Projective Planes

Jonathan Ma
johnma@udel.edu

January 20, 2026

Preface

Ahead are some notes on *An Introduction to Finite Geometry*, by Simeon Ball and Zsuzsa Weiner, as well as *Combinatorial Designs: Constructions and Analysis,* by Douglas Stinson. I am mainly concerned with projective and affine planes, and their connections with Latin squares. I've added some notes too from MATH888, Combinatorics II at UD.

1 Projective Geometry

1.1 Finite Fields

Definition 1.1. A field is a set K with two operations, usually called addition and multiplication, with the property that K is an additive group with identity 0, and $K \setminus \{0\}$ is a multiplicative group.

Theorem 1.2 (Galois)**.** *A finite field has q elements, where q is the power of a prime. The field of order q is unique.*

One proof of this was presented to me using linear algebra. The standard proof of this uses the machinery of algebra. I will denote the finite field of order q by $\mathbb{F}_q$. The following facts are useful for our discussion.

1. For all $x \in \mathbb{F}_q$, $x^q = x$.
2. Let p be prime. Then $\mathbb{F}_p$ is the set $\mathbb{Z}/p\mathbb{Z}$, where addition and multiplication is defined modulo p.
3. The finite field $\mathbb{F}_{p^h}$ can be constructed in the following way. Let $f \in \mathbb{F}_p[x]$ be a polynomial of degree h, irreducible over $\mathbb{F}_p$. The quotient ring $\mathbb{F}_p[x]/f(x)$ has p^h elements, and with the multiplication and addition as in this quotient ring, it is the field $\mathbb{F}_{p^h}$.
4. The prime p is called the characteristic of the field.
5. An element ϵ is called primitive if $\{\epsilon^i \mid i = 0, 1, \ldots, q-2\} = \mathbb{F}_q \setminus \{0\}$. The multiplicative group $\mathbb{F}_q \setminus \{0\}$ is usually denoted $\mathbb{F}_q^*$, and is cyclic.
6. The field $\mathbb{F}_{p^r}$ is a subfield of $\mathbb{F}_{p^h}$ iff $r \mid h$.
7. The field $\mathbb{F}_{p^h}$ is a vector space of rank h over $\mathbb{F}_p$.

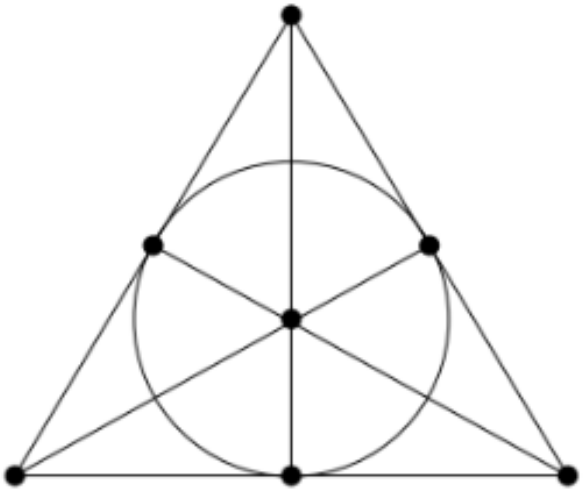

Figure 1: $PG(2,2)$, the Fano plane.

