogeneous, then $f(\lambda x) = \lambda^{\deg f} f(x)$, so $f(x)$ and $f(\lambda x)$ are either both zero, or both non-zero. Define projective space, $\mathbf{P}^{n-1}$ to be the space $\mathbf{A}^n \setminus (0, 0, \ldots, 0)$ modulo the equivalence relation $p \equiv \lambda p$, for $\lambda \neq 0$. Then, if I is a homogeneous ideal, then define

$$V(I) = \{[p] \mid f(p) = 0, \text{for all } f \in I\} \subset \mathbf{P}^{n-1}.$$

This notation conflicts with the notation above, but we shall make it explicitly clear when we use this instead of the definition above.

Definition 3.2 *Given a subset $X \subset \mathbf{A}^n$, define the ideal of X to be*

$$I(X) = \{f \in R \mid f(p) = 0 \text{ for all } p \in X\}.$$

These two operations will be our link between ideals and algebraic sets. Given an algebraic set X, it is easy to see that $V(I(X)) = X$. If X is not an algebraic set, then $\overline{X} := V(I(X))$ strictly contains X. We call $\overline{X}$ the (Zariski-) closure of X. In the other direction, it is not always true that $I(V(J)) = J$. For example, $V(x^2) = V(x)$, and $I(V(x^2)) = (x)$. Hilbert's Nullstellensatz describes precisely when equality does hold:

Theorem 3.3 **[Hilbert's Nullstellensatz]** *If $J \subset R$ is an ideal, then*

$$I(V(J)) = \{f \in R \mid f^N \in I, \quad \text{for some sufficiently large } N\}.$$

In particular, $V(J) = \emptyset$ if and only if $J = (1)$.

The algebraic construction implicit in this result is the radical:

Definition 3.4 *The radical of an ideal I is*

$$\sqrt{I} = \{f \in R \mid f^N \in I, \text{ for some sufficiently large } N\}.$$

It is easy to see that the radical is an ideal containing I. Much more difficult is to find a method to compute it! There are a number of methods for accomplishing this, but we won't have time to discuss them in these lectures. See the references at the end of these notes.

The Nullstellensatz links the geometry of algebraic sets to the algebra of ideals. There are several (seemingly) different proofs of this result. Hilbert's original proof used elimination theory and resultants. For more modern and/or simpler proofs, see Atiyah-Macdonald, or Eisenbud.

Corollary 3.5 *There is an order reversing one to one correspondence between radical ideals in R, and algebraic subsets of $\mathbf{A}^n$, given by the inverse operations $V(-)$ and $I(-)$.*

Using this correspondence, we can build a dictionary between ideals and geometry.

There are some basic facts about these two operations, which we leave as an exercise:

Exercise 3.6 The dictionary

(a) $X = \mathbf{A}^n$ is an algebraic set, $X = V(0)$.

(b) $X = \emptyset$ is an algebraic set, $X = V(1)$.

(c) If $I \subset J$ are ideals, then $V(J) \subset V(I)$, and if $X \subset Y$ are subsets of $\mathbf{A}^n$, then $I(Y) \subset I(X)$.

(d) $V(I) \cup V(J) = V(I \cap J)$.

(e) $V(I) \cap V(J) = V(I + J)$.

(f) If X is any subset of $\mathbf{A}^n$, then $X \subset V(I(X))$. This set, denoted by $\overline{X}$, is called the (Zariski) closure of X. If $X = V(I)$ is an algebraic set already, then show that $X = \overline{X}$.

(g) The Zariski topology on $\mathbf{A}^n$ is the topology whose closed sets are the algebraic sets. Show that this defines a topology.

(h) Show that if $U \subset \mathbf{A}^n$ is a non-empty (Zariski-)open set, then $\overline{U} = \mathbf{A}^n$. This means that every non-empty Zariski open subset is dense: the open sets in this topology are very big! Caution: this is *not* a Hausdorff topology!

