A Short Introduction to Projective Geometry

Vector Spaces over Finite Fields

We are interested only in vector spaces of finite dimension. To avoid a notational difficulty that will become apparent later, we will use the word ***rank*** (or *algebraic* dimension) for the dimension (number of vectors in any basis) of the vector space.

Theorem: *A rank n vector space over GF(q) has* q^n *vectors.*

Recall the important rank formula for subspaces U and W of the vector space V:

$$\textbf{rank}(\langle U,W\rangle) = \textbf{rank}(U) + \textbf{rank}(W) - \textbf{rank}(U\cap W)$$

Vector Spaces

Let V = V(n,q) denote a rank n vector space over GF(q). A rank 1 subspace of V consists of all the scalar multiples of a given vector, thus there are q vectors in such a subspace (including the zero vector). By the rank formula, the join of any two distinct rank 1 subspaces has rank 2, since they can only intersect in the zero vector which as a subspace has rank 0. If we examine two distinct rank 2 subspaces, U and W, we notice that there are several possibilities for the rank of their join. If n = 3 then rank(<U,W>) = 3 and the rank formula says that they must intersect in a rank 1 subspace. If n > 3, then there are two possibilities, either the join has rank 4 (when their intersection is just the zero vector) or rank 3 (if they intersect in a rank 1 subspace.)

Theorem: *The vector space V(n+1,q) has* $(q^{n+1}-1)/(q-1) = q^n + q^{n-1} + \ldots + q + 1$ *rank 1 subspaces.*

Projective Geometries

A ***projective geometry*** is a geometric structure consisting of various types of objects (points, lines, planes, etc.) and the relations between them which satisfies a set of axioms. Here, we will not develop the subject axiomatically (as is done in M6221) but will settle for an algebraic construction starting with a vector space which will give a structure that satisfies the (unstated) axioms. We will start with the vector space V(n+1,q) and construct the geometric structure ***PG(n,q)*** called the ***projective geometry of dimension n over GF(q)***.

Projective Geometry

The word "dimension" is used here in the classical geometric sense in which lines have 1 dimension, planes have 2 dimensions, etc. This use of the term is different from (but related to) the algebraic dimension of vector spaces (rank). Since in this treatment both geometries and vector spaces appear together, it is inevitable that confusion will arise unless one is very careful. We shall always use the term dimension in its geometric sense, sometimes using ***projective*** dimension (or ***geometric*** dimension) for additional emphasis.

Definition

Given the vector space V(n+1,q), we define ***PG(n,q)*** as follows:

The objects of PG(n,q) consist of:

points, which are the rank 1 subspaces of V(n+1,q).

lines, which are the rank 2 subspaces of V(n+1,q).

planes, which are the rank 3 subspaces of V(n+1,q).

...

i-spaces, which are the rank i+1 subspaces of V(n+1,q).

...

hyperplanes, which are the rank n subspaces of V(n+1,q).

Incidence

The relationship between the objects of PG(n,q) is called ***incidence*** and is defined by containment of the corresponding subspaces. The incidence relation is meant to be symmetric, so we say that a point is incident with a line (the point is on the line) or that a line is incident with a point (the line passes through the point) if the rank 1 subspace is contained in the rank 2 subspace.

In geometric notation, to denote that a point P is incident with a line ℓ, we would write P I ℓ or ℓ I P.

Projective Geometry

We can now rephrase statements about vector spaces in terms of the geometric objects of the projective geometry. For instance, the statement made earlier about two distinct rank 1 subspaces becomes *two distinct points determine a unique line*. The statements about rank 2 subspaces become, in PG(2,q) *every two distinct lines meet at a unique point*, while in higher dimensional projective spaces two distinct lines which meet, *lie in a unique plane* and if they do not meet (are ***skew***), *lie in a unique 3-space* (***solid***).

