Super rough draft, some direction on writing style, proof techniques, etc, would be greatly appreciated!

1 Affine and Projective Spaces

To begin we need some definitions, of latin squares and of vector spaces over finite fields.

1.1 Finite Projective Spaces

The original motivation for projective geometry was on making rigorous statements such as parallel lines meet at infinity, whose suggestion is natural in the study projection in graphic art. Whilst the study originally began with real projective spaces, whose application to perspective drawing was clear, such notions of points at infinity turn out to be useful when working in finite geometry. We will see how projective geometry has applications to the traditionally combinatorial latin squares and hypercubes, but first we need some preliminaries from finite projective geometry.

Definition 1. *The vector space $V(n,q)$ is the vector space whose vectors are the ordered n-tuples of elements in $\mathbb{F}_q$ and scalars in $\mathbb{F}_q$.*

Definition 2. *The projective space $\mathrm{PG}(n,q)$ is the geometry whose points, lines, rank k hyperplanes are lines, planes and rank $k+1$ subspaces in $V(n+1,q)$ respectively.*

Most of our work will be done using constructions involving $\mathrm{PG}(3,q)$ and $\mathrm{PG}(2,q)$. The following housekeeping lemmas will be useful for these constructions.

Lemma 1. *The number of rank k subspaces in $V(n,q)$ is $\frac{(q^n-1)(q^n-q)\ldots(q^n-q^{k-1})}{(q^k-1)(q^k-q)\ldots(q^k-q^{k-1})}$.*

Proof. The numerator of describes choosing k linearly independent points from $V(n,q)$ to span a rank k subspace. The denominator counts the number of bases in a rank k subspace. □

Corollary 1. *The number of rank k subspaces in $V(n,q)$ containing a given subspace of rank $d \leq k$ is $\frac{(q^{n-d}-1)(q^{n-d}-q)\ldots(q^{n-d}-q^{k-d-1})}{(q^{k-d}-1)(q^{k-d}-q)\ldots(q^{k-d}-q^{k-d-1})}$.*

Lemma 2. *Given two subspaces V_1 and V_2 of a vector space V, $\dim(V_1+V_2) = \dim V_1 + \dim V_2 - \dim(V_1 \cap V_2)$.*

Proof. Let V_1 and V_2 be two subspaces of a vector space V and consider a basis B for their intersection $V_1 \cap V_2$. The basis B may be extended by adding additional basis vectors to get a basis for V_1 and V_2, we will call these bases B_1 and B_2 respectively. It follows that,

$$|B_1 \cup B_2| = |B_1| + |B_2| - |B_1 \cap B_2|$$

Each term describes the dimension of V_1+V_2, V_1, V_2, and $V_1 \cap V_2$ respectively. □

We may define the dimension of a projective hyperplane H in $\mathrm{PG}(n,q)$ as one less than the dimension of the associated vector space V.

Definition 3. *The projective dimension of a hyperplane* Π *in* $\mathrm{PG}(n,q)$ *is one less than the dimension of the associated vector space in* $V(n+1,q)$.

Definition 4. *The span of* k *hyperplanes in* $PG(n,q)$, $\langle \Pi_1, \Pi_2, \ldots, \Pi_k \rangle = \bigcap \{U | U \subseteq V(n+1,q) \wedge \Pi_1 + \Pi_2 + \cdots + \Pi_k \subseteq U \wedge U \textit{ is a subspace}\}$

Lemma 2 then gives us two immediate corollaries from Definition 4.

Corollary 2. *Given two hyperplanes* Π_1 *and* Π_2 *in a finite projective space* $\mathrm{PG}(n,q)$, $\dim(\langle \Pi_1, \Pi_2 \rangle) = \dim(\Pi_1) + \dim(\Pi_2) - \dim(\Pi_1 \cap \Pi_2)$.

Corollary 3. *In* $PG(2,q)$ *two distinct lines* L_1 *and* L_2 *must always meet a point.*

Proof. Using Corollary 2,

$$\dim L_1 \cap L_2 = \dim L_1 + \dim L_2 - \dim(\langle L_1, L_2 \rangle) = 0$$

This relies on the fact that $L_1 \neq L_2$, so that $\dim(\langle L_1, L_2 \rangle) = 2$. □

When we start to work with latin squares and hypercubes we will not always have a field to work with, so it helps to define a notion of a projective space that is independent of the concept of a field. To do this we introduce the notion of an axiomatic projective plane (and later an axiomatic projective space of any dimension).

