Summer Project

Bhavana Nancherla David Drescher

August 10, 2001

Over the summer we embarked on a brief introduction to various concepts in algebraic geometry. We used the text Ideals, Varieties, and Algorithms, by Cox, Little and O'Shea, as our main source, supplementing as needed. For this paper, we will assume the reader has some knowledge of algebraic geometry.

We began by assuming an algebraically closed field k, over which we defined a polynomial ring, $k[x_1, \ldots, x_n]$. We defined an affine variety, and soon related this geometric structure to that of an ideal. Ideals and varieties provide a correspondence between algebra and geometry, one which we will come back to later. After learning the definitions of these two structures, we aimed to answer some general questions about them, posed by the text [1].

(1) Can every ideal be written as $\langle f_1, \ldots, f_s \rangle$ for some $f_1, \ldots, f_s$ in $k[x_1, \ldots, x_n]$?

(2) Given an ideal I, and $f \in k[x_1, \ldots, x_n]$, is there an algorithm to determine whether $f \in I$?

(3) Given a parametrization of a variety $V \subset k^n$

$$\begin{aligned} x_1 &= g_1(t_1, \ldots, t_m), \\ &\vdots \\ x_n &= g_n(t_1, \ldots, t_m), \end{aligned}$$

can we find a system of polynomial equations (in the x_i) which define the variety?

(4) Can we find all the common solutions in k^n of a system of polynomial equations?

$$f_1(x_1, \ldots, x_n) = \cdots = f_s(x_1, \ldots, x_n) = 0$$

(5) Given $f_1, \ldots, f_s$, what is the relationship between $\langle f_1, \ldots, f_s \rangle$ and $\mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))$ (which is the ideal of the variety defined by $f_1 = \ldots = f_s = 0$)?

The first two questions are answered using Hilbert's Basis Theorem and with the construction of Groebner bases. The third and fourth questions are solved

by the study of elimination theory, and the last problem is the motivation for the Nullstellensatz, or the Algebra-Geometry dictionary, which maps out the exact relationship between ideals and varieties.

As Groebner bases (defined below) play a significant role in all the questions, our focus lied in understanding their existence and construction. Hilbert's Basis Theorem proves the existence of a Groebner basis for all ideals, thus answering the first question in the affirmative, by stating that every ideal $I \subset k[x_1, \ldots, x_n]$ has a finite generating set.

Another important consequence of the Hilbert Basis Theorem is the Ascending Chain Condition for ideals, which states that every increasing sequence of ideals

$$I_1 \subset I_2 \subset I_3 \subset \cdots$$

eventually terminates, meaning there is some $N \geq 1$ such that

$$I_N = I_{N+1} = \cdots.$$

This idea will become important when we come to the Nullstellensatz.

The answer to the second question is straightforward if we work in a polynomial ring with only one variable. In this case, the division algorithm can be used to determine ideal membership, as the remainder of division by an ideal is unique. If we use a multivariable polynomial ring, the situation gets more complex. In $k[x_1, \ldots, x_n]$, the division algorithm is defined using a monomial ordering. However, it lacks the nice property of giving a unique remainder, which enabled it to determine ideal membership in the single variable case. The solution to this problem is to make the generators of the ideal into a Groebner basis. If we do so, it turns out that the division algorithm does indeed allow us to determine ideal membership.

Strictly defined, a Groebner basis is a finite subset $G = \{g_1, \ldots, g_s\}$ of an ideal I such that

$$\langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_s) \rangle = \langle \mathrm{LT}(I) \rangle.$$

LT is shorthand for the leading term of a polynomial, which is defined once a monomial ordering is fixed.

If we take $\{f_1, \ldots, f_s\}$ as an arbitrary set of generators for I we can create elements of I that are the result of syzygies on the leading terms of the generators. These are known as S-polynomials, denoted $S(f_i, f_j)$; they are the polynomial result of applying a syzygy that causes the leading terms of f_i and f_j cancel. Because of this cancellation, S-polynomials can be indivisible by the $\{f_1, \ldots, f_s\}$, leading to non-zero remainders, even though they are elements of I.

