BEZOUT THEOREM

One of the most fundamental results about the degrees of polynomial surfaces is the Bezout theorem, which bounds the size of the intersection of polynomial surfaces. The simplest version is the following:

Theorem 0.1. *(Bezout in the plane) Suppose $\mathbb{F}$ is a field and P, Q are polynomials in $\mathbb{F}[x, y]$ with no common factor (of degree ≥ 1). Let $Z(P, Q) := \{(x, y) \in \mathbb{F}^2 | P(x, y) = Q(x, y) = 0\}$. Then the number of points in $Z(P, Q)$ is $\leq (degP)(degQ)$.*

There are several approaches to proving the Bezout theorem. I found one approach that feels closely related to the methods we've been studying. (It appears in Joe Harris's book *Algebraic Geometry, a First Course*, exercise 13.17.)

The proof uses the unique factorization of polynomials. We recall exactly what this means.

For any field $\mathbb{F}$, the ring of polynomials over $\mathbb{F}$ in n variables, $\mathbb{F}[x_1, ..., x_n]$ obeys unique factorization. The units in this ring are exactly the non-zero elements of $\mathbb{F}$. A non-zero polynomial P is called irreducible if whenever $P = P_1 \cdot P_2$, one of P_1, P_2 is a unit. Unique factorization says that if P can be written as a product of irreducibles in two different ways, say $P = \prod_i P_i = \prod_j Q_j$, then there are the same number of factors in each product, and we can reorder the indices so that $Q_i = c_i P_i$ where $c_i \in \mathbb{F} \setminus \{0\}$.

There are a number of variations on the statement of the Bezout theorem, and we mention them later.

1. A proof of Bezout in the plane

Let $\bar{I}$ be the ideal generated by P, Q, and let $S = \mathbb{F}[x, y]/\bar{I}$. We can roughly think of S as the ring of polynomial functions on $Z(P, Q)$, and it follows from this that $|Z(P, Q)| \leq dimS$. (We think of S as a vector space over $\mathbb{F}$ in order to define its dimension.)

Lemma 1.1. $|Z(P, Q)| \leq dimS$.

Proof. For any set $X \subset \mathbb{F}_2$ let E_X be the evaluation (or restriction) map from $\mathbb{F}[x, y]$ to $Fcn(X, \mathbb{F})$. If X is a finite set, then E_X is surjective. We state this as a lemma, and we'll prove it later.

Lemma 1.2. *If $X \subset \mathbb{F}^n$ is any finite set, and $f : X \to \mathbb{F}$ is any function, then there is a polynomial which agrees with f on X.*

If $X \subset Z(P,Q)$, then $\bar{I}$ is in the kernel of E_X, and so we can think of E_X as a map from S to $Fcn(X, \mathbb{F})$. If $X \subset Z(P,Q)$ is finite, then E_X is surjective, and so $dim S \geq |X|$. □

Our goal is to bound the dimension of S by $(degP)(degQ)$. In order to do this, we will mod out by P and then by Q, and keep track of dimensions of the objects at each step.

Let I be the ideal of $\mathbb{F}[x,y]$ generated by P. Let $R = \mathbb{F}[x,y]/I$. The dimensions of R and I are both infinite, but we can get valuable information by considering polynomials of degree $\leq d$. Let $V_d \subset \mathbb{F}[x,y]$ be the polynomials of degree $\leq d$. Let $I_d = I \cap V_d$, and let $R_d = V_d/I_d \subset R$. We will consider the dimensions of these spaces as functions of d.

The dimension of V_d is $\binom{d+2}{2}$, as we have seen.

Lemma 1.3. *The dimension of I_d is $dim V_{d-D} = \binom{d-D+2}{2}$ for all $d \geq D$.*

Proof. Multiplication by P gives a linear map from V_{d-D} to I_d. We claim this linear map is an isomorphism. The kernel of the map is zero. Any element in I_d can be written as PQ for some Q, and we must have $degQ \leq d - D$, so that the map is surjective. □

The dimension of R_d is $dim V_d - dim I_d = \binom{d+2}{2} - \binom{d-D+2}{2} = Dd + (3/2D - D^2)$, for $d \geq D$.