Definition 5. *A projective plane is a set of points* P *and lines* $L \subset \mathcal{P}(P)$ *such that the following axioms hold:*

Axiom 1. *Given any pair of points* x, y *there exists a unique line* l *such that* $\{x, y\} \subseteq l$.

Axiom 2. *Given any pair of lines* l_1, l_2 *we have* $l_1 \cap l_2 = \{x\}$, *that is they intersect at a single point.*

Axiom 3. *There exists three points that are not collinear (that is not as a subset of any line).*

A projective plane is called finite if the point set is finite.

The set of all lines through a point is called the pencil of a point and the set of all points on a line is called the range of the line. The axioms we have defined give a remarkable amount of structure to our geometry.

Lemma 3. *Given a line* l *and a point* $p \notin l$ *in a finite projective plane, the number of lines through* p *is equal to the number of points on a line* l.

Proof. Consider an arbitrary point p not on a line l in a finite projective plane. Given any point $q \in l$ our Axiom Axiom 1. gives us a line through p and q, so the number of points on l is at most the number of lines through p. On the other hand, any line through p must intersect l by Axiom Axiom 2., so the number of points on l is at least the number of lines through p. Therefore the number of lines through p is equal to the number of points on l. □

Corollary 4. *Given any two lines l_1, l_2, $|l_1| = |l_2| = q + 1$ for some positive integer q.*

Proof. Consider a point p not on l_1 and l_2 (note that this may always be done due to Axiom Axiom 3.) and the set of lines through p, L. The set of points P_1 on l_1 may be put in bijection with L, so $|P_1| = |L|$. The set of points P_2 on l_2 may also be put in bijection with lines through p, so $|P_2| = |L| = |P_1| = q + 1$. □

Corollary 5. *If in a finite projective plane with point set P and line set L the number of points (lines) incident to a line (point) is $q + 1$, then $|P| = |L| = q^2 + q + 1$.*

Proof. Consider an arbitrary point p in the plane. There are $q+1$ lines through p and each point has $q+1$ points, q excluding p. Thus $|P| = q(q+1)+1$. To see that $|P| = |L|$ we can double count $S = \{\{p, l\}|p \in l\}$. Incident to each point p is $q + 1$ lines, so $|S| = (q + 1)|P|$, and incident to each line l is $q + 1$ points, so $|S| = (q+1)|L|$. Therefore $(q+1)|P| = (q+1)|L|$ and $|P| = |L| = q^2+q+1$. □

The q for which $|P| = q^2 + q + 1$ is called the *order* of the projective plane. As support for later proofs we will want the following lemma,

Lemma 4. *A set of $n^2 + n + 1$ points P and $n^2 + n + 1$ lines L such that,*

1. *Each line $l \in L$ has $n + 1$ points.*
2. *Any pair of lines intersects at exactly one point.*
3. $|P| = |L| = n^2 + n + 1$

is a projective plane of order n.

Proof. Axiom Axiom 2. is already given, so we need only show Axiom Axiom 1. and Axiom Axiom 3.. Axiom Axiom 2. follows from the fact that because every pair of lines intersects at a unique point, every pair of points must be on at most one line. There are $\binom{n^2+n+1}{2}$ pairs of points in P and $(n^2+n+1)\binom{n+1}{2}$ pairs of points covered by lines in L, and because $\binom{n^2+n+1}{2} = \frac{(n^2+n+1)(n^2+n)}{2} = (n^2 + n + 1)\frac{n(n+1)}{2} = (n^2 + n + 1)\binom{n+1}{2}$ every pair of points must be on exactly one line. Axiom Axiom 3. follows from the fact that if I pick a pair of points $p \neq q$ (which can only exist on one line) and one of the n^2 points not on the line determined by p and q these points cannot be collinear (due to the unique of a line containing p, q). □

One question we still haven't answered is for what q is it possible to construct an axiomatic projective plane? This is an open problem with the following famous conjecture,

Conjecture 1 (Prime Power Conjecture)**.** *The order of any finite projective plane is always p^k, for some prime p and integer $k \geq 1$.*

1.2 Duality

The axioms of the projective plane are self-dualising, that is if one exchanges the roles of points and lines in Axioms Axiom 1., Axiom 2. and Axiom 3. equivalent axioms will fall out. This duality can produce dual theorems that are sometimes useful, for instance the alternative proof that $|P| = |L|$ in Corollary would be to dualise the argument counting points and count the number of lines. Duality can be expressed more in a general projective space $\mathrm{PG}(d, q)$ by exchanging the roles of points and hyperplanes, span with intersection and the phrases "contianed in" with "containing". For instance we have the following statement following from Corrolary 2, the intersection of any two distinct hyperplanes in $\mathrm{PG}(d, q)$ is a plane with co-dimension 2. The dual statement reads "the span of any two distinct point in $\mathrm{PG}(d, q)$ is a line". We will use ideas of duality to help us work with some tricky hyperplanes.

