Summer Project Report: Latin Hypercubes and Finite Projective Geometry

Jake Faulkner, University of Canterbury
Geertrui Van de Voorde, University of Canterbury

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", where in particular artists were interested in perspective drawing that accurately reflected projective properties of eyesight (such as parallel train tracks appearing to meet at the horizon). Whilst the study of projective geometry 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 too. We will see how projective geometry has can help us understand 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, dimension k subspaces are lines, planes and rank $k+1$ subspaces in $V(n+1,q)$ respectively. Incidence of subspaces in $\mathrm{PG}(n,q)$ is inherited naturally from incidence in $V(n+1,q)$.*

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

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

Proof. The numerator of describes the number of ways we can choose k ordered linearly independent points from $V(n,q)$ to span a rank k subspace. The denominator counts the number of ordered 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 $\frac{(q^{n-d}-1)(q^{n-d}-q)\dots(q^{n-d}-q^{k-d-1})}{(q^{k-d}-1)(q^{k-d}-q)\dots(q^{k-d}-q^{k-d-1})}$.*

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 subspace Π in $\mathrm{PG}(n,q)$ as one less than the dimension of the associated vector space V.

Definition 3. *The projective dimension of a subspace 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 projective span of k subspaces in $PG(n,q)$, $\langle \Pi_1, \Pi_2, \ldots, \Pi_k \rangle = \bigcap \{U | U \subseteq V(n+1,q) \wedge \Pi_1 + \Pi_2 + \cdots + \Pi_k \subseteq U \wedge U \textit{is a vector subspace}\}$*

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:*

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

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.*

3. *There exists four points, no three of which are collinear.*

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

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 l.*

Proof. Consider a line l, and a point $p \notin l$ in a finite projective plane. Given any point $q \in l$ 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 at a single point by Axiom 2, so the number of points on l is at least the number of lines through p. No two lines through p can intersect l at the same point without violating Axiom 2. 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, $|l_1| = |l_2| = n+1$ for some positive integer n.*

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

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 $n+1$, then $|P| = |L| = n^2+n+1$.*

Proof. Consider an arbitrary point p in the plane. There are $n+1$ lines through p and each of these lines has n points excluding p. Other than at p the lines are disjoint, thus $|P| = n(n+1)+1$. To see that $|P| = |L|$ we can double count $S = \{(p,l) | l \in L, p \in l\}$. By Corollary 4 incident to each point p is $n+1$ lines, so $|S| = (n+1)|P|$, and incident to each line l is $n+1$ points, so $|S| = (n+1)|L|$. Therefore $(n+1)|P| = (n+1)|L|$ and $|P| = |L| = n^2+n+1$. □

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

Definition 6. *A projective plane with n^2+n+1 points is a projective plane of order n.*

Lemma 4. *Let $n \geq 2$. 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 2 is already given, so we need only show Axiom 1 and Axiom 3. Axiom 1 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 $\binom{n^2+n+1}{2} = (n^2+n+1)\binom{n+1}{2}$ every pair of points must be on exactly one line. To show Axiom 3 consider two lines l, m intersecting at a point u. Because each line has $n+1 \geq 3$ points there are two points on l, p and q, and two points on m, r and s that are not shared between l and m and are distinct from u. No line can then contain any three of p, q, r, s without violating Axiom 1 or Axiom 2. □

One question we still haven't answered is for what n 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 $n = p^k$, for some prime p and integer $k \geq 1$.*

1.2 Affine Planes

An axiomatic affine plane is more like the geometry taught in schools, where lines may be parallel to each other. Here we formally define the notion of parallelism and explore affine planes in relation to projective planes.

Definition 7. *An affine plane is a set of points P and lines $L \subset \mathcal{P}(P)$ such that the folloming axioms hold:*

1. *Every two points are incident with a unique line.*
2. *Given a line l and a point $p \notin l$, there exists a unique line m through p such that $m \cap l = \emptyset$.*
3. *There are three points that are not collinear.*

We call two lines l and m satisfying $m \cap l = \emptyset$ or $l = m$ "parallel", and we can show that the natural relationship induced by parallelism is an equivalence relation.

Lemma 5. *For any pair of lines l, m in an affine plane, let $l \sim m$ if and only if l and m are parallel, then $\sim$ is an equivalence relation.*

Proof. From the definition of parallelism $\sim$ is clearly reflexive and symmetric. To see that the transitivity property holds, suppose we have a line m and two lines l, l' distinct from m, 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 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, which aree the equivalence classes of $\sim$.