Now let J be the ideal of R generated by Q. Let $S = R/J$, and note that this is the same ring S defined above. Let $J_d = J \cap R_d$ and $S_d = R_d/J_d$.

Lemma 1.4. *The dimension of J_d is $\geq dim R_{d-E}$.*

Proof. Multiplication by Q gives a map from R_{d-E} to J_d. We claim that this map is injective. Suppose $r_1 \in R_{d-E}$ is in the kernel of the map. Let $P_1 \in V_{d-E}$ be a polynomial representing r_1. We see that QP_1 is in I, so $QP_1 = PP_2$ for some polynomial P_2. By unique factorization, we see that P divides P_1. But then $P_1 \in I$ and $r_1 = 0$. □

(Exercise: Do we get equality in this lemma?)

The dimension of S_d is $dim R_d - dim J_d \leq dim R_d - dim R_{d-E}$. If $d \geq D + E$, then

$$dim R_d - dim R_{d-E} = \left[Dd + (3/2D - D^2)\right] - \left[D(d-E) + (3/2D - D^2)\right] = DE.$$

Since this holds for every d, we conclude that $dim S \leq DE$ and so $|Z(P,Q)| \leq DE$.

1.1. **Polynomials with prescribed values.** Now we return to Lemma 1.2 at the beginning of the last section:

Lemma 1.5. *If $X \subset \mathbb{F}^n$ is any finite set, and $f : X \to \mathbb{F}$ is any function, then there is a polynomial P of degree $\leq |X| - 1$ which agrees with f on X.*

Proof. For each $p \in X$, we will construct a polynomial P_p with $P_p(p) = 1$ and $P_p = 0$ on $X \setminus p$. Fix p. For each $q \in X \setminus p$, let L_q be a polynomial that vanishes at q but not at p. Then define $P_p = c \prod_{q \in X \setminus p} L_q$. We see that $P_p(q) = 0$ for each $q \in X \setminus p$, and that $P_p(p) \neq 0$. By choosing the constant c, we can arrange that $P_p(p) = 1$. The degree of P_p is $|X| - 1$.

Finally, for an arbitrary function f, we define $P = \sum_{p \in X} f(p) P_p$. □

2. Statements of the Bezout theorem

The Bezout theorem is usually stated as an equality (by algebraic geometers). It roughly says that if P and Q have no common factor, then the "number" of points in $Z(P, Q)$ is equal to $(degP)(degQ)$. To make this work we need to work over an algebraically closed field and we need to work over projective space, and we need to count intersections with multiplicity.

For example, let's try to consider two circles $x^2 + y^2 = 100$ and $(x-5)^2 + y^2 = 100$. Initially, we consider x, y in $\mathbb{R}$, where we can easily visualize the circles. They appear to intersect in two points. Where are the other two points? What if we allow x, y to be complex numbers? In fact this doesn't lead to any more intersection points. But if we work over complex projective space, we get two more interesection points at infinity. Now what if we slide the circles apart so that they become tangent and then disjoint. In $\mathbb{R}^2$, the number of intersection points goes from 2 to 1 to 0. When the circles become disjoint over $\mathbb{R}^2$ they develop two points of intersection in $\mathbb{C}^2 \setminus \mathbb{R}^2$. At the moment of tangency, there is only one intersection point in $\mathbb{C}^2$, plus two intersection points at infinity. But this one intersection point at the tangency has "multiplicity 2". Counting with multiplicity, there are still exactly four intersection points.

The full statement of the equality Bezout theorem requires some work to define the multiplicities of the intersections. Because the statement is more complicated the full proof is rather longer than this. But the inequality version is what we will need in our applications. In my opinion, the inequality version of the Bezout theorem is somewhat underrated. It takes only a fraction of the effort to state and prove it, and it still has many applications.