1.3 Affine Planes

An axiomatic affine plane is a perhaps more familiar geometry, with the notion of parallel lines appearing and formally defined.

Axiom 1. Every two points are incident with a unique line.

Axiom 2. Given a line l and a point not on that line p, there exists a line m through p such that $m \cap l = \emptyset$.

Axiom 3. There are three points that are not collinear.

We call two lines l and m satisfying $m \cap l = \emptyset$ parallel, and we can show that the relationship $l \ m$ iff $l = m$ or l and m are parallel is an equivalence relation.

Lemma 5. *Let $l \sim m$ if and only if $l = m$ or l and m are parallel. $\sim$ is an equivalence relation.*

Proof. From the definition is certainly reflexive and symmetric. To see the transitivity property holds, suppose we have a line m and two lines distinct from m, l, l', such the l is parallel to m and m is parallel to l' but there exists $p \in l \cap l'$. It then follows that because m is parallel to both l and l' that $p \notin m$, Axiom Axiom 2. says there should be a unique line parallel to m through p, and therefore $l = l'$. Thus if l is parallel to m and m is parallel to l' then l is parallel to l'. □

Because parallelism forms an equivalence relation we can partition the set of lines into parallel classes, characterised by the fact that they are pairwise parallel to each other. The following housekeeping lemmas will use this fact to show that the number of lines and points in an affine plane can be parameterised by an integer n which we will call the *order* of the affine plane.

Lemma 6. *Let P_1 and P_2 be the parallel classes of two lines l_1 and l_2 that are not parallel, then $|P_1| = |P_2|$.*

Proof. Begin by picking a point p on $l_1 \setminus l_2$ and q on $l_2 \setminus l_1$. The line m through p and q intersects l_1 and l_2 and is thus in neither parallel class. For each point on $m \setminus \{p\}$ a there is a unique line passing through p parallel to l_1, each line parallel to l_1 must intersect m (and these no intersection point may be shared by two parallel lines), so it follows that $|m| = |P_1|$. Similar logic follows for lines through P_2 and m so that $|P_2| = |m|$. Thus $|P_1| = |m| = |P_2|$. □

The order of the affine plane will be the size of the parallel class.

Lemma 7. *In an affine plane of order n, every line has n points.*

Proof. Following our prior logic, if we pick a line l and another line m such that m is not parallel to l we may put the points of l in one to one correspondence with lines in the parallel class of l so that $|l| = n$. □

Lemma 8. *There are n^2 points in an affine plane of order n.*

Proof. Pick a line l and it's parallel class P. For any point p either $p \in l$ or there is a unique line m parallel to l through p. At the same time $l_1 \cap l_2 = \emptyset$ for any pair of distinct lines l_1 and l_2 in P. Therefore the lines of P partition the point set of the affine plane. It therefore follows that there are n^2 points in the affine plane. □

Lemma 9. *In an affine plane of order n there is $n(n+1)$ lines.*

Proof. Picking any two distinct points we can construct a unique line through both, and for any line we pick any pair of points that determine the same line. Therefore there are

$$\frac{\binom{n^2}{2}}{\binom{n}{2}} = n(n+1) \tag{1}$$

distinct lines in an the affine plane of order n. □

Lemma 10. *In an affine plane of order n every point has $n+1$ points incident to it.*

Proof. Fix a point p in the plane. Picking one of the $n^2 - 1$ points q will determine a line through p. For each pair (p, q) spanning a line l, $n - 1$ other choices for q would've spaned the same line, so the number of lines through a point is

$$\frac{n^2-1}{n-1} = n+1 \tag{2}$$

□

The relationship between projective planes and affine planes is predictably close, in fact the existence of an affine plane is equivalent to the existence of a projective plane.