Groebner bases avoid this problem as they are a set of generators whose leading terms generate the leading terms of every element in I. This means there can be no polynomials whose leading terms are not divisible by the generators in I. In other words, when we use a Groebner basis, there can be no S-polynomials whose remainder on division by I is nonzero.

In fact, this is exactly the nature of the algorithm used to generate a Groebner basis for I. Buchberger's algorithm calculates all the S-polynomials for the

given set of generators of I, and then computes their remainders from division by I. Those non-zero remainders get appended to the list of generators, (and correspondingly, more S-polynomials calculated.) This process continues until no non-zero remainders occur, which indicates that all the S-polynomials are divisible by the set of generators. This indicates that the set of generators is a Groebner basis. An important point is that this algorithm always terminates.

Improvements of Buchberger's algorithm involve decreasing the number of S-polynomials to check, by removing any redundant ones. S-polynomials, and more generally, syzygies, will come up again when we discuss modules and resolutions. We also briefly looked at a paper by Pottier [3] which outlined another algorithm for generating a Groebner basis.

Another important process is reduction of a Groebner basis. A Groebner basis G is reduced if $\forall p \in G$,

(i) the leading coefficient of p is 1, and

(ii) no monomial of p lies in $\langle \mathrm{LT}(G - \{p\})\rangle$.

In general, given any ideal $I \neq \{0\}$, once we choose a monomial ordering, I has a unique reduced Groebner basis. Thus, we have the answer to the second question: the division algorithm in combination with a Groebner basis determines ideal membership.

Groebner bases are also involved in the solutions to the remaining questions. The next two questions are the motivation for the study of elimination theory, which holds over any algebraically closed field, although some of the theorems we studied were proved only over $\mathbf{C}$.

The l^{th} elimination ideal, I_l, is defined for $I = \langle f_1, \ldots, f_s\rangle \subset k[x_1, \ldots, x_n]$, where

$$I_l = I \cap k[x_{l+1}, \ldots, x_n].$$

The Elimination Theorem states that the Groebner basis of I_l, for $1 \leq l \leq n$, is

$$G_l = G \cap k[x_{l+1}, \ldots, x_n],$$

where G is the Groebner basis of I with respect to the lexicographical monomial ordering, and where $x_1 > x_2 > \cdots > x_n$. Elimination is used to implicitize equations, and this is the process used to get rid of parameters, as described in the third question.

If we work with the varieties of the ideals instead of the ideals themselves, we find that not all the solutions in the variety of the l^{th} elimination ideal, $\mathbf{V}(I_l)$, can be completed to ones in $\mathbf{V}(I)$. The Extension Theorem gives the conditions necessary for a partial solution to extend to one in $\mathbf{V}(I)$. This theorem states that if we rewrite each polynomial in I such that the polynomial in the last l variables is the leading "coefficient" of each polynomial, then extension fails when all of these leading coefficients vanish simultaneously. The Closure Theorem focuses on the varieties themselves, describes the relationship between $\mathbf{V}(I_l)$ and the projection map $\pi_l(V)$ which consists of exactly those partial solutions of $\mathbf{V}(I_l)$ which can be extended to $\mathbf{V}(I)$. An important aside is that if we

choose to work in projective space, an analogous, but slightly different theorem called the Projective Elimination Theorem states that all partial solutions will always extend to complete solutions. We will come back to projective spaces later.

Elimination theory also aids in answering the fourth question, as we can use the implicitized polynomial to solve for partial solutions. The Extension theorem then tells us which of these solutions can be extended to complete ones. Briefly, we also studied singular points and envelopes of a variety, which are an application of elimination theory. Finally, we learned about resultants, which provide an alternative method of proving the theorems of elimination theory.