3. The Hilbert polynomial

To give context, we mention without proof some important related concepts. (I don't really know this area myself. I hope there are not errors. Anyway, we won't use any of these statements later.)

Let's look back at the proof of the Bezout theorem in the plane. Recall that I is the ideal generated by P and $R = \mathbb{F}[x,y]/I$. A key observation was the formula for the dimension of R_d:

$$dim R_d = Dd + (3/2D - D^2), \text{ for } d \geq D.$$

In general, for any ideal I in $\mathbb{F}[x_1, ..., x_n]$, we can define $R = \mathbb{F}[x_1, ..., x_n]/I$ and $R_d = V_d/I_d$, and we can study the dimension of R_d. Another basic example is given by the ideal $I = 0$. In this case, $R = \mathbb{F}[x_1, ..., x_n]$, and so we have seen that

$$dim R_d = \binom{d+n}{n} = (1/n!)d^n + \text{ lower order terms.}$$

In general, the dimension of R_d is always given by a polynomial, called the Hilbert polynomial, for all d sufficiently large.

$$dim R_d = h_I(d) = \sum_{j=0}^{m} a_j d^j, \text{ for } d \geq d_0.$$

The leading term of the Hilbert polynomial, $a_m d^m$ is particularly interesting. In the first example above, the leading term was Dd. In the second example, the leading term was $(1/n!)d^n$. In general, m will be the dimension of $Z(I)$ and $m! a_m$ will be the degree of $Z(I)$. (We have not defined dimension and degree anywhere else. These can be taken as definitions, and they are equivalent to other definitions in algebraic geometry...)

In the polynomial method, it was very important to observe that in n dimensions, the space of polynomials of degree $\leq d$ has dimension growing like d^n. In the Hilbert polynomial perspective, this feature can be taken as the definition of the dimension of a variety $Z(I)$.

4. The Bezout theorem in higher dimensions

The Bezout theorem can be generalized to higher dimensions. The full statement gets harder to prove. In our applications, we will need the following minor generalization. Let $\mathbb{F}$ be an infinite field.

Theorem 4.1. *If $P, Q \in \mathbb{F}[x,y,z]$ have no common factor (of degree ≥ 1), then the number of lines in $Z(P,Q)$ is $\leq (degP)(degQ)$.*

Proof. We define $\bar{I}$ to be the ideal generated by P and Q, and we define S to be the ring $\mathbb{F}[x,y,z]/\bar{I}$. If the ring S contains many lines, then it must be large in some sense. But if the degrees of P and Q are small, then S must be small in some sense. Let us make this precise. Let $V_d \subset \mathbb{F}[x,y,z]$ be the polynomials of degree $\leq d$. Let

$\bar{I}_d = \bar{I} \cap V_d$, and $S_d = V_d/\bar{I}_d$. On the one hand, we will bound the dimension of S_d from above using the degrees of P and Q:

$$dim S_d \leq (degP)(degQ)d + c(P,Q).$$

On the other hand, if $Z(P,Q)$ contains L lines, then we will bound the dimension of S_d from below as follows:

$$dim S_d \geq Ld - c(L).$$

Given these two bounds, taking $d \to \infty$, we see that $L \leq (degP)(degQ)$.

Now we turn to the upper bounds on S_d.

We closely follow the argument in the planar case. Let $D = degP$ and $E = degQ$. I is the ideal generated by P, and R is $\mathbb{F}[x,y,z]/I$. J is the ideal of R generated by Q. $S = R/J$.

The dimension of I_d is equal to $dim V_{d-D} = \binom{d-D+3}{3}$ for $d \geq D$.

The dimension of R_d is $dim V_d - dim I_d = \binom{d+3}{3} - \binom{d-D+3}{3} = (1/2)Dd^2 +$ lower order terms.

The dimension of J_d is $\geq dim R_{d-E} = (1/2)D(d-E)^2 +$ lower order terms.

The dimension of S_d is $dim R_d - dim J_d \leq dim R_d - dim R_{d-E} = DEd +$ lower order terms.