Components, ideal quotients and saturations

Example 3.7 Let A be a 3 by 3 matrix over $\mathbf{C}$. Let us study the equations which give the eigenvalues and eigenvectors of A. Let I be the ideal in four variables x, y, z, and λ, defined by the entries of the matrix

$$A\begin{pmatrix} x \\ y \\ z \end{pmatrix} - \lambda \begin{pmatrix} x \\ y \\ z \end{pmatrix}.$$

For example, take

$$A = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}.$$

The ideal I is

$$I = (y + z - \lambda x,\ x + z - \lambda y,\ x + y - \lambda z).$$

A has $\lambda = 2$ as an eigenvalue, with eignvector $\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$, and $\lambda = -1$ as its only other eigenvalue, with eigenspace $span(\begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix})$. One doesn't really need Gröbner bases to describe $V(I)$, but it is instructive to see what the lexicographic Gröbner basis (with $x > y > z > \lambda$) looks like:

$$G = \{x - y\lambda + z,\ (y - z)(t + 1),\ z(t - 2)(t + 1)\}.$$

Using this, or computing directly, it follows that $V(I)$ is the union of the sets

$$E_1 = \{(t, t, t, 2) \mid t \in \mathbf{C}\} \ = \ V(x - y, y - z, t - 2),$$

$$E_2 = \{(s + t, -s, -t, -1) \mid s, t \in \mathbf{C}\} \ = \ V(x + y + z, \lambda + 1),$$

and

$$Z = \{(0, 0, 0, t) \mid t \in \mathbf{C}\} \ = \ V(x, y, z).$$

The solutions in E_1 and E_2 do correspond to the eigenvalues and eigenvectors of A. The solutions in Z are degenerate solutions: eigenvectors nust have at least one non-zero component.

The sets E_1, E_2 and Z are examples of irreducible algebraic sets: An *irreducible* algebraic set is a subset X which is not the union of two proper algebraic sets. If X is not irreducible, we call X *reducible.* So $V(I)$ in this example is a reducible algebraic set.

The corresponding algebraic notion is: An ideal I is *prime* if whenever $fg \in I$, then either $f \in I$ or $g \in I$.

Exercise 3.8 Let $X \subset \mathbf{A}^n$ be an algebraic set. Prove that $I = I(X)$ is prime if and only if X is irreducible.

It is not trivial to decide whether an ideal I is prime. There are algorithms for doing this, but we won't have time to discuss them in these lectures.

Each algebraic set X can be written uniquely as an irredundant finite union of irreducible sets. This is called the irreducible decomposition of X.

Exercise 3.9 If $X = X_1 \cup \ldots \cup X_m$ is the irreducible decomposition of X, and $P_i = I(X_i)$, then $I(X) = P_1 \cap \ldots \cap P_m$.

One often wants to "remove" degenerate loci: For example, in our eigenvalue example, we might want to find the ideal J defining the union of the "good" components: $V(J) = E_1 \cup E_2$. The bad locus is the locus where $x = y = z = 0$ (eigenvectors are not zero vectors).

Problem 3.10 **[Removal of components]** Given an ideal I, with $V(I) = X_1 \cup \ldots \cup X_m$ an irreducible decomposition, and given an ideal L, find an ideal J such that $V(J)$ is the union Y of the components X_i with $X_i \not\subset V(L)$.

If $I = I(X)$ is the radical ideal defining X, then J should be the radical ideal defining Y.

An alternate method of describing this problem is:

Problem 3.11 **[Removal of components, version 2]** Given the ideal I of X, and given an algebraic set Z, find the ideal defining $\overline{X \setminus Z}$

So in our example, we want $\overline{V(I) \setminus V(x, y, z)}$.

Removal of components is related to division: if $gh^N \in I(X)$, for any N, then $g \in I(X \setminus V(h))$. This motivates the following definitions.