1.2 Projective Spaces

Suppose $V(n+1,q)$ is a vector space of dimension[1] $n+1$ over $\mathbb{F}_q$. The projective space $PG(n,q)$ is the geometry whose points, lines, planes, ..., hyperplanes are the subspaces of $V(n+1,q)$ of dimension $1,2,3,\ldots,n$. The dimension of $PG(n,q)$ is one less than the rank of a subspace of $V(n+1,q)$. (Geometrically, the projective space of $V(n+1,q)$ is derived by considering the equivalence classes of non-zero vectors of $V(n+1,q)$ under scalar multiplication. So each point in $PG(n,q)$ corresponds to a 1-dimensional subspace in $V(n+1,q)$.)
The incidence structure in Fig. 1 is what we get when we set $n=q=2$. It has a group of 168 automorphisms, (we're assuming this means that the group of automorphisms defined on the set of points of the Fano plane has size 168), isomorphic to the 3×3 non-singular matrices whose elements come from $\mathbb{F}_2$.
As in linear algebra, we write $\langle x,y,z\rangle$ to be the space spanned by x,y,z. We define co-dimension of a subspace as the dimension of the ambient space minus the dimension of the subspace. A hyperplane is a subspace of co-dimension 1. The following is stated by the authors, but not proven, so I will attempt to justify this.

Proposition 1.3. *If H is a hyperplane, and l is a line not contained in H, then $H\cap l$ is a point.*

Proof. Consider the sum $H+l$. Then

$$\dim(H+l)=\dim(H)+\dim(l)-\dim(H\cap l).$$

Since $H+l$ is the smallest subspace of $PG(n,q)$ containing both H,l, and l is not contained in H, $H+l$ must be $PG(n,q)$, since $\dim(H+l)>\dim(H)$, and $\dim(H)=n-1$. Thus,

$$\begin{aligned} n &= n-1+2-\dim(H\cap l)\\ \implies \dim(H\cap l) &= 1. \end{aligned}$$

Hence, $H\cap l$ is a point.

□

[1]The authors use rank and dimension interchangeably.

The geometry $PG(2,q)$ has the property that every two lines are incident in a unique point. The rank of the vector space $V(3,q)$ is 3, and the lines U, V are subspaces of rank 2. Hence, the rank of $U \cap V$ is 1, so $U \cap V$ is a point.

Proposition 1.4. *The number of subspaces of rank k in $V(n,q)$ is*

$$\begin{bmatrix} n \\ k \end{bmatrix}_q := \frac{(q^n-1)(q^n-q)\cdots(q^n-q^{k-1})}{(q^k-1)(q^k-q)\cdots(q^k-q^{k-1})}.$$

Proof. The number of k-tuples of linearly independent vectors in a vector space of rank n is

$$(q^n-1)(q^n-q)\cdots(q^n-q^{k-1}).$$

(The authors assume this is standard. But for those who haven't seen this combinatorial argument before, the proof goes like this. Choose the first vector in a linearly independent list of k vectors. There are (q^n-1) choices, since there are q^n vectors in $V(n,q)$, and a linearly independent list of vectors cannot include the zero vector. For the second vector, there are q vectors spanned by our first choice of vector, so there are (q^n-q) vectors to choose from. For the third vector, we cannot choose a vector which is a linear combination of the first and second vector. The span of our first and second vectors has dimension q^2. From here, the argument should be clear.)
The number of subspaces of rank k is the number of k-tuples of linearly independent vectors in $V(n,q)$ divided by the number of k-tuples of linearly independent vectors in $V(k,q)$, since subspaces of rank k of $V(n,q)$ are isomorphic to $V(k,q)$. □

Theorem 1.5. *The number of subspaces of rank k through a given subspace of rank $d \leq k$ in $V(n,q)$ is* $\begin{bmatrix} n-d \\ k-d \end{bmatrix}_d$.

Here, a subspace W is said to go through another subspace U if $U \subset W$.

Proof. This is an application of the linear algebraic correspondence theorem (from group theory, regarding cosets and quotient groups)[2]. Let U be a subspace of $V(n,q)$ with dimension d. Since each subspace T of $V(n,q)$ of dimension k such that $U \leq T \leq V$ corresponds to a subspace of V/U with dimension $k-d$, we can just count the number of subspaces of V/U with dimension $k-d$. Note that the dimension of V/U is $n-d$. □

2 Desargues' Theorem

We say that two lines are concurrent if they intersect at a single point. We say that the triangles ABC, $A'B'C'$ of $PG(n,q)$ are *in perspective* if the lines AA', BB', and CC' are concurrent. Some texts call this point of intersection the perspector. A set of points is said to be collinear if they lie on the same line.