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 $|P_1| = |m| = |P_2|$. □

We can use Lemma 6 to define a notion of order similar to Definition 6 for Projective Planes.

Definition 8. *An affine plane with a parallel class P of size n is an affine plane of order n. By Lemma 6 the order of an affine plane is well defined.*

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

Proof. Following our prior logic in Lemma 6, 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 m so that $|l| = n$. □

Lemma 8. *An affine plane of order n has n^2 points.*

Proof. Pick a line l and it's parallel class P. For any point p 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. By Lemma 7 it therefore follows that there are n^2 points in the affine plane. □

Lemma 9. *An affine plane of order n has $n(n+1)$ lines.*

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

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

distinct lines in an the affine plane of order n, using Lemma 7 and Lemma **??**. □

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

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

$$\frac{n^2 - 1}{n - 1} = n + 1. \qquad (1)$$

□

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 pair of nonparallel lines in the affine plane will still intersect at a single point and every pair of parallel lines will now intersect at l_∞ as they belong to the same parallel class, every line by definition will intersect l_∞ at it's parallel class. From Lemma 4 this implies our points and lines form a projective plane of order n.

Now assume we are given a projective plane of order n with points P and lines L. Pick any line $l \in L$ and let $L' = \{l' \setminus l | l' \in L \setminus \{l\}\}$ and $P' = P \setminus \{l\}$. We will now show P' and L' forms an affine plane of order n. The lines in L' may be partitioned into classes $\{P_1, P_2, \ldots, P_{n+1}\}$, one class for each point $p \in l$ containing each of the n lines apart from l incident to p in the projective plane. Because each pair of lines in a projective plane intersects at one point the lines in P_i must be parallel (having removed their intersection on l), and moreover as the lines have n points each and $|P_i| = n$ they partition the points and satisfy Axiom 2 of an affine plane. Lines from distinct parallel classes must intersect at a unique point in P' as they intersected at a unique point not on l in the projective plane. Any pair of points in P' will still have a line through both as they did in the projective plane. A set of three points that are not collinear may be obtained by taking two points on a given line $m \in L'$ and a single point not on m, these points cannot be collinear. Thus (P', L') forms an affine plane of order n. □

1.3 k-nets of order n

Definition 9. *A net of 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 that lines of distinct parallel classes meet in a unique point.*

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

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 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, 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 3 follows from the fact that if $n \geq 2$ one can identify 3 points, two on one line l, and a third not on l, these points cannot be collinear. □

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 it 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 can be extended in a unique way to an $(n+1)$-net of order n.*

Proof. Suppose we have an n-net of order n, N, we will define a set of n new lines that, together with N, will form the $(n+1)$-net of order n, N'. Pick a point p_1 from among the set of n^2 points in N, and define the line l_1 to be set of $n+1$ points not collinear with p_1. The next line l_2 will be constructed by picking $p_2 \notin l_1$ and taking the set of points not collinear to p_2, and so on to get a set of n lines and points $p_1, l_1, p_2, l_2, \dots, p_n, l_n$. To see that the lines are disjoint we are going to show that the relationship "$p \parallel q \iff p = q \text{ or} p \text{and} q \text{are not collinear in } N$" is an equivalence relation. Reflexivity and symmetry are clear so it just remains to show that the relationship $\parallel$ is transitive. Suppose we have three distinct points p, q, r such that $p \parallel q$, $q \parallel r$, but p and r are collinear. The net axioms guarantee exactly one line through q that is parallel to pr. 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, a contradicton since every pair of points in a net can have at most one line through them. As the relation $\parallel$ is reflexive, symmetric and transitive, it is by definition an equivalence relation. The lines $l_1, l_2, \dots, l_n$ are the equivalence classes of $\parallel$ and therefore are pairwise disjoint. Now consider a line m in the original n-net N. Each of the n points on m must lie on exactly one of the lines $l_1, l_2, \dots, l_n$, and no pair of points may lie on a line as they are collinear on m. It therefore follows that there is a bijection between the n points on m and the lines $l_1, l_2, \dots, l_n$ and so each line l_i intersects each line in the net N exactly once. So the net N', defined by adding the lines $l_1, l_2, \dots, l_n$ to N, is an $(n+1)$-net of order n. □