Definition 3.12 **[Ideal quotient and saturation]** *If $I, L \subset R$ are ideals, and $h \in R$, then we define the ideal quotient*

$$(I : h) = \{g \in R \mid gh \in I\},$$

and the saturation

$$(I : h^\infty) = \{g \in R \mid gh^N \in I, \text{ for } N \text{ sufficiently large}\}.$$

Similarly, define the ideal quotient:

$$(I : L) = \{g \in R \mid gL \subset I\},$$

and the ideal saturation

$$(I : L^\infty) = \{g \in R \mid gL^N \subset I, \text{ for } N \text{ sufficiently large}\}.$$

For radical ideals I, ideal quotients and saturations will always be equal, but in general this won't happen: $(x^3y : x) = (x^2y)$, whereas $(x^3y : x^\infty) = (y)$. In the rest of this lecture we will consider mainly ideal saturations.

Here is the dictionary entry for ideal saturations:

Proposition 3.13 *Let $X = V(I)$, and let $Y = V(L)$. Then*

$$V(I : L^\infty) = \overline{X \setminus Y}.$$

Proof. ∎

There are several methods available to compute saturations. If the ideal L is singly generated, then the following method works reasonably well.

Proposition 3.14 *If $I \subset R$ is an ideal, and $h \in R$, then*

$$(I : h^\infty) = (I, hz - 1) \cap k[x_1, \ldots, x_n],$$

where z is an additional variable.

Proof. ∎

If the ideal I is homogeneous, and h is a variable, then a usually much better way is to use Bayer's method (see the exercises).

Example 3.15 In the eigenvalue example above, let's remove the "bad" locus Z: We wish to compute $I : (x, y, z)^\infty$. Note that by definition, this is the intersection $(I : x^\infty) \cap (I : y^\infty) \cap (I : z^\infty)$. Each of these three terms is equal. The common result is

$$(I : (x, y, z)^\infty) = ((t + 1)(t - 2),\ (y - z)(t + 1),\ x - yt + z).$$

Projections and Elimination theory

Here is a question: What is $J = I \cap k[x_i, \ldots, x_n]$ *really*? In other words, what is $V(J)$ in terms of $V(I)$?

The answer involves projections. Let

$$\phi : \mathbf{A}^n \longrightarrow \mathbf{A}^{n-i+1}$$

be the projection map defined by

$$\phi(p_1, \ldots, p_n) = (p_i, p_{i+1}, \ldots, p_n) \in \mathbf{A}^{n-i+1}.$$

Proposition 3.16 *If $X = V(I) \subset \mathbf{A}^n$, and if $J = I \cap k[x_i, \ldots, x_n]$, then the ideal $I(\phi(X)) = J$. In particular, the ideal of (the closure of) $\phi(X)$ is J.*

Proof. ∎

Example 3.17 Suppose that $X \subset \mathbf{A}^n$ is a finite set of points, and let $I = I(X)$. Consider the projection $\phi : \mathbf{A}^n \longrightarrow \mathbf{A}^1$, given by projection onto the last coordinate. The ideal $J = I \cap k[x_n]$ will be of the form $J = (f(x_n))$, where the roots of f give the last coordinates of the points in X.

Exercise 3.18 Suppose that $X \subset \mathbf{A}^n$ is a finite union of d points, and that the last coordinates of the d points are all distinct. Let $I = I(X)$. Show that using the lexicographic order $x_1 > x_2 > \ldots > x_n$, the Gröbner basis of I has the form

$$G = \{x_1 - g_1(x_n), \ldots, x_{n-1} - g_{n-1}(x_n), f(x_n)\},$$

where $f(x_n)$ is a polynomial of degree exactly d.

Let's now consider more general polynomial maps. For example, consider the polynomial map

$$F : \mathbf{A}^1 \longrightarrow \mathbf{A}^2$$

given by

$$F(t) = (x, y) = (t^4, t^3 - t^2 + 1).$$

The question we wish to ask is: what is the ideal of the image of this map? This is the problem of going from an explicit parametrization to the implicit equation of the image. The ideal of the image will be generated by those polynomials $g(x, y)$, such that $g(t^4, t^3 - t^2 + 1) = 0$. Below, we will compute this ideal.