Theorem 1. *The existence of an affine plane of order n is equivalent to the existence of a projective plane of order n.*

Proof. Assume we have an affine plane of order n with points P and lines L. Partition the set of lines in the plane L into parallel classes $P_1, P_2, \ldots, P_{n+1}$. Add $n+1$ points $E_1, E_2, \ldots, E_{n+1}$ to P representing each parallel class and add a line $L_\infty = \{E_i | 1 \leq i \leq n+1\}$ to L. Then for each line $l \in L$ we will add the point E_i to l where E_i represents the parallel class P_i that l belongs to. We now have n^2+n+1 points, and n^2+n+1 lines with the property that any pair of lines intersects at exactly one point, each nonparallel line in the affine plane will still intersect at a single point and every parallel line will now intersect at l_∞ as they belong to the same parallel class. From Lemma 4 this implies our points and lines form a projective plane of order n. □

1.4 k-nets of order n

Definition 6. *A net degree $k \geq 2$ and order n (hereafter a k-net of order n) is a set of n^2 points and k parallel classes such that each parallel class consists of n disjoint lines of size n and such thta lines of distinct parallel classes meet in a unique point.*

k-nets can be thought of as a generalisation of the incidence properties an affine plane, indeed the following lemma establishes that affine planes are a special case of affine planes.

Lemma 11. *An $n+1$-net of order $n \geq 2$ is an affine plane of order n.*

Proof. Suppose we have an (n + 1)-net of order n, we will show that the axioms for an affine plane follow from those of the net. Axiom Axiom 1. directly follows from the definition of a net, as every pair of lines is either parallel or intersecting in a single point. The next axiom, Axiom 2., follows from the fact that because the parallel classes partition the plane, given a line l identifying a parallel class and a point p not on that line there is a single line in the parallel class through p. The third axiom, Axiom Axiom 3. follows from the fact that if $n \geq 2$ one can identify 3 points, which cannot be included on the same line. □

Because each parallel class partitions the point set every point in a k-net of order n is incident to k lines, one from each parallel class.

One remarkable property of a n-net of order n is that they may be extended uniquely to an affine plane. This will be used later to show some interesting theorems about mutually orthogonal latin squares.

Lemma 12. *An n-net of order n may be extended to an $(n+1)$-net of order n.*

Proof. We will begin by constructing a set of n parallel lines. The procedure to do this will be to pick a point p_1 from among the set of n^2 points in the net, and construct the line l_1 consisting of all points not on any line through p_1 plus p_1 itself. Because p_1 is on n lines concurrent at p_1 only, there are $n^2 - n(n-1) - 1 = n - 1$ points not covered by any line through p_1 and therefore $|l_1| = n$. The next line l_2 will be constructed by picking $p_2 \notin l_1$ and taking the set of points not on any line through p_2, and so on to get a set of n lines and points $p_1, l_1, p_2, l_2, \ldots, p_n, l_n$. To see that the lines are disjoint we are going to show that the relationship $p \sim q \iff p = q$or p and q are not on a line together is an equivalence relation. Reflexivity and symmetry are clear so it just remains to show that the relationship is transitive. Suppose I have three distinct points p, q, r such that p and q are not on a line together, q and r are not on a line together, but p and r are on a line together. By our net axioms there is exactly one line through q that is parallel to pr. Other than that the remaining $n-1$ lines through q must intersect the line pr in one of n points on pr except p and r since q is on a line with neither. However by the pigeonhole principle we conclude that two lines through q must intersect at the same point on the line pr and by contradiction we conclude that p cannot be collinear with r. Because the collinearity relationship is an equivalence relation the lines form equivalence classes that partition the plane. All that needs to be checked then is that these new lines do not intersect twice with another line from the original net. If l_i is a line constructed from points not collinear with p_i and m a line from the original net, assume that $\{p, q\} \subseteq l_i \cap m$. By taking the unique parallel lines through each point in $l_i \setminus m$ we have $n-1$ lines that must intersect with at most $n-2$ points in $l_i \setminus m$, so at least two lines must intersect at the same point in $l_i \setminus m$ — which contradicts the parallel properties of these lines. Thus we have an $(n+1)$-net of order n. □

2 Projective Spaces and Orthogonal Hypercubes

Definition 7. *A latin square of order n is an $n \times n$ array, where each entry in the array is assigned one of n symbols such that every symbol appears exactly once in each row and each column.*

For any order $n \geq 2$ a latin square may always be constructed by constructing the array $A = [a_{ij}]$ where $a_{ij} = i + j$. Because $\mathbb{Z}_n$ is a group under addition for all n it follows that A each row and column should have each element exactly once (since the equation $i + j = c$ has a unique solution when fixing either of i or j).