2 Projective Spaces and Orthogonal Hypercubes

Definition 10. *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.*

Given two latin squares we say they are *orthogonal* if when superimposing the first square over the second each of the n^2 possible ordered pair of symbols appears exactly once. A set of $M \geq 2$ of latin squares is *mutually orthogonal* it is pairwise orthogonal, this is often abbreviated to a set of MOLS of order n. Lemma answers the quesiton "What is the largest set of mutually orthogonal latin squares of 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 $1, 2, 3, \dots n$, 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 multi-set $N = \{A^1_{21}, A^2_{21}, \dots, A^{|M|}_{21}\}$. Because the symbol above A^i_{21} is fixed to one $A^i_{21} \in 2, 3, \dots, n$ 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 subset of $2, 3, \dots, n$ and $|M| = |N| \leq n - 1$. □

We call a set of $M = n - 1$ mutually orthogonal latin squares of order n a *complete set.*

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. Denote the row lines $r = \{r_1, r_2, \dots, r_n\}$ and coordinate lines $c = \{c_1, c_2, \dots, c_n\}$ respectively. Each point can be uniquely determined by the intersection of a row line and a column line, so we may coordinatise the entries of a latin square according to intersections of 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. There are n lines through L_i excluding L_∞, $S^i_1, S^i_2, \dots, S^i_n$. The latin square A^i will be constructed by letting $A^i_{x,y} = j$ if and only if the intersection point of r_x and c_y lies on S^i_j. Because each symbol line intersects each coordinate line only once, and any pair of row (column) lines cannot intersect in the affine plane, 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 superimposing the two latin squares and so the set of $n - 1$ latin squares we have defined is mutually orthogonal. □

Theorem 2 may seem redundant in light of what follows in Theorem 3, however the logic in the proof of Theorem 2 is crucial to understanding the setup for Theorem 6 later on so keep this slightly repititive thinking in mind. Theorem 3 seeks to find a constructive equivalence between a net and a set of MOLS.

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

Proof. Suppose we have a set $M = \{A^1, A^2, \dots, A^k\}$ of k MOLS of order n. Let $\mathcal{P} = \mathbb{Z}^2_n$ be a set of n^2 points. To define a $(k + 2)$-net of order n we will define $k + 2$ parallel classes of lines with points in $\mathcal{P}$. The rows and columns,

$r_i = \{(i,y) | y \in \mathbb{Z}_n\}$ and $c_j = \{(x,j) | x \in \mathbb{Z}_n\}$, form the first two parallel classes R and C respectively. For each latin square $A^i \in M$ we let $P_i = \{l_1^i, l_2^i, \ldots, l_n^i\}$ be the parallel class defined by $(x,y) \in l_j^i$ if and only if $A_{x,y}^i = j$. Clearly each pair of lines $(r,c) \in R \times C$ intersect at exactly one point. Because no position in A^i is assigned twice the lines in P_i are indeed parallel. Because each symbol j appears once in A^i for each row and column it follows that each line in P_i has n points and intersects each line in R and C just once. Let $l_j \in P_i$ and $l_k \in P_l$ for some $i \neq l$, because A^i and A^l are orthogonal there is exactly one point (x_0, y_0) such that $A_{x_0,y_0}^i = j$ and $A_{x_0,y_0}^l = k$, so the lines l_j and l_k meet at exactly one point. So we have a set of $k+2$ parallel classes of n lines containing n points meeting Definition 9 and hence the points $\mathcal{P}$ and defined in P form a $(k+2)$-net of order n.

Starting from a $(k+2)$-net of order n with points $\mathcal{P}$ and lines L, pick two distinct parallel classes $R = \{r_1, r_2, \ldots, r_n\}$ and $C = \{c_1, c_2, \ldots, c_n\}$. To coordinatise the points, let $\varphi : \mathbb{Z}_n^2 \to \mathcal{P}$ be the function defined by $\varphi(x,y) = p$ if and only $r_x \cap c_y = \{p\}$. To see that φ is one to one, suppose $\varphi(x,y) = \varphi(x',y')$ and WLOG assume $x \neq x'$ (the case $y \neq y'$ is identical), then $r_x \cap c_y = r_{x'} \cap c_{y'} = \{p\}$ which implies $r_x \cap r_{x'} \neq \emptyset$, this is a contradiction as we know these lines are parallel. Because $|\mathbb{Z}_n^2| = |\mathcal{P}| = n^2$ and φ is one to one we may also conclude φ is onto and bijective. From the remaining k parallel classes besides R and C $\{P_1, P_2, \ldots, P_k\}$, we will define a set M of k MOLS of order n, $M = \{A^1, A^2, \ldots, A^k\}$. For each of the n lines in P_i, $\{l_1, l_2, \ldots, l_n\}$, define $A_{x,y}^i = j$ if and only $\varphi(x,y) \in l_j$. Because two lines from distinct parallel classes intersect at a unique point, it follows that A^i is a latin square as each line from P_i intersect each line in R and C exactly once. A pair of distinct latin square A^i and A^l defined in this manner are also orthogonal, because two lines $l_j \in P_i$ and $l_k \in P_l$ intersect at exactly one point p, and so $A_{x,y}^i = k$ and $A_{x,y}^l = l$ intersect at exactly one point $(x,y) = \varphi^{-1}(p)$. It follows then that M is a set of k mutually orthogonal latin squares. □