Suppose that $X = V(J) \subset \mathbf{A}^n$, and $f_1, \ldots, f_r \in R$. Let $F : X \longrightarrow \mathbf{A}^r$ be the polynomial map defined by

$$F(p) = (f_1(p), \ldots, f_r(p)) \in \mathbf{A}^r.$$

Our first question is: what is the ideal of the image of this map? That is, find the equations defining the closure $\overline{F(X)}$.

There is a "trick" which is often used to reduce questions about general polynomial maps to questions involving only projections.

Definition 3.19 [Graph of a polynomial map] *Given the polynomial map F as above, define the graph of F, $graph(F)$ to be the subset of $\mathbf{A}^n \times \mathbf{A}^r = \mathbf{A}^{n+r}$ defined by*

$$graph(F) = \{(p, q) \in X \times \mathbf{A}^r \mid F(p) = q\}.$$

In the exercises, you will be asked to verify that the ideal of $graph(F)$ in the polynomial ring $k[x_1, \ldots, x_n, y_1, \ldots, y_r]$ is

$$I(graph(F)) = J + (y_1 - f_1, \ldots, y_r - f_r).$$

Using this, it is easy to answer our original problem:

Proposition 3.20 *The ideal of* $\overline{F(X)}$ *is*

$$(J + (y_1 - f_1, \ldots, y_r - f_r)) \cap k[y_1, \ldots, y_r].$$

Example 3.21 In order to compute the ideal of the image for the one variable example above, we compute a Gröbner basis for the ideal using an elimination order eliminating t:

$$I = (t^4 - x, t^3 - t^2 - y).$$

The Gröbner basis with respect to the lexicographic order $t > x > y$ is:

$$\begin{pmatrix} x^3 - 4x^2y - x^2 + 2xy^2 - y^4 \\ ty^3 + 2ty^2 + x^2 - xy^2 - 4xy - x + y^3 + y^2 \\ tx + ty^2 - xy - x + y^2 \\ t^2 + ty - x + y \end{pmatrix}$$

The first polynomial (the one involving just x and y: no t's) defines the image. It is reasonably complicated for such a simple example. What this means in practice is that one should work with parametrizations instead of the implicit equations of an algebraic set (assuming one is lucky enough to even have a parametrization!).

By examining the Gröbner basis, we obtain quite a bit more information about the map. The second polynomial being equal to zero can be solved for t if the coefficient of t is non-zero (in this case: this means if $y \neq 0, -2$):

$$t = -\frac{x^2 - xy^2 - 4xy - x + y^3 + y^2}{y^3 + 2y^2},$$

This defines an inverse of the map, at least off the locus where $y = 0$ or $y = -2$. Similarly, if $x + y^2 \neq 0$, then

$$t = \frac{xy + x - y^2}{x + y^2}.$$

There is no inverse if both denominators are zero. This happens for $(x, y) = (0, 0)$ and $(x, y) = (-4, -2)$. The point $(0, 0)$ has one inverse image: the curve has a cusp at this point. The point $(-4, -2)$ has two inverse images: $t = 1 + i, t = 1 - i$. This is a double point on the curve.

4 Exercises for Lecture # 1.

Exercise 4.1 Let $>$ be the (non-graded) reverse lexicographic order: $x^A > x^B$ if the last non-zero entry of $A - B$ is negative. Is this order a term order?

Exercise 4.2 Let $w \in \mathbf{R}^n$ be a vector, and let $>_1$ be any term order. Define a new order $>$, called a *weight* order, by $x^A > x^B$ if $w \cdot A > w \cdot B$, or $w \cdot A = w \cdot B$, and $x^A >_1 x^B$. Show that this is a term order. If $w = (1, 1, \ldots, 1, 0, \ldots, 0)$, where the number of 1's in the vector is m, then the resulting term order is called the mth elimination order.

