18.704: Projective Space

David Glasser

2/18/2005

1 Projective Space

Projective n-space over the field F, or $\mathbb{P}^n(F)$ for short, is defined to be the set of lines through the origin in F^{n+1} (a more technical definition is below). Why $n+1$ and not n? Let's look at a simple example: $\mathbb{P}^1(\mathbb{R})$, which is often referred to as $\mathbb{R}P^1$. This is the space of all lines through the origin in the plane. Now, if we draw the vertical line at $x = 1$, we see that just about every line through the origin intersects this line in exactly one point, and in fact we can (almost!) make a bijection between points on this 1-dimensional line and "points" (which look like lines) in $\mathbb{P}^1(\mathbb{R})$. In fact, the point $(1, m)$ corresponds to the line $y = mx$. Since the line $x = 1$ is clearly 1-dimensional, and we have this very natural map between the set of lines through the origin of $\mathbb{R}^2$ and that line, it makes sense to consider this set of lines to be 1-dimensional, so we call it $\mathbb{P}^1(\mathbb{R})$. I said "almost" above, because the vertical line through the origin ($x = 0$) doesn't intersect the line $x = 1$ at all. But just have a single extra point doesn't really seem like it'll change the "dimension" of the space (and yes, this seems like a bad proof, but that's because it isn't a proof, it's just a justification for a definition). This line contains all points of the form $(0, a)$. Thus, we see that every line through the origin (ie, every element of $\mathbb{P}^1(\mathbb{R})$) contains exactly one point of the form $(1, m)$ or $(0, 1)$.

Similarly, if we look at $\mathbb{P}^2(\mathbb{R})$, we want to consider all of the lines through the origin in $\mathbb{R}^3$. Most of these contain exactly one point of the plane $x = 1$. The only ones that don't lie entirely in the plane $x = 0$. But then most of them contain exactly one point in the plane $y = 1$. The only line that is the single line defined by has $x = 0$ and $y = 0$ everywhere. So we see that every element of $\mathbb{P}^2(\mathbb{R})$ has exactly one point of the form $(1, a, b)$ or $(0, 1, c)$ or $(0, 0, 1)$.

The neat thing to notice here is that in this example, we started by looking at the lines that intersect the right-hand plane $x = 1$; these correspond to points of the form $(1, a, b)$ for all real numbers a and b, so it's essentially a copy of the plane $\mathbb{R}^2$. And what do the "weird" lines that don't intersect that plane look like? Well, they're all the lines through the origin that lie in the plane $x = 0$. But if you just pretend that the plane $x = 0$ is the entirety of known space, all we're talking about is the set of lines through the origin in $\mathbb{R}^2$, which is to say $\mathbb{P}^1(\mathbb{R})$! That is to say, the interesting intersection points we've noted above in $\mathbb{P}^n(\mathbb{R})$ consist of a copy of $\mathbb{R}^n$ with "1" glued onto the front, and a copy of $\mathbb{P}^{n-1}(\mathbb{R})$ with "0" glued onto the front.

2 How It's Actually Defined

The definition of n-dimensional projective space over an arbitrary field F is still just "the set of $n+1$-dimensional lines through the origin", but what does that mean? Well, consider a point $(f_0, f_1, \dots, f_n)$ in $n+1$-dimensional F-space (so each $f_i \in F$). The points on the same line through the origin are just $(af_0, af_1, \dots, af_n)$ for each $a \in F$. So we can define the points of $\mathbb{P}^n(F)$ to be the equivalence classes of vectors $(f_0, f_1, \dots, f_n)$, where two vectors g and h are considered to be equivalent if there is a scalar $a \in F$ such that $g = ah$. We require both that the point is not the origin $(0, 0, \dots, 0)$, and that the scalar $a \neq 0$; otherwise the origin would end up on all of the lines, and we wouldn't have an equivalence relation. For example, back in $\mathbb{P}^1(\mathbb{R})$, we have that $(1, 2)$ and $(3, 6)$ are equivalent and thus fall in the same "point" of $\mathbb{P}^1(\mathbb{R})$, but $(1, 2)$ and $(2, 7)$ are on different "points".

As it turns out, our decomposition argument still holds! That is, if there's *any* point $(f_0, f_1, \dots, f_n)$ in a line through the origin with $f_0 \neq 0$, then since F is a field we can see that $f_0^{-1}(f_0, f_1, \dots, f_n) = (1, f_0^{-1}f_1, \dots, f_0^{-1}f_n)$ is the *unique* point on the line that it determines with 1 for its first coordinate. And on the other hand, if 0 is the first coordinate for any point on a line (except for the origin itself), then 0 is the first coordinate for *every* point on that line. The lines satisfying this property are the lines through the origin in the n-dimensional subspace defined by $f_0 = 0$, so it's basically just a copy of $\mathbb{P}^{n-1}(F)$ with a zero glued onto the front of every point.

So every line in F^{n+1} (ie, every point of $\mathbb{P}^n(F)$) passes through exactly one point of the form

$$(1, f_1, f_2, \dots, f_n)$$

or

$$(0, 1, f_2, \dots, f_n)$$

or

$$(0, 0, 1, \dots, f_n)$$

or ... or ...

$$(0, 0, 0, \dots, 1)$$

We can use this to count the number of element of $\mathbb{P}^n(F)$ where F is the finite field with q elements (this argument works whether this q is prime and it's one of the nice fields $\mathbb{Z}/p\mathbb{Z}$ or whether q is a prime power and it's one of the weirder finite fields). There are q^n elements of the first type here, since each f_i can be any of q elements. The rest of the elements correspond to elements of $\mathbb{P}^{n-1}(F)$. So we've shown that $|\mathbb{P}^n(\mathbb{F}_q)| = q^n + \left|\mathbb{P}^{n-1}(\mathbb{F}_q)\right|$. As a base case, $\left|\mathbb{P}^0(F)\right| = 1$ for any field: this is essentially the scalars modulo the scalars, or the set of lines in a line, and so there is only one. Unrolling the last formula, we get $|\mathbb{P}^n(\mathbb{F}_q)| = q^n + q^{n-1} + \cdots + q^0$; this formula is equal to $\frac{q^{n+1}-1}{q-1}$ as long as $q \neq 1$, which it will be because there are no one-element fields. So this is the number of points in $\mathbb{P}^n(F_q)$. (Note that if you had insisted on plugging in 1 for q before making the last transformation, you would have gotten $n+1$; this means that this formula gives us what is called a "q-analog" for $n+1$.)