The proof of the Closure Theorem is dependent on the Nullstellensatz. In fact, $\mathbf{V}(I_l)$ is the Zariski closure of $\pi_l(V)$. This final topic rounds out our study of ideals and varieties by showing the relationship between these two structures. Until now, our focus has been algebraic, on computing and manipulating ideals. Studying the Nullstellensatz revealed the geometric picture, and introduced the radical ideal, $\sqrt{I}$, which is equal to $\mathbf{I}(\mathbf{V}(I))$ for any ideal I. This allows for the creation of a bijection between radical ideals and varieties. Further correspondences can be made, notably the Descending Chain Condition for varieties, which is the inclusion-reversing result of the Ascending Chain Condition of ideals mentioned above. A relationship exists between irreducible varieties and prime ideals, and ideal sums, products, intersections, and quotients also have analogous geometric structures.

We will be doing some of our computations in n-dimensional projective space over a field k, $\mathbb{P}^n(k)$. We define this as the set of equivalence classes of '$\sim$' on $k^{n+1} - \{0\}$, where $(x'_0, \ldots, x'_n) \sim (x_0, \ldots, x_n)$ if there exists a λ such that $(x'_0, \ldots, x'_n) = \lambda(x_0, \ldots, x_n)$. So $\mathbb{P}^n(k) = (k^{n+1}) - \{0\}/\sim$.

Since $\mathbb{P}^n(k)$ is the union of $n+1$ copies of the affine space k^n ($\mathbb{P}^n(k) = \bigcup_{i=0}^{n} U_i$, where $U_i = \{(x_0, \ldots, x_n) \in \mathbb{P}^n(k) : x_i \neq 0\}$) it makes sense to want to define varieties in this new context. If we look at a polynomial $f \in k[x_0, \ldots, x_n]$, the variety $\mathbf{V}(f)$ only makes sense if f is homogeneous. So we can define a projective variety, $\mathbf{V}(f_0, \ldots, f_s)$, in the same way as a variety of the affine space $k[x_0, \ldots, x_n]$, but with the extra stipulation that the polynomials $f_0, \ldots, f_s$ are all homogeneous. We can also convert a projective variety into its corresponding affine variety by taking the intersection of the variety with one of the affine spaces whose union makes up $\mathbb{P}^n(k)$. This will give us an affine variety, V, in k^n.

A relation similar to that in the affine case exists between ideals and varieties. Obviously an ideal in $k[x_0, \ldots, x_n]$ cannot contain only homogeneous polynomials even if the generating polynomials are homogeneous since adding two homogeneous polynomials does not always result in a homogeneous polynomial (i.e. if the two polynomials have different degree). However the affine definition of an ideal $I \in k[x_0, \ldots, x_n]$ can be extended to the projective case by adding the requirement that for each $f \in I$, the homogeneous components of f are in I also.

From this definition of a projective ideal we can establish the obvious speci-

fications for such an ideal. For example, an ideal, I, is homogenous if and only if I has a basis of homogeneous polynomials. This assertion follows directly from our definition of a homogeneous ideal and the use of the Hilbert Basis Theorem. We can also show that the reduced Groebner bases of a homogenous ideal consists of homogeneous polynomials. These two properties of homogeneous ideals lead us to the relations between projective varieties and homogeneous ideals. Given the maps $\mathbf{I}$ and $\mathbf{V}$, the homogeneous ideal $I \subset k[x_0, \ldots, x_n]$, and the projective variety $V \subset \mathbb{P}^n(k)$–where:

$$\mathbf{V}(I) = \mathbf{V}(f_1, \ldots, f_s)$$

if $I = \langle f_1, \ldots, f_s \rangle$.

$$\mathbf{I}(V) = \{f \in k[x_0, \ldots, x_n] : f(a_0, \ldots, a_n) = 0, \quad \text{with} \quad (a_0, \ldots, a_n) \in V\}.$$

Then $\mathbf{V}(I)$ is a projective variety and $\mathbf{I}(V)$ is a homogeneous ideal. In addition, if k is an algebraically closed field, then these two maps bijections and inverses of each other by the projective version of the Nullstellensatz (provided $\mathbf{V}(I)$ is nonempty, and $I \neq \langle x_0, \ldots, x_n \rangle$).