Exercise 4.3 **[Product order]** Let $>_1$ and $>_2$ be term orders on $k[x_1, \ldots, x_m]$ and $k[t_1, \ldots, t_r]$ respectively. Define an order $>$ on $k[x_1, \ldots, x_n, t_1, \ldots, t_r]$, called the *product* order, by $x^A t^B > x^C t^D$ if $x^A >_1 x^C$, or $x^A = x^C$, and $t^B >_2 t^D$. Show that this order is a term order.

Exercise 4.4 Show that the graded reverse lexicographic order has the following property: If $f \in R$ is a non-zero homogeneous polynomial, then x_n divides $in(f)$ if and only if x_n divides f.

Exercise 4.5 Show that the lexicographic order has the following property: If $f \in R$ is non-zero and $1 \leq i \leq n$, then $in(f) \in k[x_i, x_{i+1}, \ldots, x_n]$ if and only if $f \in k[x_i, x_{i+1}, \ldots, x_n]$.

Exercise 4.6 Let $J = (x^{A_1}, \ldots, x^{A_r})$ be a monomial ideal: that is, an ideal generated by monomials. Find algorithms or formulas to compute:

(a) Whether x^B is in J.

(b) The ideal quotient $(J : x^B) := \{g \in R \mid x^B g \in J\}$.

(c) The intersection $J \cap I$, where I is another monomial ideal.

(d) A minimal set of generators for J (that is, a set of generators, such that no subset generates). Show that there is a unique minimal generating set consisting of monomials for a monomial ideal J.

Exercise 4.7 Let $>$ be a fixed term order, and fix an ideal $I \subset R$. Show that there is a unique auto-reduced Gröbner basis of I.

Exercise 4.8 Show that the monomials $\{in(f) \mid f \in I, f \neq 0\}$ form a k-basis for the ideal $in(I)$.

Exercise 4.9 Let $>$ be a term order, and let S be a finite set of monomials. Show that there exists an integral vector $w \in \mathbf{Z}^n$, such that for $x^A, x^B \in S$, $x^A > x^B$ if and only if $w \cdot A > w \cdot B$. Interesting problem: Can you bound the size of the entries of w in terms of the size of the exponents of monomials in S?

Exercise 4.10 Prove Gordan's Lemma (Lemma1.9).

5 Exercises for Lecture # 2.

Playing with Gröbner bases

Exercise 5.1 Compute by hand the Gröbner basis of the ideal

$$I = (s^3 - a, s^2t - b, st^2 - c, t^3 - d) \subset k[s, t, a, b, c, d],$$

using the lexicographic order $s > t > a > b > c > d$. Find a generating set for $I \cap k[a, b, c, d]$.

Exercise 5.2 Let $I \subset k[a, b, c, d]$ be the ideal generated by three random homogeneous degree 4 polynomials. Using *Macaulay 2*, or another computer algebra system, compute the Gröbner bases of I using the graded reverse lexicographic order, and the graded lexicographic order. What is the highest degree of a Gröbner basis element for each of these two cases? Why do you suppose that one of these is so much more complicated than the other?

Exercise 5.3 Prove that if G is a Gröbner basis, any choice of i in the first case of the definition of $R_G(h)$ leads to the same remainder.

Exercise 5.4 Prove Proposition2.4

Exercise 5.5 Show that the elimination weight order defined in Exercise4.2, and any product order (defined in Exercise4.3) are elimination orders.

Exercise 5.6 Prove Proposition2.15.

Exercise 5.7 Let I and J be two ideals in R. Find an algorithm to compute the intersection $I \cap J$.