In other words, $dim S_d = DEd + c$, where c is a constant that depends on P, Q but not on d.

Now we turn to the lower bounds on the size of S_d related to the lines in $Z(P,Q)$.

For any set $X \subset \mathbb{F}^3$, let E_X be the restriction map from V_d to $Fcn(X, \mathbb{F})$.

Lemma 4.2. *If X is a union of L lines in $\mathbb{F}^n$, then the rank of $E_X : V_d \to Fcn(X, \mathbb{F})$ is $\geq Ld - c(L)$. (Recall that $\mathbb{F}$ is an infinite field.)*

We will come back to the proof of this lemma. For now, we use this lemma. If $X \subset Z(P,Q)$, then $\bar{I}$ is in the kernel of E_X, and so E_X is a map from S_d to $Fcn(X, \mathbb{F})$. In particular, the dimension of S_d is at least the rank of the map $E_X : V_d \to Fcn(X, \mathbb{F})$. If $Z(P,Q)$ contains L lines, then Lemma 4.2 implies that the dimension of S_d is at least $Ld - c(L)$.

Now we turn to the proof of Lemma 4.2

Proof. Fix d. After a linear change of variables, we can assume that each line is transverse to planes of the form $x_n = h$. Choose $d - L$ values $h_1, ..., h_{d-L}$ so that each plane $x_n = h_j$ intersects the L lines in L distinct points. Let $X_0 \subset X$ be these $L(d-L)$ points.

We claim that for any function $f : X_0 \to \mathbb{F}$, there is a degree d polynomial that agrees with f on X_0. This will imply that $rank E_X : V_d \to Fcn(X, \mathbb{F})$ is at least $|X_0| = Ld - L^2$.

Fix a value h_j. The set X_0 intersects the plane $x_n = h_j$ at L points, $(y_{1,j}, h_j), ..., (y_{L,j}, h_j)$ with $y_{k,j} \in \mathbb{F}^{n-1}$. By Lemma 1.5, we can find a degree L polynomial P_j in $n-1$ variables so that $P_j(y_{k,j}) = f(y_{k,j})$ for each $y_{k,j}$.

Now we want to find a polynomial P in n variables with degree $\leq d$ so that $P(y, h_j) = P_j(y)$ for all y and all j from 1 to $d - L$. Let's expand out P_j and P:

$$P_j(y) = \sum_I c_I(j) y^I, \text{ where } I \text{ is an exponent in (n-1) variables of degree at most } L.$$

Now we will choose P to have the following form:

$$P(y, x_n) = \sum_I P_I(x_n) y^I, \text{ where } |I| \leq L \text{ and } degP_I \leq d - L.$$

It suffices to choose P_I so that $P_I(h_j) = c_I(j)$ for each $j = 1, ..., d - L$. We can do this by applying Lemma 1.5 again. □

This finishes the proof of Theorem 4.1. □

Exercise: Figure out what happens in finite fields. Check that the result is still true if $degP, degQ < |\mathbb{F}|$ or if the theorem is phrased carefully.

Finally, we discuss/explore what might be true more generally in higher dimensions. Suppose that we have some ideals I_j in $\mathbb{F}[x_1, ..., x_n]$. Suppose that I_j has dimension m_j and degree D_j. In other words, if $R_{j,d} = V_d / I_{j,d}$, then

$$dim R_{j,d} = D_j (m_j!)^{-1} d^{m_j} + \text{ lower order terms, for all } d \text{ sufficiently large.}$$

Let I be the ideal generated by I_j. Suppose that it has dimension m and degree D. Now we may pose the following question:

Question 1. *If* $(n - m) = \sum_j (n - m_j)$, *then is* $D \leq \prod_j D_j$*?*

The condition on the dimensions is similar to asking that P and Q have no common factor in the planar version of Bezout.

It would be cool to know whether this is true, and also to see if there is a proof in the spirit of the arguments above.

18.S997 The Polynomial Method
Fall 2012