Given two latin squares we say they are orthogonal if when overlaying the first square over the second each of the n^2 possible ordered pair of symbols appears exactly once. A set of latin squares is *mutually orthogonal* it is pairwise orthogonal. Lemma 1 answers the quesiton "What is the largest set of mutually orthogonal latin squares for a given order?".

Lemma 13. *Let M be a set of mutually orthogonal latin squares of order $n \geq 2$, then $|M| \leq n-1$.*

Proof. Let $M = A^i$ be a set of mutually orthogonal latin squares $A^i, 1 \leq i \leq |M|$ of order $n \geq 2$. Without loss of generality we may assume that the first row of each latin square is given by $1, 2, 3, \ldots n$, because we may permute symbols to make this so if it isn't already for any given latin square without affecting orthogonality. We will now count the set $N = \{A^1_{21}, A^2_{21}, \ldots, A^{|M|}_{21}\}$. Because the symbol above A^i_{21} is fixed to one $A^i_{21} \in 2, 3, \ldots, n$ for each i, and moreover because $(A^i_{1k}, A^j_{1k}) = (k, k)$ for each $1 \leq i, j \leq |M|, 1 \leq k \leq n$ we cannot have $A^i_{21} = A^j_{21}$ for any $1 \leq i, j \leq |M|$. It therefore follows that N is a permutation of $2, 3, \ldots, n$ and $|N| = n-1$. □

Theorem 2. *A set of $n-1$ mutually orthogonal latin squares of order n always exists if n is a prime power.*

Proof. Consider $PG(2, n)$, which always exists for prime powers, and the line at infinity L_∞. Distinguish two of the $n+1$ points on this line as r and c respectively. We will call the n lines through r (excluding the line at infinity) our row lines, and the n lines through c our column lines, generically these lines are referred to as coordinate lines. Each pair of lines has a unique intersection that is by construction among the n^2 points not on the line at infinity, and because every pair of points has a unique line through it, each of the n^2 points has a unique pair of coordinate lines that intersect at it. It therefore makes sense to coordinatise the remaining points in the plane with reference to their intersection of coordinate lines. Because a latin square also has n^2 entries, we will coordinatise the entries of a latin square according to intersections of the coordinate lines. The remaining $n-1$ points on the line at infinity each have n lines through them (excluding the line at infinity) and these lines we will refer to as symbol lines. Each of the $n-1$ points will be used to define a latin square. Fix a point in $L_\infty - \{r, c\}$ and call it L_i. Where each symbol line S_j through L_i intersects the remaining n^2 points we will place the symbol j in the corresponding entries of the ith latin square. Because each symbol line intersects each coordinate line only once, each row and column has exactly one of each symbol. Taking the set of $n-1$ latin squares defined in this fashion we need only show orthogonality. Given two symbol lines S_i and S_j from two different latin squares we know that these intersect at a single point which cannot be in the line at infinity. Where the symbol lines intersect is therefore the only place where (i, j) appears upon overlapping the two latin squares and so the set of $n-1$ latin squares we have defined is mutually orthogonal. □

We can also go the other way and show that the existence of a complete set of mutually orthogonal latin squares of order n is equivalent to the existence of a projective plane of order n.

Theorem 3. *The existence of k mutually orthogonal latin squares of order n is implies the existence of a $k+2$-net of order n.*