Exercise 5.8 Let $f_1, \dots, f_r$ be polynomials in R. Let

$$A = k[f_1, \dots, f_r] \subset k[x_1, \dots, x_n],$$

be the sub k-algebra generated by the f_i. The ring A has a presentation as

$$A = k[y_1, \dots, y_r]/L,$$

for some ideal L. Notice that L is the kernel of the ring homomorphism $\phi : k[y_1, \dots, y_r] \longrightarrow k[x_1, \dots, x_n]$, where $y_i \mapsto f_i$. Find an algorithm or formula for L. Similarly, if $I \subset R$ is an ideal, compute the kernel of the induced map $k[y_1, \dots, y_r] \longrightarrow R/I$.

Exercise 5.9 [Hilbert series] Hilbert series are one of the most important applications of Gröbner bases. Suppose that $I = \{f_1, \ldots, f_r\} \subset R$ is a homogeneous ideal (that is, each f_i is a homogeneous polynomial). Let $I_d \subset R_d$ be the vector space of all polynomials in I which are homogeneous of degree d. The Hilbert series of R/I is the formal power series

$$H(R/I, t) := \sum_{d=0}^{\infty} (\dim_k R_d/I_d)\; t^d.$$

It is fairly easy to show (see Atiyah-Macdonald) that $H(R/I, t)$ is a rational function of the form

$$H(R/I, t) = \frac{P(t)}{(1-t)^e},$$

where $P(t)$ is a polynomial with integral coefficients, and $P(1) \neq 0$.

Given this form, one can read off the dimension and degree of R/I (if you are not familiar with these notions, you can use these as the definitions!). The (Krull) dimension of R/I is e. The degree of R/I is $P(1)$.

(a) Show that

$$H(R, t) = \frac{1}{(1-t)^n}.$$

(b) Show that if $>$ is any term order, and I is a homogeneous ideal, then $\dim in(I)_d = \dim I_d$, for all d. Therefore R/I and $R/in(I)$ have the same Hilbert series.

(c) Show that if $f \in R$ is homogeneous of degree d, and $I \subset R$ is a homogeneous ideal, then

$$H(R/(I, f), t) - H(R/I, t) + H(R/(I : f), t - d) = 0.$$

(d) Use (c) to give an algorithm for computing the Hilbert series of R/J, where J is a monomial ideal. By (b), this gives an algorithm to find the Hilbert series of R/I, for any homogeneous ideal.

(e) Find the Hilbert series of the ideal of the twisted cubic curve: $I = (bc - ad, b^2 - ac, c^2 - bd) \subset k[a, b, c, d]$.

Exercise 5.10 [Gröbner bases in skew-commutative polynomial rings] Let A be the k-algebra generated by elements $x_1, \ldots, x_n$ satisfying the skew commutativity relations $x_i x_j = -x_j x_i$, if $i \neq j$, and $x_i^2 = 0$. Define a notion of Gröbner basis for this ring, give an algorithm to compute it (in particular, what are the "s-pairs"?). Try your algorithm on some ideals in this ring. (An example of an interesting case: Take a simplicial complex, and let $I \subset A$ be the face ideal (i.e. the ideal generated by the monomials whose support are the non-faces in the simplicial complex). This is a monomial ideal in A. Now make a random linear change of coordinates. The initial ideal of this new ideal (w.r.t. any term order) is the face ring of a simplicial complex. What is it? (This is a vague question, since this is still a research problem.)

Exercise 5.11 **[Gröbner bases in the Weyl algebra]** Let A be the non-commutative k-algebra generated by $x_1, \ldots, x_n$, and $\partial_1, \ldots, \partial_n$, where all pairs of variables commute, except

$$\partial_i x_i = 1 + x_i \partial_i,$$

for each $i = 1, \ldots, n$. Find a definition of a Gröbner basis of a 2-sided ideal in A. How must one modify Buchberger's algorithm to compute such a Gröbner basis?