Example

Let our field be GF(4) whose elements are 0, 1, a and a^2. Recall that this is a field of characteristic 2, so 1 + 1 = 0 and that $a^2 = a + 1 = 1/a$. With respect to the standard basis, the vectors of V (3,4) (4^3= 64 in total) are represented by 3-tuples over GF(4), such as: (0,1,0), (a,0,0), (a,a^2,1), and (a^2, 1, a). Now, a rank 1 subspace of this vector space containing a non-zero vector consists of the zero vector and three non-zero vectors. For instance, $<(a,a^2,1)> = \{(0,0,0), (a,a^2,1), (a^2,1,a), (1,a,a^2)\}$. A rank 2 subspace consists of all linear combinations of two vectors which are not in the same rank 1 subspace (i.e., are linearly independent). Thus, there will be 16 vectors in a rank 2 subspace, the zero vector and 15 non-zero vectors. If a vector is in this subspace, then all of its scalar multiples are as well, so the 15 non-zero vectors are divided up into 5 sets of size 3, and there are 5 rank 1 subspaces contained in a rank 2 subspace.

Example Continued

For instance, the rank 2 subspace containing (0,1,0) and (a,0,0) consists of the vectors A(0,1,0) + B(a,0,0) = (Ba,A,0) as A and B run through GF(4). We get the following vectors:

(0,0,0)
(a,0,0), $(a^2,0,0)$, (1,0,0)
(0,1,0), (a,1,0), $(a^2,1,0)$, (1,1,0)
(0,a,0), (a,a,0), $(a^2,a,0)$,(1,a, 0)
$(0,a^2,0)$, $(a,a^2,0)$, $(a^2,a^2,0)$, $(1,a^2,0)$

And when we reorganize this list by grouping the scalar multiples together we get:

$(0,0,0), <(1,0,0)>, <(0,1,0)>, <(1,1,0)>, <(1,a,0)>, <(1,a^2,0)>$

PG(2,4)

The projective geometry PG(2,4) then consists of 21 points (rank 1 subspaces) and 21 lines (rank 2 subspaces). Each line contains 5 points and each point is contained in 5 lines. All the points and lines are contained in 1 plane, so we call this geometry a ***projective plane of order 4***. Note that in this case the hyperplanes of the geometry are lines.

PG(2,q)

The same arguments can be generalized to different fields, so we get the following counts:

1) The number of points of PG(2,q) is $q^2 + q + 1$.
2) The number of lines of PG(2,q) is $q^2 + q + 1$.
3) The number of points on a line in PG(2,q) is $q + 1$.
4) The number of lines through a point in PG(2,q) is $q + 1$.

Furthermore, every two distinct points determine a unique line and every two distinct lines meet at a common point.

Coordinates

It is easily seen from this construction that the points of the geometry have a natural relation to coordinates, namely we can take as coordinates of a point any non-zero vector written as an (n+1)-tuple in the rank 1 subspace corresponding to that point. If we do this, then unlike the situation in Euclidean geometry, one point has several possible coordinates, but they are all related by being scalar multiples of each other. Such coordinates are called ***projective*** (or ***homogeneous***) coordinates. It is often convenient to select a standard representative from the set of equivalent coordinates for a point. Two common conventions are to select the coordinate whose last non-zero entry is a 1, and to select the coordinate whose first non-zero entry is a 1. It is always to be remembered that no matter what convention is used, the coordinates can at any time be replaced by any non-zero scalar multiple.

Hyperplanes

In terms of these point coordinates, it is easy to describe the set of points on a hyperplane by means of a linear equation.

A hyperplane is a rank n subspace of V(n+1,q), and so, its orthogonal complement is a rank 1 subspace. Thus the (standard) dot product of any vector in the hyperplane with any vector in this rank 1 subspace must be 0. So, if $(a_0, a_1, ..., a_n)$ is a fixed non-zero vector, and $(x_0, x_1, ..., x_n)$ represents a variable non-zero vector of V (n+1,q), then the solutions of:

$$a_0x_0 + a_1x_1 + ... + a_nx_n = 0$$

are the vectors in the hyperplane which is the orthogonal complement of the fixed vector.