To get a better grasp on the properties of degree and dimension we delved into the topic of modules. The notion of modules and of varieties and ideals are in fact related. Given a variety $V \subset k[x_1, ..., x_n]$, V corresponds algebraically to the ideal $\mathbf{I}(V) = \langle g_1, \ldots, g_s \rangle$, where the g_i's form a Groebner basis of V. In this case $I = \mathbf{I}(V)$ is a simple module of the polynomial ring $k[x_1, \ldots, x_n]$. Given a basis of the ideal, $f_1, \ldots, f_t$,

$$I = a_1 f_1 + \cdots + a_t f_t, \forall a_i \in k[x_0, \ldots, x_n].$$

So we see that the ideal I satisfies all of the requirements of a module over $k[x_0, \ldots, x_n]$. This seems somewhat arbitrary, after all whether we call it a module or an ideal it still has the same structure. However, by treating I as a module we can work with module homomorphism on modules over the same ring as I. Given a ring, R, and two R-modules N and M, if $N = R^l$ and $M = R^k$ for some $l, k \in \mathbb{N}$, then any homomorphism $\varphi : N \to M$ is just multiplication by an $l \times k$ matrix. This follow from the one dimensional case, where if we have a homomorphism $\theta : R \to R$, then $\forall a \in R$

$$\theta(a) = \theta(a \cdot 1) = a\theta(1).$$

This can be done because $R = \langle 1 \rangle$. So given $\theta(1) = f$, θ is defined simply as multiplication by f. We can generalize to the case of R^l and R^k by treating the generators as the unit vectors $e_1, \ldots, e_l$ and $e_1, \ldots, e_k$, where e_i is defined as a column vector with a 1 in the ith row and zeros in all of the other rows. With our original homomorphism φ we see that the homomorphism can be completely defined by the values of $\varphi(e_i)$ since these column vectors generate R^l. Since φ is a map to R^k, φ is just matrix multiplication. Thus it is pretty straightforward to deal with homomorphisms between the free modules of the form R^i, $i \in (N)$, free here meaning having a linearly indpendent basis. Things

are not so simple when we deal with the case $R = k[x_1, \ldots, x_n]$ and a module that is generated by more than two elements of degree greater than zero in R. For example looking at the module $M = \langle x^2, y^3 \rangle \subset k[x, y]$, a homomorphism cannot be just an arbitrary assignment on the generators of M. If we define a homomorphism, $\varphi : M \to R$ by $\varphi(x^2) = y$ and $\varphi(y^3) = x$ we get the undesirable result:

$$\varphi(y^3x^2 - x^2y^3) = \varphi(0) = 0.$$

$$\varphi(y^3x^2 - x^2y^3) = \varphi(y^3x^2) + \varphi(-x^2y^3) = y^3\varphi(x^2) - x^2\varphi(y^3) = y^4 - x^3 \neq 0.$$

So we see that φ is not properly defined in this case. If we generalize this example we see that if we are not dealing with a free module then we cannot simply define a homomorphism by mapping the basis elements of a module. Let M be any R-module generated by two or more elements of R, given two such elements f_1 and f_2 we have an automatic relation $f_2f_1 - f_1f_2 = 0$. So to understand any non-free finitely generated module we must know the relations of its generators.

Given a finitely generated module $M \subset R^t$, and a set of generators of M, $f_1, \ldots, f_s$, any relation between generators will have the form:

$$a_1f_1 + \cdots + a_sf_s = 0, \text{with} \quad a_1, \ldots, a_s \in R^t$$

We see that the set of all such relations is just the set of syzygies on the generators. This turns out, not surprisingly, to be a submodule of M (a quick check reveals that it's closed under addition and scalar multiplication) hence is also finitely generated. So determining the generators of the syzygy module will give us all of the information we need about the relations on the generators of M.

In order to compute the generators of a syzygy module, we must first be able to find a Groebner basis in terms of modules. Looking at Buchberger's algorithm for ideals, we only need to modify our monomial order to account for the position of a term as well as its value, and to modify our notion of the S-polynomial to allow for column vectors. Both of these tasks can be worked out easily using the notion of basis vectors, and the resulting changes to Buchberger's algorithm gives us a method for determining a Groebner basis for a module. With such a basis we can compute a Groebner basis for the syzygy module using Schreyer's Thm.