Theorem 2.1. *Assume that in $PG(n,q)$, ABC, and $A'B'C'$ are two triangles in perspective. Let AB be the intersection point of the lines $\langle A,B\rangle$ and $\langle A',B'\rangle$, and define the points AC, BC similarly (see Figure 2). Then the points AB, AC, and BC are colinear.*

Proof. I'll only present the non planar case. The planar case is longer, and I don't have time to dive into it. In Figure 2, AA', BB', CC' intersect in the point O, which we say $ABC, A'B'C'$ is in perspective of. The points AB, AC, BC[3] lie in the planes $\langle A,B,C\rangle$, and $\langle A',B',C'\rangle$. If all of Figure 2 is not contained in a plane, then $\langle A,B,C\rangle, \langle A',B',C'\rangle$ are distinct planes both contained in some 3-space $\langle O,A,B,C\rangle$, so their intersection is a line containing AB, AC, BC. □

[2] https://math.stackexchange.com/questions/3187795/correspondence-theorem-in-linear-algebra.
[3] Seems to be a typo in the original text, where AB is repeated twice in place of BC.

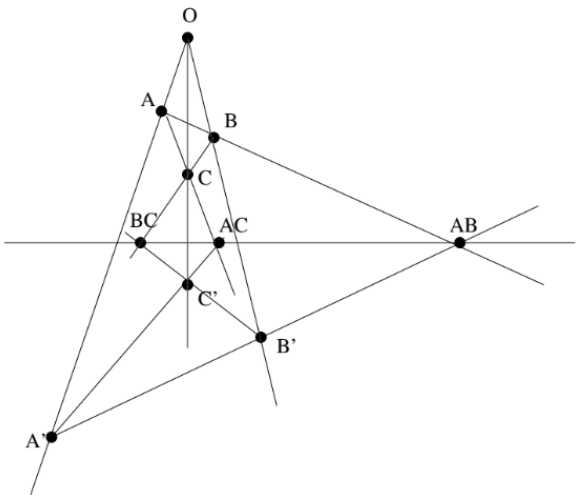

Figure 2: Desargues' configuration.

3 Projective Planes

Projective planes are an incidence structure which mimics the nice properties that $PG(2, q)$ have. They are a common occurrence in the study of incidence structures. Later, we'll talk about connections between projective planes (and affine planes) with regular, strongly regular, and distance regular graphs.

Definition 3.1. A projective plane is an incidence structure of points and lines with the following properties.

(PP1) Every two points are incident with a unique line.

(PP2) Every two lines are incident with a unique point.

(PP3) There are four points, no three collinear.

The axioms (PP1)-(PP3) are self-dual. Hence the dual of a projective plane is also a projective plane. So if we prove a theorem for points in a projective plane, then the dual result holds automatically for lines. The dual P^* of a projective plane P is the plane where the lines of P become the new points in P^*, and the points of P become the new lines. The incidence relation remains the same: a line containing a point in P corresponds to a point lying on a line in P^*.
The geometry $PG(2, q)$ is an incidence structure satisfying these properties. It is called the Desarguesian projective plane because of the following theorem.

Theorem 3.2. *If π is a projective plane with the property that for every pair of triangles ABC, and $A'B'C'$ in perspective, the points AB, AC, and BC, defined in Figure 2 are colinear, then π is $PG(2, q)$, for some q.*

Definition 3.3. The order n of a projective plane is one less than the number of points incident with a line.

To justify that this order makes sense, the following must be proven.