Proof. Suppose we have a complete set of k MOLS $M = \{A^1, A^2, \ldots, A^k\}$ of order n. Let $P = \{(x, y)|x, y \in \mathbb{Z}_n\}$, be a set of n^2 points. Let our lines be the $kn + 2n = (k + 2)n$ lines constructed by taking $L^i_j = \{(x, y)|(x, y) \in P \wedge A^i_{x,y} = j\}$ for $1 \leq i \leq n - 1, j \in \mathbb{Z}_n$ and the $2n$ lines $R_i = \{(x, i)|x \in \mathbb{Z}_n\}$ and $C_j = \{(j, y)|y \in \mathbb{Z}_n\}$ for each $i, j \in \mathbb{Z}_n$. Because we get one occurence of the symbol j in each row of a latin square A^i, $|L^i_j| = n$. We may partition the line set into $k + 2$ parallel classes, each of the k classes $P_i = \{L^i_1, L^i_2, \ldots, L^i_n\}$ plus the row class $R = \{R_1, R_2, \ldots, R_n\}$ and column class $C = \{C_1, C_2, \ldots, C_n\}$. The lines in the row and column classes are clearly parallel, and the lines in the latin square classes are parallel because no two symbols are assigned to the same position in a given latin square. In addition no two lines from distinct parallel classes are parallel, because each line L^i_j intersects every row and column line once (one symbol in each row and column by definition) and because A^i and A^k are orthogonal for $i \neq k$, there is a unique intersection of the lines L^i_j and L^k_l for all $i \neq k, j, l$. Each point (x, y) will have a single line from each parallel class incident to it, namely R_x, C_y and for each $1 \leq i \leq k$ the line L^i_j is incident to (x, y) if and only if $A^i_{x,y} = j$. So we have a set of points and lines such that each of the $(k + 2)n$ lines has n points, each belongs to one of k parallel classes with n lines each, and every point is incident to k lines (one from each class). It follows that by definition the set of points P and lines $\{L^i_j|1 \leq i \leq n - 1\} \cup \{R_x|x \in \mathbb{Z}_n\} \cup \{C_y|y \in \mathbb{Z}_n\}$ forms a $(k + 2)$-net of order n. □

Corollary 6. *The existence of a set of $n-1$ MOLS of order n is equivalent to the existence of an affine plane of order n.*

Corollary 7. *The existence of a set of $n-1$ MOLS of order n is equivalent to the existence of a projective plane of order n.*

One can also extend a set of $n-2$ MOLS of order n to a set of $n-1$ MOLS of order n.

Theorem 4. *A set of $n-2$ MOLS of order n may be extended to a $n-1$ MOLS exists of order n.*

Proof. Assume we have a set of $n-2$ MOLS of order n, $M = \{A^1, A^2, \ldots, A^{n-2}\}$. Using Theorem 3 we may take M and construct a n-net, and then using Lemma 12 obtain a $n + 1$-net of order n. Then by Corollary 7 and Theorem 2 we can construct a set of $n - 1$ MOLS, $n - 2$ will be the original MOLS in M and the last coming from the extension in Lemma 12. □

We will attempt to generalise some of our results to latin squares in higher dimensions, but first we need some definitions of what that even means.

Definition 8. *A (d, n, r, t)-hypercube of dimension d, order n, class r and type t is an $n \times n \times \cdots \times n$ (d times) array on n^r distinct symbols such that in every co-dimension-t-subarray (that is, fix t coordinates and allow the remaining $d - t$ coordinates to vary) each of the n^r distinct symbols appears exactly*

n^{d-t-r} times. Moreover, if $d \geq 2r$ two such hypercubes are orthogonal if when superimposed each of the n^{2r} possible distinct pairs appears exactly n^{d-2r} times. A set of hypercubes is mutually orthogonal if each pair of hypercubes in the set are orthogonal.

The familiar latin square is a $(2, n, 1, 0)$-hypercube. The following theorem is due to John T. Ethier, Gary L. Mullen, et al,

Theorem 5 (Ethier-Mullen-Panario-Stevens-Thomson)**.** *The maximum number of mutually orthogonal hypercubes of dimension d, order n, type t and class r is bounded above by*

$$\frac{1}{n^r - 1}\left(n^d - 1 - \binom{d}{1}(n-1) - \binom{d}{2}(n-1)^2 - \cdots - \binom{d}{t}(n-1)^t\right).$$

For the machinery of the approaching theorem we also require this small result,

Lemma 14. *In $PG(3, q)$ if any three distinct planes do not intersect at a common line, they must intersect at a point.*

Proof. Consider three distinct planes Π_1, Π_2, Π_3 in $PG(3, q)$ whose intersection is not a line. By an extension of Lemma 2 and treating each projective plane as subspaces of $V(4, q)$,

$$\dim(\Pi_1 + \Pi_2 + \Pi_3) = \sum_i \dim \Pi_i - \sum_{i \neq j} \dim \Pi_i \cap \Pi_j + \dim \Pi_1 \cap \Pi_2 \cap \Pi_3.$$

The intersection of any pair of these planes must be a line (by the same logic as Lemma 2). Because these planes are distinct, and because they do not intersect at a common line, their sum must span $V(4, q)$ and so $\dim(\Pi_1 + \Pi_2 + \Pi_3) = 4$.

$$4 = 3 + 3 + 3 - 2 - 2 - 2 + \dim \Pi_1 \cap \Pi_2 \cap \Pi_3.$$

The only way this equation holds therefore is if the dimension of the intersection $\Pi_1 \cap \Pi_2 \cap \Pi_3$ is a line in $V(4, q)$ and thus a point in $PG(3, q)$. □

We now present a generalised construction of Theorem 2 for $(3, n, 1, 2)$-hypercubes.