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 set of $n-1$ MOLS 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 11. *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 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. We will be interested in extending the classic result given in Theorem 2, to do this we require a theorem that bounds the size of a mutually orthogonal set of hypercubes of dimension d, order n, type t and class r. In [2] we have the following theorem bounding sets of MOHC:

Theorem 5. *[2, Theorem 2.4] The maximum number of mutually orthogonal hypercubes (MOHC) of dimension d, order n, type t and class r is bounded above by*

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

A complete set of mutually orthogonal (d, n, r, t)-hypercubes is a set of MOHC attaining the bound in Theorem 5. The following theorem is a generalisation of Theorem 2 to arbitrary dimensions.

Theorem 6. *Let q be a prime power, then there exists a complete set of mutually orthogonal $(d, q, 1, d-1)$-hypercubes.*

Proof. Let q be a prime power, and let $X = \{e_1, e_2, \ldots, e_d\}$ where $e_i = (0, 0, \ldots, 1, 0, \ldots, 0)_q$ is a point in $\mathrm{PG}(d, q)$ whose homogeneous coordinates have a 1 in the ith position and zero everywhere else. Define H_∞ to be the hyperplane at infinity in $\mathrm{PG}(d, q)$. By removing some $e_i \in X$ from X we get a subset S of $d-1$ points in X that spans a codimension 2 space contained in H_∞. Furthermore there are q hyperplanes through S apart from H_∞. These planes are defined by the equations $x_i X_i + X_{d+1}$ and $X_i = 0$. The q hyperplanes through the projective span of some subset S of X we will call coordinate hyperplanes. Let D be a set of d coordinate hyperplanes through the projective span of d codimension 2 spaces with basis $X \setminus \{e_i\}$ for each $i \in \{1, 2, \ldots, d\}$. To show that these hyperplanes intersect at a single affine point construct the homogeneous system of linear equations $A\mathbf{x} = \mathbf{0}$ where,

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

Where $\alpha_l = 0$ if the hyperplane it describes is defined by the equation $X_l = 0$ and $\alpha_l = 1$ otherwise. This matrix has rank d and hence $A\mathbf{x} = \mathbf{0}$ a single projective point as a solution, namely $(\alpha_1 x_1, \alpha_2 x_2, \ldots, \alpha_d x_d, 1)$, and this proves the claim that the intersection of the hyperplanes in D is a single affine point in $\mathrm{PG}(d, q)$. We will now coordinatise the points of the affine space in terms of the intersection of coordinate hyperplanes through the d codimension 2 spaces with basis $X \setminus \{e_i\}$ for each $i \in \{1, 2, \ldots, d\}$. Our analogue to symbol planes in Theorem 5 will be symbol hyperplanes whose intersection with the hyperplane at infinity does not include X. Let H be the set of codimension 2 spaces in H_∞ not containing X. These hyperplanes are described by systems of equations $X_{d+1} = 0$ and $c_1 X_1 + c_2 X_2 + \cdots + c_d X_d = 0$ with each $c_i \neq 0$, and hence there are $\frac{(q-1)^d}{q-1} = (q-1)^{d-1}$ hyperplanes in H_∞ not intersecting X at any point.

Let $\mathcal{H} = \{H^1, H^2, \ldots, H^{(q-1)^{d-1}}\}$ be a set of $q \times q \times \cdots \times q$ (d times) arrays. To define $\mathcal{H}^i$ one considers all q hyperplanes $S_1, S_2, \ldots, S_n$ through some codimension 2 space in the set H and let $\mathcal{H}^i_{(x_1, x_2, \ldots, x_d)} = j$ if and only if $(x_1, x_2, \ldots, x_d, 1) \in S_j$. We must show that these arrays are a complete set of MOHC. Taking any hyperplane through any of the planes in $\mathcal{H}$ gives us a hyperplane of the form $c_1 X_1 + c_2 X_2 + \ldots + c_d X_d + c_{d+1} X_{d+1} = 0$, with each c_i non-zero (to avoid including one of the basis vectors). We can now consider its intersection with $d-1$ coordinate planes (describing a $(d-1)$-subarray), 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,

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

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 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 and thus that any 1-subarray in a cube H^i will contain each of the q symbols exactly once, and hence that H^i is a hypercube. Picking two symbol hyperplanes from two distinct hypercubes H_i and H_j their intersection is a $(d-2)$-dimensional space with $\sum_i^{d-2} q^i - \sum_i^{d-3} q^i = q^{d-2}$ affine points, so H_i and H_j are orthogonal.