Proposition 3.4. *Every point in a projective plane is incident with a constant $n + 1$ lines. Dually, every line is incident with $n + 1$ points.*

Proof. Choose a line l. By (PP3), there is some point P not incident with l. (Otherwise, every point is on l, violating (PP3).) By (PP1), and (PP2), the number of points incident with l is equal to the number of lines incident with P. Using (PP3) again, we can find some point Q, $Q \neq P$, such that Q is not on l. (Otherwise, every point but P is on l, but this violates (PP3).) The number of lines incident with Q is equal to the number of points incident with l, which is equal to the number of lines incident with P. The points P, Q were chosen arbitrarily, so every point is incident with a constant number of lines. □

Proposition 3.5. *A projective plane of order n has $n^2 + n + 1$ points and $n^2 + n + 1$ lines.*

Proof. Let P be a point of a projective plane. There are $n + 1$ lines incident with P, and each is incident with n other points. Hence, by (PP1), the number of points in a projective plane of order n is $n(n+1)+1$. The number of lines follows from the dual argument. □

A projective line over $\mathbb{F}_q$ has $\begin{bmatrix} 2 \\ 1 \end{bmatrix}_q = (q^2-1)/(q-1) = q+1$. Hence, the projective plane $PG(2, q)$ has order q. Thus, there are examples of projective planes of order n, for every prime n. There are many projective planes known that are not isomorphic to $PG(2, q)$, but all known examples end up having prime power order. This brings us to the first, and probably most famous conjecture in finite geometry.

Conjecture 1. The order of a projective plane is the power of a prime.

Finally, we note that similarly to defining projective planes, one could define projective higher dimensional spaces, mimicking $PG(n, q)$, but it turns out that such projective spaces are isomorphic to $PG(n, q)$, for some n.

3.1 Bruck-Ryser-Chowla Theorem

Here is a useful theorem.

Theorem 3.6. *If there is a projective plane of order n, and $n \equiv 1$, or $2 \bmod 4$, then n is the sum of two squares.*

We will use this later in our discussion of mutually orthogonal latin squares. The numbers 1, and $2 \bmod 4$ are $1, 2, 5, 6, 9, 10, 13, 14, \ldots$. Now, $2 = 1^2 + 1^2$, $5 = 1^2 + 2^2$,, $9 = 0^2 + 3^2, 13 = 2^2 + 3^2$. There exist projective planes of of these orders. However, the theorem implies that there is no projective plane of order 6, nor 14. Euler also proves this non-existence of projective planes of order 6 by showing that there are no two mutually orthogonal latins quares of order 6. Lam, Thiel, and Swiercz concluded, with the aid of a computer, that there is no projective plane of order 10[4]. Therefore, the smallest possible counter-example to the aforementioned conjecture is a projective plane of order 12. Here are useful lemmas from number theory that we will use to prove our theorem.

Lemma 3.7. *We have the following identities:*

$$(a_1^2 + a_2^2)(x_1^2 + x_2^2) = (a_1x_1 - a_2x_2)^2 + (a_1x_2 + a_2x_1)^2,$$

where

$$(a_1^2 + a_2^2 + a_3^2 + a_4^2)(x_1^2 + x_2^2 + x_3^2 + x_4^2) = y_1^2 + y_2^2 + y_3^2 + y_4^2,$$

[4]C. W. H. Lam, L. H. Thiel and S. Swiercz, The non-existence of finite pro- jective planes of order 10, Canadian J. Math. 41 1117–1123 (1989).

and

$$\begin{aligned} y_1 &= a_1x_2 - a_2x_2 - a_3x_3 - a_4x_4, \\ y_2 &= a_1x_2 + a_2x_1 + a_3x_4 - a_4x_3, \\ y_3 &= a_1x_3 + a_3x_1 + a_4x_2 - a_2x_4, \\ y_4 &= a_1x_4 + a_4x_1 + a_2x_3 - a_3x_2. \end{aligned}$$

Proof. According to the authors, the identities hold by direct calculation. □

Lemma 3.8. *Let p be prime. If there exists two integers such that*

$$x_1^2 + x_2^2 \equiv 0 \bmod p,$$

then p is the sum of two squares.