Example

In the PG(2,4) example above we calculated the vectors in a rank 2 subspace. Since a rank 2 subspace is a hyperplane, we can describe these vectors in an alternate way. Consider the vector (0,0,1). The vectors in the orthogonal complement of the subspace containing this vector must satisfy the equation $(0,0,1)\bullet(x_0,x_1,x_2) = 0$, i.e. the linear equation $x_2 = 0$. Notice that this is the set of vectors given in the example:

$$<(1,0,0)>, <(0,1,0)>, <(1,1,0)>, <(1,a,0)>, <(1,a^2,0)>$$

Ovals

In a projective plane, PG(2,q) a set of q+1 points with no three on the same line is called an ***oval***. Clearly, a line can intersect an oval in only 0, 1 or 2 points. A line intersection an oval in 2 points is called a ***secant line*** to the oval, in 1 point a ***tangent line*** to the oval and in 0 points, an ***exterior line*** of the oval. Consider a point P on the oval Ω. As there are q+1 lines that pass through P, and q of these are secants determined by the other points of Ω, there is exactly one line through P which is a tangent line.

Thus, in PG(2,q), with respect to an oval Ω there are:

$q+1$ tangent lines;

$\frac{1}{2}(q)(q+1)$ secant lines, and

$\frac{1}{2}(q)(q-1)$ exterior lines.

Conics

To get a specific example of an oval we will look at some sets of points determined by algebraic equations involving the coordinates. A ***plane quadric*** in PG(2,q) is the set of points defined in terms of their coordinates by

$$\{(x,y,z) \mid Ax^2 + Bxy + Cy^2 + Dxz + Eyz + Fz^2 = 0\},$$

where the coefficients of the quadratic equation come from GF(q). Because the equation is homogeneous, any scalar multiple of a solution is also a solution, so this really does define points of PG (2,q). The plane quadrics which correspond to non-degenerate quadratic equations all contain exactly q+1 points and are called ***conics***. Since a linear equation can have no more than two common solutions with a non-degenerate quadratic equation, no line intersects a conic in more than 2 points ... Conics are therefore ovals.

Conics

Beniamino Segre (1957) has shown that if the characteristic of the field is odd, then all ovals of PG(2,q) are conics, but *in even characteristic there are ovals which are not conics*. The even characteristic case is different in another way as well. For any oval in a projective plane over a field of even characteristic, it can be shown that all of the tangent lines to the oval meet at a single point, called the ***knot*** of the oval (in odd characteristic, through a point not on the oval (conic) there pass either 0 or 2 tangent lines). The knot of a conic is called the ***nucleus*** of the conic.[Most authors use the words knot and nucleus interchangeably, but I prefer to maintain this distinction.] If the knot of an oval is added to the oval, the larger set is called a ***hyperoval*** and it still has the property that no three of its points lie on the same line. If the oval is a conic, the corresponding hyperoval is called a ***hyperconic*** (other terms in the literature for this are *regular hyperoval*, and *complete conic*).

Knots

Consider an oval Ω in PG(2,q), q even. Let ℓ be a secant line and P a point of ℓ not on Ω. There are q – 1 points of Ω not on ℓ. Each secant line through P contains 2 oval points, and since q-1 is odd, there must be an odd number of tangent lines through P. So, there is at least one tangent line through every point P on ℓ (including the two oval points on ℓ). Since there are q+1 tangent lines and q+1 points on ℓ, through each point of the secant ℓ there passes exactly one tangent line.

Now, in a projective plane, every two lines meet. In particular, any two tangent lines must meet. Say that two tangent lines meet at a point K. By the above argument, no secant lines can pass through K, so all the lines joining K to points of Ω must be tangent lines. Since K is joined to each point of Ω, all of the q+1 lines through K are all of the tangent lines. K is thus the knot of Ω.

Example

Consider PG(2,4) and the conic Ω given by $x^2 + yz = 0$.

The points of Ω are: (0,1,0), (0,0,1), (1,1,1), $(a,a^2,1)$ and $(a^2,a,1)$.

The 10 secant lines of Ω are:
$x = 0$, $x + z = 0$, $x + az = 0$, $x + a^2z = 0$, $x + y = 0$, $ax + y = 0$, $a^2x + y = 0$, $a^2x + y + az = 0$, $ax + y + a^2z = 0$, $x + y + z = 0$.

The 5 tangent lines are:
$z = 0$, $y = 0$, $y + z = 0$, $y + a^2z = 0$ and $y + az = 0$.

All the tangent lines pass through the point (1,0,0) which is therefore the nucleus of Ω.