With this method in hand we can start to use exact sequences to learm more about the structure of a finitely generated module M. Given a sequence of R-modules and homomorphisms

$$\cdots \to M_{i+1} \xrightarrow{\varphi_{i+1}} M_i \xrightarrow{\varphi} M_{i-1} \xrightarrow{\varphi_{i-1}} \cdots$$

the sequence is said to be exact at M_i if the image of φ_{i+1} is equal to the kernel of the map φ_i. The sequence is exact if it is exact at all of the modules but the first and last.

Given a finitely generated R-module, M, we can then begin to build a sequence where every module is a free module besides M and which is exact. First

we define a trivial homomorphism mapping all of M to zero. Then we can define a homomorphism, $\varphi_0 : R^{s_0} \to M$ defined by multiplication by the matrix

$$\begin{pmatrix} g_1 & g_2 & \cdots & g_s \end{pmatrix}$$

where the g_i's form a Groebner basis of M. The image of φ_0 is M since M consists of all $f \in R$ of the form

$$f = a_1 g_1 + \cdots + a_s g_s, \quad (a_1, \ldots, a_s) \in R^{s_0}.$$

Thus $textrmim(\varphi_0)$ is equal to the kernel of the trivial homomorphism from M to 0. If we take a look at the kernel of φ_0, we see that this is just the syzygy module of M. Using Schreyer's theorem we can then compute a Groebner basis for the syzygy module, denoted by $h_1, \ldots, h_t$ where $h_i \in R^{s_0}$ for each i. We define a homomorphism $\varphi_1 : R^{s_1} \to R^{s_0}$ by multiplication by the matrix

$$\begin{pmatrix} h_{11} & \cdots & h_{1s_1} \\ \vdots & \ddots & \vdots \\ h_{s_0 1} & \cdots & h_{s_0 s_1} \end{pmatrix}$$

where the h_{ij}'s are the ith entries of the jth syzygy generator. Since we have a Groebner basis of the first syzygy module we can use Schreyer's theorem again to compute a Groebner basis of the second syzygy module, the syzygy module for the first syzygy generators. We can then create another homomorphism, φ_2 from the second syzygy module to the first. If we keep adding modules and homomorphisms in this manner we get an exact sequence

$$\cdots \xrightarrow{\varphi_3} R^{s_2} \xrightarrow{\varphi_2} R^{s1} \xrightarrow{\varphi_1} R^{s_0} \xrightarrow{\varphi_0} M \to 0$$

in which each φ_i, except φ_0, is matrix multiplication by a matrix whose columns are the generators of the syzygy module of the columns of the φ_{i-1} matrix. So our sequence is exact because the image of φ_i is by construction the kernel of φ_{i-1}. The sequence is finite if the kernel of φ_i, for some i, is a free module. At this point, we can define the homomorphism $\varphi_{i+1} : R^{s_i+1} \to R^{s_i}$ in the usual manner so that im(φ_{i+1} is equal to the syzygy module ker(φ_i). Since ker(φ_{i+1}) = 0, from the fact that the generators of im(φ_{i+1}) are linearly independent, we can make the sequence exact at R^{i+1} by defining a trivial homomorphism of identity from 0 to R^{i+1}. Thus we will have a finite exact sequence of free modules describing the module M. All free resolutions are not necessarily finite, but since we will be working over the polynomial ring, $k[x_1, \ldots, x_n]$, we can use Hilbert's Syzygy Theorem, which states that all free resolutions of finitely generated $k[x_1, \ldots, x_n]$-modules are finite of length at most n. Hence the last free module in our free resolution outlined above will be R^{s_n}.