Theorem 6. *A complete set of mutually orthogonal (3, n, 1, 2)-hypercubes always exists if n is a prime power.*

Proof. Due to Theorem 5, if we can construct a set of $(n-1)^2$ mutually orthogonal hypercubes we will have a complete set. To do this we are going to work in $PG(3, n)$ and use the plane at infinity Π_∞ in much the same way the line at infinity was used in Theorem 2. Designate three non-concurrent lines in Π_∞, R,

C, and S and the vertices of the triangle defined by their intersection x_1, x_2, x_3 (this is always possible as there are three non-colinear points in any projective plane). There are $n^2+n+1-(n+1)-n-(n-1) = (n-1)^2$ lines that do not intersect R, C or S at x_1, x_2, x_3. By Lemma 1 there are $n+1$ planes through each line in Π_∞ and n planes besides Π_∞. The $3q$ distinct planes through R, C and S are going to be our coordinate planes, and by Lemma 14 because any pair of planes from a triple of coordinate planes intersect at distinct lines containing the non-colinear points x_1, x_2, x_3, each triple intersects at a point. Moreover one can construct any point p of the q^3 points in $PG(3, q)$ not contained in Π_∞ by constructing the planes containing it and each of lines R, C, S in turn. It therefore makes sense to coordinatise each of the q^3 points of a (3, n, 1, 2)-hypercube by the intersections of coordinate planes. Note that a 2-subarray correpsonds to the intersection of two coordinate planes. Considering any of the $(n-1)^2$ lines not incident to x_1, x_2, x_3 we can take each of the q planes (apart from Π_∞) through this line and call them symbol planes. A symbol plane S_i contains n^2+n+1 points, $n+1$ of which are in Π_∞ and so places the symbol i at n^2 positions in a hypercube. Because our chosen line defining S_i is not incident to x_1, x_2, x_3 the intersection of S_i with two coordinate planes Π_1, Π_2 through two distinct lines among $\{R, C, S\}$ must intersect at a point. The previous assertion is equivalent to saying that each 2-subarray of the hypercube will contain the symbol i exactly once. Because any pair of symbol planes chosen from the same line only intersect at that line in Π_∞ the symbol planes partition the n^2 coordinate points and thus assigning the symbol i to each point in the hypercube touching the symbol plane S_i defines a $(3, n, 1, 2)$-hypercube. Defining the set of $(n-1)^2$ hypercubes in a similar fashion gives us a set H. The set H must be mutually orthogonal because any pair of symbol planes S_i, S'_j from different lines in Π_∞ will intersect at a line for which q points are outside Π_∞ and this is equivalent to each pair of symbols occurring exactly n times when overlapping any pair of hypercubes in H. □

Proof of equivalence is not yet shown (but strongly held belief exists).

We can also prove a more general result for arbitrary dimensions.

Theorem 7. *A complete set of mutually orthogonal $(d, n, 1, d-1)$-hypercubes will always exist if n is a prime power.*

Proof. Let $X = \{e_1, e_2, \ldots, e_d\}$ where $e_i = (0, 0, \ldots, 1, 0, \ldots, 0)$ is a point in $\mathrm{PG}(d, n)$ having a 1 in the ith position and zero everywhere else. By removing some e_i we get a subset S of $d-1$ points in X that spans a $d-2$ plane in the hyperplane at infinity, furthermore there are q hyperplanes through S apart from the hyperplane at infinity — $x_i X_i + X_{d+1}$ and $X_i = 0$. The hyperplanes constructed by removing some e_i from X we will call coordinate hyperplanes. If we take d coordinate planes we can show their intersection is an affine point. Pick d hyperplanes constructed by removing one of $e_1, e_2 \ldots e_d$ in turn, to obtain their intersection we must find a solution to the following system of homogenous equations:

$$A = \begin{bmatrix} x_1 & 0 & \dots & 0 & \alpha_1 & \\ 0 & x_2 & \dots & 0 & \alpha_2 & \\ \dots & & & & & \\ 0 & 0 & \dots & 0 & x_d & \alpha_d \end{bmatrix}$$

Where $\alpha_i = 0$ if the hyperplane it describes is X_i and $\alpha_i = 0$ otherwise. This system has rank d and a single projective point as a solution, namely $(\alpha_1 x_1, \alpha_2 x_2, \dots, \alpha_d x_d, 1)$. This allows us to coordinatise the affine space in terms of hyperplanes at infinity.