Lemma 3.9. *Let p be a prime. If there exists four integers such that*

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \bmod p,$$

then p is the sum of four squares.

Lemma 3.10. *Every number is the sum of four squares.*

Lemma 3.11. *If $nx^2 = w^2 + y^2$ has a solution in integers, then n is the sum of two squares.*

Proof. Assume that $n = p_1p_2 \cdots p_t$, where p_i are distinct primes. Then

$$w^2 + y^2 \equiv 0 \bmod p_i,$$

so each p_i is the sum of two squares. But then, n is the sum of two squares. If n does not have such a prime factorization, then $n = m^2r$, where r is the product of distinct primes. Now,

$$r(mx)^2 = w^2 + y^2,$$

and we have just seen that this implies we can write $r = a^2+b^2$ for some a, b. Thus, $n = (ma)^2+(mb)^2$. □

Let us prove our theorem.

Proof of Theorem 3.6. Let $\{P_i \mid i = 1, \ldots, N\}$ be the points of a projective plane of order n, and let $\{l_i \mid i = 1, \ldots, N\}$ be the lines, where $N = n^2 + n + 1$. Let $A = (a_{ij})$ be the matrix defined by

$$a_{ij} = \begin{cases} 1 & P_i \in l_j \\ 0 & P_i \notin l_j. \end{cases}$$

The axioms (PP1), (PP2) imply that $A^TA = J + nI$, where J is the all ones matrix. Let $z = Ax$, where $x = (x_1, x_2, \ldots, x_N)$, and each x_i is indeterminate. Then we have

$$z^Tz = x^TA^TAx = x^TJx = nx^Tx.$$

Thus,

$$z_1^2 + z_2^2 + \ldots + z_N^2 = w^2 + n(x_1^2 + x_2^2 + \ldots + x_N^2),$$

where $w = x_1 + x_2 + \ldots + x_N$. Now, add nx_{N+1}^2 to both sides:

$$z_1^2 + z_2^2 + \ldots + z_N^2 + nx_{N+1}^2 = w^2 + n(x_1^2 + x_2^2 + \ldots + x_N^2 + x_{N+1}^2).$$

Since $n \equiv 1$ or $2 \bmod 4$, $N+1 = 0 \bmod 4$. By Lemma 3.10, n is the sum of four squares, and so by Lemma 3.7, there exists y_j that are linear combinations of the x_i's such that

$$z_1^2 + z_2^2 + \ldots + z_N^2 + nx_{N+1}^2 = w^2 + y_1^2 + y_2^2 + \ldots + y_N^2 + y_{N+1}^2. \tag{3.1}$$

By definition, the z_j's are also linear combinations of the x_i's. At least one of the z_j's, and at least one of the y_j's must be linear combinations of the x_j's that contain x_1 (since $z = Ax$, and there are $n+1$ 1's in the first row of A), so let us assume WLOG that z_1, y_1 do. If we put $z_1 = y_1$, then we can solve for x_1 unless the coefficient of x_1 in y_1 and z_1 is the same. If this is the case, put $z_1 = -y_1$, and solve for x_1. When we substitute this solution into Eq. (3.1), the z_1^2 term will cancel with the y_1^2 term.
We repeat this proecess with x_2, and continue to reduce the number of indeterminates, unless at some stage, we make a substitution of one (or more) of the x_j's. Suppose x_l no longer appears in any of the remaining z_j's or y_j's. Let x_l be one of the four $x_k, x_{k+1}, x_{k+2}, x_{k+3}$, for which by Lemma 3.7, $(y_k, y_{k+1}, y_{k+2}, y_{k+3}) = (x_k, x_{k+1}, x_{k+2}, x_{k+3})B$, for some matrix B determined by n. If, after substituting x_j, for $j < l$ with linear combinations of the x_j's, with $j \geq l$, there are no y_j's in which x_l occurs, then putting all $x_j = 0$, for $j > l$, we have that $(y_k, y_{k+1}, y_{k+2}, y_{k+3}) = 0$, and so B is singular. This is not the case, since its determinant is $(a_1^2 + a_2^2 + a_3^2 + a_4^2)^2 = n^4$. Therefore, we can continue reducing the number of indeterminates in Eq. (3.1) until we have