If we work in projective space we can get even more information about a module. First, we must work with homogeneous modules, similar to homogeneous ideals, these are generated by vectors of homogeneous polynomials, and have Groebner bases that are made up of such vectors. With $R = k[x_0, \ldots, x_n]$,

R has a graded structure—meaning that we can represent R as the direct sum of the additive groups of homogenous polynomials of the same degree. If we let R_t represent the group of polynomials of degree t, then we have

$$R = \bigoplus_{t \in \mathbb{N}} R_t.$$

We can see the graded structure on a homogeneous module M, by defining M_t as $(R_t)^s \cap M$, where $M \subset R^s$. By the definition of a module, the M_t's will also be additive groups and

$$M = \bigoplus_{t \in \mathbb{N}} M_t.$$

We can also define homomorphisms between homogeneous modules by specifying that a graded homomorphism sends each graded segment of a module to its own graded segment. In other words, a graded homomorphism maintains the structure of a graded module—if $\varphi : M \to N$ is a graded homomorphism between two graded modules, then $\varphi(M_t) \subset N_{t+d}$ for all t. In this case, we see that φ sends degree t polynomials to degree $t + d$ polynomials, and φ is said to have degree d.

We can encode information about the degree of a homomorphism into its domain by introducing the notation

$$M(d) = \bigoplus_{t \in \mathbb{Z}} M_{d+t},$$

where the module $M(d)$ is simply M offset by degree d. Thus we can turn our homomorphism φ into a degree zero homomorphism by specifying its domain as $M(-d)$. Since $M(-d)_t = M_{t-d}$, we have $\varphi(M(-d)_t) \subset N_t$. From our notion of a free resolution we can now derive the notion of a graded resolution—a free resolution of a homogeneous module consisting in free modules and graded homomorphisms of degree zero. Fortunately, Hilbert's Syzygy Theorem also holds for graded resolutions, so every finitely generated homogeneous module has a finite graded resolution of length at most n.

So given such a module, we have its graded resolution

$$0 \to R(d_n)^{s_n} \xrightarrow{\varphi_n} \cdots \xrightarrow{\varphi_1} R(d_0)^{s_0} \xrightarrow{\varphi_0} M \to 0.$$

With this we can determine the Hilbert function, the function determining the dimension of M over the field k (since in our case M is a module over $k[x_0, \ldots, x_n]$). First the dimension of the free modules will be defined by

$$H_{R(d)}(t) = \dim_k R(d)_t = \binom{t+d+n}{n},$$

which is just a simple adaptation of the $R(0)$ case. Then using the fact that with a linear map $\theta : V \to W$, $\dim_k(V) = \dim_k(\ker(\theta)) + \dim_k(\mathrm{im}(\theta))$, we see

that the alternating sum of the dimensions of the modules in our resolution equals zero. Hence for our graded resolution above

$$H_M(t) = \dim_k M_t = \sum_{i=0}^{n} (-1)^i \dim_k (R(d_i)^{s_i})_t.$$

In this context, the formula gives us not only the Hilbert function, but the Hilbert polynomial as well. It is useful to obtain this polynomial because it provides us with some useful information

2

. If we have a homogeneous ideal $I \subset k[x_0, \ldots, x_n]$ that determines the variety $V = \mathbf{V}(I)$, then the degree of the Hilbert polynomial of R/I is the dimension of the variety, and the leading coefficient is of the form $D/d!$ where $d = \dim V$ and D is the degree of V. So determining the Hilbert polynomial answers many of our original questions about varieties and ideals.

The experimental section of our project began with the study of the rational normal curve. This is a curve in projective n-space, $k[x_0, \ldots, x_n]$, where the variables $x_0, \ldots, x_n$ are parametrized by s and t as follows:

$$x_0 = s^n \qquad x_1 = s^{n-1}t \qquad \ldots \qquad x_{n-1} = st^{n-1} \qquad x_n = t^n$$

The curve is then defined by all the relations between the $\{x_i\}$. The set of these relations can be generated by the set of determinants of the 2×2 minors of the following $2 \times n$ matrix:

$$\begin{pmatrix} x_0 & x_1 & \ldots & x_{n-1} \\ x_1 & x_2 & \ldots & x_n \end{pmatrix}$$

This is a result which we took for granted.

We used Macaulay 2 to perform computations involving this ideal. First, we verified that these relations form a Groebner basis for the ideal they generate. Then, we studied the resolutions of this curve for different values of n, and tried to come up with a general pattern for the n^{th} case.