Our analogue to symbol planes in Theorem 5 will be symbol hyperplanes whose intersection with the hyperplane at infinity does not include X. To count such hyperplanes let A_i be the set of $d-2$ hyperplanes containing the point $e_i \in X$, we wish to count $|\bigcap A_i'|$ and this can be done with the principle of inclusion-exclusion and repeated application of Lemma 1

$$\begin{aligned}
|\bigcap A_i'| &= \sum_{i=0}^{d-1} (-1)^i \binom{d}{i} \frac{n^{d-i}}{n-1} \\
&= \frac{1}{n-1} \left(\sum_{i=0}^{d-1} (-1)^i \binom{d}{i} n^{d-i} - \sum_{i=0}^{d-1} (-1)^i \binom{d}{i} \right) \\
&= \frac{1}{n-1} \left(\sum_{i=0}^{d-1} (-1)^i \binom{d}{i} n^{d-i} - \left(\sum_{i=0}^{d} (-1)^i \binom{d}{i} - (-1)^d \right) \right) \\
&= \frac{1}{n-1} \left(\sum_{i=0}^{d-1} (-1)^i \binom{d}{i} n^{d-i} + (-1)^d \right) \\
&= \frac{1}{n-1} \left(\sum_{i=0}^{d} (-1)^i \binom{d}{i} n^{d-1} \right) \\
&= \frac{1}{n-1} (n-1)^d \\
&= (n-1)^{d-1}
\end{aligned}$$

Taking any hyperplane through any of the $(n-1)^{d-1}$ planes at infinity gives us a hyperplane of the form $c_1 X_1 + c_2 X_2 + \ldots + c_d X_d + c_{d+1} X_{d+1}$ with each c_i non-zero (to avoid including one of the basis vectors). We can now consider it's intersection with $d-1$ coordinate planes, and WLOG assume that these planes are of the form $x_i X_i + X_{d+1}$ for each $1 \leq i \leq d-1$. Their intersection is the homogenous solution to the following,

$$A = \begin{bmatrix} x_1 & 0 & \dots & 0 & \alpha_1 & \\ 0 & x_2 & \dots & 0 & \alpha_2 & \\ \dots & & & & & \\ 0 & 0 & \dots & x_{d-1} & 0 & \alpha_d \\ c_1 & c_2 & \dots & c_d & c_{d+1} & \end{bmatrix}$$

This system has rank at least $d-1$ and at most d so the solution space is either a point or a line. If the solution space is a line, or if a point at infinity we may add the restriction $X_{d+1} = 0$ and obtain, $X_1 = X_2 = \ldots = X_{d-1} = 0$ and plugging this into our last equation get $c_d X_d = 0$. Because $c_d \neq 0$ we have $X_d = 0$ and the solution $(0, 0, \ldots, 0)$ — a contradiction. Thus the solution must be an affine point, i.e that the symbol hyperplanes intersect each 1-subaray at a single point. By each of $a \in \mathbb{F}_q$ to each of the q hyperplanes through each of the $(d-2)$-dimensional spaces in the hyperplane at infinity not intersecting X we get a set of $(n-1)^{d-1}$ hypercubes. These hypercubes are orthogonal because the intersection of any pair of symbol planes must be a $(d-2)$-dimensional space with $\sum_i^{d-2} q^i - \sum_i^{d-3} q^i = q^{d-2}$ affine points.

By Theorem 5 we have a complete set of mutually orthogonal $(d, n, 1, d-1)$-hypercubes.

□

There is a connection between the proof Theorem 5, Theorem 7 and existing proofs of similar theorems in the literature. In particular, in REFERENCE TO MULLEN AND LAYWINE HERE, we have a theorem which interpreted in the language of Definition 8 essentially shows Theorem **??**. More to the point, they construct general hypercubes using polynomials and these polynomials may be put in correspondence with the symbol and coordinate planes in our theorems. This is most clear in the $d = 2$ case where the polynomials Mullen defines are of the form $ax + y$ for non-zero a. These lines are precisely the $n-1$ lines that do not contain the points $(1, 0, 0)$ and $(0, 1, 0)$ at infinity.