$$nx_{N+1}^2 = w^2 + y_{N+1}^2,$$

where w, y_{N+1} are rational multiples of x_{N+1}. Choose x_{N+1} so that this equation has integer solutions. Lemma 3.11 implies that n is the sum of two squares.

□

4 Affine Spaces

The affine space $AG(n, q)$ is the geometry whose points, lines, planes, ..., hyperplanes, are the cosets of the space $V(n, q)$ of rank $0, 1, 2, \ldots, n-1$. The dimension of a subspace of $AG(n, q)$ is the dimension of a subspace of $V(n, q)$.

5 Affine Planes

Definition 5.1. An affine plane is an incidence structure of points and lines with the following properties.

(AP1) Every two points are incident with a unique line.

(AP2) Given a point P, and a line l, such that $P \notin l$, there exists a unique line m such that $P \in M$, and $m \cap l = \emptyset$.

(PP3) There are three points that are not collinear.

If m, l are lines of an affine plane such that $m \cap l = \emptyset$, then we say that m and l are parallel. If m, l are parallel, and l and r are parallel, then m and r are parallel. If not, then there is a point $P \in M \cap r$, such that $P \notin l$, which contradicts (AP2). So parallelism is an equivalence relation.

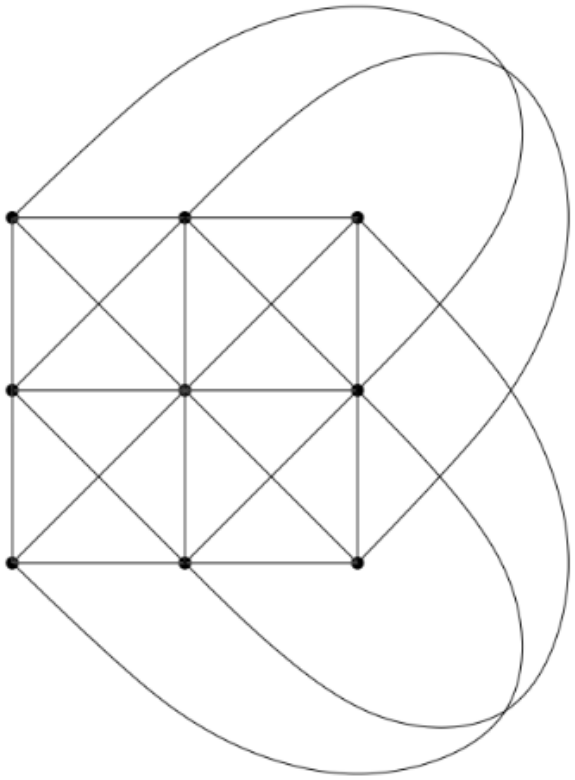

Figure 3: $AG(2,3)$

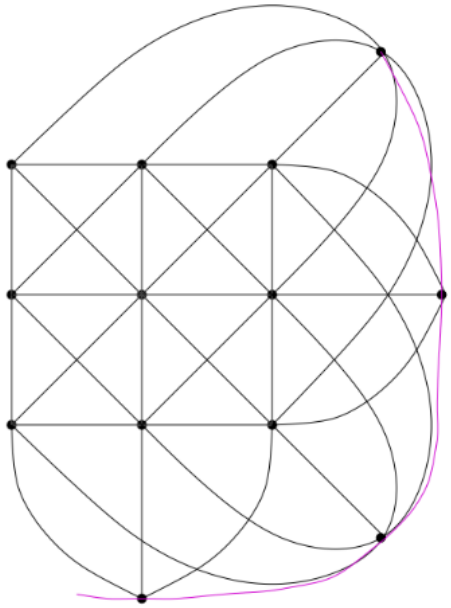

Figure 4: The completion of $AG(2,3)$ yields $PG(2,3)$.