We noticed that the generators of the first syzygy module are encoded in the $3 \times n$ matrices created by appending each of the 2 rows in turn to the $2 \times n$ matrix shown above. By taking the 3×3 minors of either of these matrices, and expanding their determinants along the bottom row, we found that each minor gave a generator for the first syzygy module (although some of these generators were redundant and unnecessary). We hypothesized that this pattern continues, where the i^{th} syzygy module is generated by the determinants encoded in the $(i+2) \times n$ matrices. These are created recursively by appending each row in turn to each of the $(i-1)^{th}$ syzygy module generating matrices. This process should terminate with the creation of $n \times n$ matrices, which must then correspond to the final syzygy module. As we always start with $3 \times n$ matrices for the first syzygy module, and end with the $n \times n$ matrices, this implies that the rational normal curve in $\mathbf{P}^n$ has a resolution of length $n - 2$.

We also looked at the gradings for these resolutions. The graded resolutions for a few values of n are given below. There appears to be a relationship between the grading on each module and the number of generators for that module, such that one can predict the resolution for a given n. Here, $K = k[x_0, \ldots, x_n]$.

n	Resolution
2	$0 \to K(-2)^1 \to I \to 0$
3	$0 \to K(-3)^2 \to K(-2)^3 \to I \to 0$
4	$0 \to K(-4)^3 \to K(-3)^8 \to K(-2)^6 \to I \to 0$
5	$0 \to K(-5)^4 \to K(-4)^{15} \to K(-3)^{20} \to K(-2)^{10} \to I \to 0$
6	$0 \to K(-6)^5 \to K(-5)^{24} \to K(-4)^{45} \to K(-3)^{40} \to K(-2)^{15} \to I \to 0$

If we look only at the syzygy module gradings (ignoring the 0 and I modules), and we take the product of the grading and the power for each module, we see the following:

n	Products
2	(-2)
3	$(-6, -6)$
4	$(-12, -24, -12)$
5	$(-20, -60, -60, -20)$
6	$(-30, -120, -180, -120, -30)$

Now when we pull out the greatest common factor of each row of products, and call it x, we see that the product pattern is Pascal's triangle, and that x also follows a pattern.

n	x	Pattern
2	-2	(1)
3	-6	$(1, 1)$
4	-12	$(1, 2, 1)$
5	-20	$(1, 3, 3, 1)$
6	-30	$(1, 4, 6, 4, 1)$
n	$-n(n-1)$	$(n-2)^{th}$ row of Pascal's $\triangle$

We can take this pattern and apply it back onto the resolution to formulate a general format for the resolution of the rational normal curve in $\mathbf{P}^n$. A typical resolution of length $n-2$ for the ideal I is written as follows:

$$0 \to F_{n-2} \to F_{n-1} \to \cdots \to F_1 \to F_0 \to I \to 0.$$

If we take I to be the ideal of the rational normal curve in $\mathbf{P}^n$, then our pattern reveals that for each i, $F_i = K(-i-2)^j$ where K is as defined above, and $j = n(n-1)\binom{n-2}{i}/(i+2)$.

Given this pattern for the resolution, we can easily see that the Hilbert polynomial, which relies on the grading and the number of generators (the power), also follows a pattern. Using Macaulay 2 (and also manually, in some cases), we calculated the Hilbert polynomial for the quotient ideal of the polynomial ring modulo the ideal of the rational normal curve, and found that this indeed

was the case. For the rational normal curve in projective n-space, the Hilbert polynomial of the quotient ideal is $nt + 1$. This implies that the dimension of the curve is 1 and the degree of the curve is n.