6 Exercises for Lecture # 3.

Exercise 6.1 Suppose that $I : h^\infty = I : h^m$. Show that $I = (I, h^m) \cap (I : h^\infty)$. This simple but important formula is one key part of algorithms for computing the primary decomposition of an ideal.

Exercise 6.2 Let $A = R/I$, and let f/g be a fraction with f and g in R. Devise an algorithm for finding a presentation $B = k[x_1, \ldots, x_n, y]/L$ of the ring $A[f/g]$. (You may suppose that g is a non-zero-divisor on I).

Exercise 6.3 **[Bayer's method for ideal saturations]** Suppose that I is a homogeneous ideal (that is, I is generated by homogeneous polynomials. Let $>$ be the graded reverse lexicographic order. Show how to use the Gröbner basis of I to compute $(I : x_n)$ and $(I : x_n^\infty)$.

Exercise 6.4 **[Homogenization]** Let $I = (f_1, \ldots, f_r) \subset k[x_1, \ldots, x_n]$ be an ideal. For a polynomial g, let g^h denote the homogenization of g with respect to a new variable z. So $g^h = z^{\deg g} g(x_1/z, \ldots, x_n/z)$. The *homogenization* of I, I^h, is the ideal in $k[x_1, \ldots, x_n, z]$ generated by $\{g^h \mid g \in I\}$. Find an algorithm to compute I^h.

Use this algorithm to compute the homogenization of the ideal

$$I = (x_2 - x_1^2, x_3 - x_1^3).$$

Exercise 6.5 **[Secant locus]** Given an algebraic set $X \subset \mathbf{A}^n$, the secant locus is defined by

$$Sec(X) = \bigcup_{p \neq q \in X} \overline{pq}.$$

i.e. Sec(X) is the union of all lines connecting distinct pairs of points on X. Determine a way of computing $Sec(X)$, given generators for $I = I(X)$.

Exercise 6.6 **[Blow-up algebra]** Given algebraic sets $Y \subset X \subset \mathbf{A}^n$, the *blow-up algebra* $Bl_Y(X)$ is defined to be the ring $A[Jt] \subset A[t]$, where $J = I(Y)$, $I = I(X)$, and $A = R/I$. Find a way of computing

$$Bl_Y(X) = k[x_1, \ldots, x_n, y_1, \ldots, y_r]/L,$$

where J has r generators.

Exercise 6.7 [**Normal cone, or associated graded ring**] Let notation be as in the previous exercise. The normal cone of Y in X is defined to be the ring

$$N_{Y/X} = R/I \oplus I/I^2 \oplus I^2/I^3 \oplus \cdots .$$

Find an algorithm to compute a presentation of this ring.

References

M.F. Atiyah, I.G. MacDonald (1969) *Introduction to Commutative Algebra*, Addison-Wesley, Reading, Massachusetts.

D. Bayer (1982): The division algorithm and the Hilbert scheme. Thesis, Harvard University, Cambridge, MA.

D. Bayer, M. Stillman (1987): A criterion for detecting m-regularity, *Invent. Math.* **87** 1–11.

G. Bergman (1978): The diamond lemma for ring theory, *Adv. in Math.* **29** 178–218.

B. Buchberger (1976): A theoretical basis for the reduction of polynomials to canonical forms, *ACM SIGSAM Bull.* **39** 19–29.

D. Cox, J. Little, D. O'Shea (1992,1997): *Ideals, Varieties and Algorithms*, Second Edition, Springer, New York-Berlin-Heidelberg.

D. Eisenbud (1995): *Commutative Algebra with an eye towards Algebraic Geometry*, Springer, New York-Berlin-Heidelberg.

D. Eisenbud, C. Huneke, W. Vasconcelos (1992): Direct methods for primary decomposition, *Invent. Math.* **110** 207–235.

P. Gianni, B. Trager, G. Zacharias (1988): Gröbner bases and primary decomposition of polynomial ideals, in *Computational Aspects of Commutative Algebra*, edited by L. Robbiano, Academic Press, New York, 15–33.