Example 5.2. Let $\mathcal{P}$ be the set of points of an affine plane. Let $\mathcal{L}$ be the set of lines, and let $\mathcal{E}$ be the set of equivalence classes of parallel lines. Each line belongs to an equivalence class, say $E \in \mathcal{E}$. Define a new line $l^+ = l \cup \{E\}$. The incidence structure whose points are $P \cup \mathcal{E}$, and whose lines are $\{l^+ \mid l \in \mathcal{L}\}$, and the line at infinity $l_\infty = \{E \mid E \in \mathcal{E}\}$ is a projective plane.

On the other hand if we delete a line and all the points incident with that line from a projective plane, then the remaining structure is an affine plane. The deleted line is often called the "line at infinity". It is interesting to note that deleting different lines from a projective plane can yield non isomorphic affine planes.

Proposition 5.3. *In an affine plane every line is incident with a constant n points and every point is incident with $n+1$ lines.*

Proof. Complete the affine plane to a projective plane. □

We define the integer n to be the order of an affine plane.

Proposition 5.4. *An affine plane of order n has n^2 points, and n^2+n lines.*

6 Mutually Orthogonal Latin Squares

A latin square of order n is an $n \times n$ matrix with entries from $\{1, 2, \ldots, n\}$ with the property that every element of $\{1, 2, \ldots, n\}$ appears exactly once in each row and column.

Definition 6.1. A pair of latin squares $A = (a_{ij})$, $B = (b_{ij})$ are called orthogonal if for all (k, l) there exists a unique (i, j) such that $a_{ij} = k$, and $b_{ij} = l$.

Example 6.2. The matrices $\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix}$ and $\begin{bmatrix} 1 & 3 & 2 \\ 2 & 1 & 3 \\ 3 & 2 & 1 \end{bmatrix}$ are orthogonal latin squares.

Let $N(n)$ denote the maximum number of mutually orthogonal latin squares of order n.

Proposition 6.3. *There are at most $n-1$ mutually orthogonal latin squares of order n, so $N(n) \leq n-1$.*

Proof. Note that after permuting the set $\{1, 2, \ldots, n\}$, in each latin square individually, the $n-1$ mutually orthogonal latin squares will still be mutually orthogonal. Hence, WLOG, we can suppose that the 1 is the entry $(1,1)$ in each of the mutually orthogonal latin squares. In each latin square, the $(n-1)^2$ entries that are not in the first row or the first column contain $n-1$ 1's, and 1 does not occur in the same cell in two different matrices, since the entry $(1,1)$ is 1 in all the latin squares, by assumption. Hence $N(n)(n-1) \leq (n-1)^2$, where the lhs counts the number of total 1's in the $N(n)$ mutually orthogonal latin squares, and $(n-1)^2$ counts the maximum possible number of 1's in the $N(n)$ MOLS. □

6.1 MOLS, Affine Planes

Given a set of $n-1$ mutually orthogonal latin squares $A_1, A_2, \ldots, A_n$, we can construct an affine plane of order n in the following way. Let the set $\{(i,j) \mid i,j = 1,2,\ldots,n\}$ be the points, and the sets

$$\{(x,j) \mid x = 1,2,\ldots,n\}, \quad j = 1,2,\ldots,n.$$

be n "horizontal" lines, the sets

$$\{(j,x) \mid x = 1,2,\ldots,n\} \quad j = 1,2,\ldots,n$$

be "vertical" lines, and for each A_m, we define for each $k = 1,2,,\ldots,n$ a line