We extended the project to study random projections of the rational normal curve from n-space to $(n-1)$-space. These projections were generated by taking linear combinations of $s^i t^{n-i}$ where the coefficents were randomly generated integers in the field $\mathbf{Z}$ mod k for some prime number k. These linear combinations were then assigned to $n-1$ variables, $x_1, \ldots, x_n$, as shown here.

$$\begin{aligned} x_1 &= a_{1,0}s^n + a_{1,1}s^{n-1}t + \ldots + a_{1,n-1}st^{n-1} + a_{1,n}t^n \\ x_2 &= a_{2,0}s^n + a_{2,1}s^{n-1}t + \ldots + a_{2,n-1}st^{n-1} + a_{2,n}t^n \\ &\vdots \\ x_n &= a_{n,0}s^n + a_{n,1}s^{n-1}t + \ldots + a_{n,n-1}st^{n-1} + a_{n,n}t^n \end{aligned} \qquad a_{i,j} \in \mathbf{Z}/k; k \text{ prime}$$

We then used Macaulay 2 and applied elimination theory to create implicitized generators in $\{x_1, \ldots, x_n\}$. We used these generators to define an ideal, for which we then computed the quotient ideal (as above) of the polynomial ring modulo the ideal. We then compared the Hilbert polynomials of these quotient ideals in hopes of finding a general trend.

For this process, we wrote a program which can be used in Macaulay 2 that generates a set of random linear combinations of the rational normal curve and then gives the Hilbert polynomial of the quotient ideal created from that set. The code and instructions for the program are given in further detail below.

Our method can be replicated by creating a file with file name "projections" in one's home directory, and putting the following text in this file.

```
R = ZZ/k[s,t,MonomialOrder=>Lex]
S = ZZ/k[s,t,x_1..x_r,MonomialOrder=>Lex]
T = ZZ/k[x_1..x_r,MonomialOrder=>Lex]
a = substitute(matrix{{x_1}..{x_r}},S)
g = s -> (b = substitute(
matrix table(s,1,(i,j) -> random(s,R)),S) - a,
hilbertPolynomial(T/substitute(ideal(selectInSubring(2,
generators(gb(ideal b)))),T),Projective=>false))
f = i -> for k from 1 to i do print g r
```

It is important that there are no return keystrokes placed in the midst of an assignment (especially that of 'g'). Errors may occur unless each assignment is made in one continuous line. After creating this file, start Macaulay 2. Here, one needs to numerically define `k` as some prime number. This number is used to define the field as $\mathbf{Z}$ mod k. Also numerically define `r`, which is the value for the n-space that the projection is made from. For example, if `r` $= 4$, this will create a projection from projective 4-space to projective 3-space. Once these values have been defined, type:

```
load "projections"
f m
```

Here `m` is the number of times you would like the algorithm to repeat; one round of `f` gives one set of random linear combinations and the Hilbert polynomial generated by this set.

Using this program, we ran trials for different values of `r` and `k`. Approximately 40 to 50 trials were done for each value of `r` and `k` was usually 101 or 31991, although we did also use 2 to produce the degenerate Hilbert polynomials. The following Hilbert polynomials for each value of `r`. The second column shows the Hilbert polynomial that was generated most frequently, followed in the third column by values for degenerate linear combinations.

	Hilbert polynomials	
`r`	Most frequent	Others seen
2	t+1	1
3	3t	2t+1,t+1
4	4t+1	4t-2,3t+1,3t,t+1
5	5t+1	5t,5t-1,4t+1,4t
6	6t+1	6t,6t-1,5t+1,5t

Looking at these results, we can observe that the dimension of the curve is almost always 1, except for a degenerate case of 2-space to 1-space, where the dimension is 0. The degree is predictable for larger values of `r`, as the general Hilbert polynomial then takes the form $\mathtt{r}t + 1$. This is analogous to the case of the rational normal curve. The degenerate Hilbert polynomials are not entirely predictable, although for `r`-values of 5 and 6, the Hilbert polynomials generated give analogous sets for the respective `r`.

These computations concluded our study of algebraic geometry this summer. Further work on this topic could include proving the conjectures made in this paper, especially that of the resolution pattern for the rational normal curve.

References

[1] D. Cox, J. Little, and D. O'Shea (1997), *Ideals, Varieties, and Algorithms,* Springer-Verlag, New York-Berlin-Heidelberg.

[2] D. Cox, J. Little, and D. O'Shea (1998), *Using Algebraic Geometry,* Springer-Verlag, New York-Berlin-Heidelberg, 179-221, 234-271.

[3] L. Pottier (July, 1996), *The Euclidean Algorithm in Dimension* n*,* ISSAC 96, ACM Press.