$$\{(i,j) \mid (A_m)_{ij} = k\}.$$

On the other hand, given an affine plane of order n, we can construct $n-1$ mutually orthogonal latin squares by fixing two parallel classes as the horizontal lines and the vertical lines, coordinatizing the points with respect to the horizontal and vertical lines, and following the above construction in reverse.
Since we know that there are affine planes of order n whenever n is the power of a prime, in these cases, we can attain the bound in Proposition 6.3. However, if n is not the power of a prime, $N(n)$ would be an indication of how close we can get to constructing an affine (hence projective) plane. By Theorem 3.6, there is no affine plane of order 6. In fact, there are not even 2 orthogonal latin squares of order 6, which was conjectured and partially proved by Euler. There are however two orthogonal latin squares of order 10; it is not known if there are three MOLS of order 10.
Given MOLS of order r, s, we can construct MOLS of order rs in the following way. Consider a latin square of order r whose entries come from an r-element set G. Define a multiplication $*$ on G by the rule $g_i * g_j = g_k$, if g_k is the (i,j) entry in the latin square. Then the two latin squares $(G,*)$, and $(G,\circ)$ ($\circ$ defined analogously) are orthogonal if for all $g_k, g_l \in G$, there exists a unique pair (i,j) such that $g_i * g_j = g_k$, and $g_i \circ g_j = g_l$. If $(H,*)$ and $(H,\circ)$ are orthogonal latin squares of order s, then the latin squares $(G \times H, *)$ and $(G \times H, \circ)$ are orthogonal, where $(G \times H, *)$ is defined by the rule

$$(g_1, h_1) * (g_2, h_2) = (g_1 * g_2, h_1 * h_2).$$

Proposition 6.4. *If $n = p_1^{n_1} \cdots p_r^{n_r}$, where p_i are distinct primes, and $n_i > 0$, then $N(n) \geq q-1$, where q is the smallest $p_i^{n_i}$.*

Proof. We can construct $p_i^{n_i} - 1$ mutually orthogonal latin squares of order $p_i^{n_i}$ from $AG(2, p_i^{n_i})$. □

Corollary 6.4.1. *If $n \not\equiv 2 \bmod 4$, then there exist at least 2 orthogonal latin squares of ordeer n.*

The remainder of chapter one of IFG is about how the group $GL(n,q)$ acts on $PG(n-1,q)$, and the construction of $PSL(n,q)$.

7 Orthogonal Arrays and MOLS

The rest of this document is from Stinson.

Definition 7.1. Let $k \geq 2$, and $n \geq 1$ be integers. An orthogonal array $OA(k, n)$ is an $n^2 \times k$ array, A, with entries from a set X of cardinality n such that within any two columns of A, every ordered pair of symbols from X occurs in exactly one row of A.

We provide a construction of $OA(s + 2, n)$ from s MOLS of size n. Suppose WLOG $L_1, \ldots, L_s$ are MOLS on the symbol set $\{n\}$, and their rows and columns are labeled $\{1, 2, \ldots, n\}$. For every $i, j \in \{1, \ldots, n\}$, construct an $(s + 2)$-tuple

$$(i, j, L_1(i, j), \ldots, L_s(i, j)).$$

Then form an array A whose rows consist of these n^2 $(s+2)$-tuples. We will show that A is $OA(s+2, n)$. We need to show that every ordered pair of symbols occurs in any two columns a, b, where $1 \leq a < b \leq s + 2$. We consider several cases.

1. If $a = 1$, $b = 2$, then we are good.
2. If $a = 1, b \geq 3$, then we get every ordered pair because every row of L_b is a permutation of $[n]$.
3. If $a = 2, b \geq 3$, then we get every ordered pair because every column of L_b is a permutation of $[n]$.
4. If $a \geq 3$, then we get every ordered pair because L_a, L_b are orthogonal.

The process can be reversed, but its not important for my homework.

Closing

You'll notice most of the claimed constructions are not proven to actually work. They are all homeworks for MATH888.