By Theorem 5, the maximum number of mutually orthogonal $(d, q, 1, d-1)$-hypercubes is $(q-1)^{d-1}$, so $\mathcal{H}$ is a complete set of mutually orthogonal $(d, n, 1, d-1)$-hypercubes. □

Theorem 6 has been proven elsewhere in literature, notably in [5] (albeit a slight generalisation is given there). Mullen and Laywine use polynomials of the form $f_{a_1,a_2,\ldots,a_d}(x_1,x_2,\ldots,x_d) = a_1x_1 + a_2x_2 + \ldots a_dx_d$, with at least two a_i nonzero, to define a complete set of mutually orthogonal $(d,n,1,0)$-hypercubes. The polynomials for which all a_i is nonzero are precisely the hyperplanes not through X given in Theorem 6. The remaining polynomials correspond to hyperplanes that intersect with one or more of the basis points in X. Whilst this proof was found indepedently of Laywine and Mullen, we have shown it is the same as what they end up with.

It would be nice if, like in the two dimensional case, the existence of a complete set of $(d,n,r,0)$-hypercubes implied the existence of a projective space PG(d,n), however [6] suggests that without further restrictions of the hypercubes chosen we cannot construct the right geometry.

3 Mutually Orthogonal Soduku

Soduku are a special case of latin squares, an object we have already discussed. A soduku of order n^2 is a latin square of order n^2 with the property that each $n \times n$ subsquare has each symbol exactly once. Because soduku are latin squares the definition of orthogonality for latin squares is equally valid for soduku. However soduku differ from latin squares in terms of how many orthogonal soduku one can have, as the following lemma demonstrates.

Lemma 14. *If M is a set of k mutually orthogonal soduku latin squares (MOSLS) of order n^2, then $k \leq n^2 - n$*

Proof. Suppose we have a set $M = \{S^1, S^2, \ldots S^k\}$ of k soduku of order n, and WLOG assume that the first row of symbols in each soduku in M are such that the first row is given by $1, 2, \ldots, n^2$. Now consider how many possible symbols we may pick for the entry (2, 1) of each soduku. For each soduku we have a choice of one of q^2 symbols, of which $1, 2, \ldots n$ are forbidden as they are in the first subsquare of the soduku. If for some $i \neq j$ we have $S^i_{2,1} = k = S^j_{2,1}$ then S^i and S^j are not orthogonal because $S^i_{1,k} = k = S^j_{1,k}$ so no $k \leq q^2 - q$. □

As we saw in Theorem 4 it is always possible to extend a set of $n-2$ MOLS of order n to a set of $n-1$ MOLS of order n. The natural extension of Theorem **??** would be something like the following,

Conjecture 2. *For $n \geq 2$, if there exists a set M of n^2-n-1 MOSLS of order n^2, then there exists an extension of M to a complete set of $n^2 - n$ MOSLS of order n^2*

However Conjecture 2 is not true, and in fact it's not even true for the nicest cases (the prime powers). In [1], Theorem 7 was shown with a constructive proof.

Theorem 7. *Let $q > 3$ be a prime power, then there exists a maximal set of $q^2 - q - 1$ MOSLS of order q^2.*

The proof of this makes use of a correspondence between a soduku latin square of order q^2 for prime powers q and the projective space $\mathrm{PG}(4, q)$. The $q^2 \times q^2$ array $A = (a_{ij})$ is coordinatised by identifying the position (i, j) in A with the projective point with homogeneous coordinates $(1, a, b, c, d)_q$, where $1 \leq a, b, c, d \leq q$ are integers (mapped to $\mathbb{F}_q$) such that $i = (a-1)q + b$ and $j = (c-1)q + d$. In this way each affine point of $\mathrm{PG}(4, q)$ corresponds to a unique position in A. Soduku latin squares of the *parallel type* are defined by taking a line l in H_∞ skew to three chosen lines, $R : x_0 = x_1 = x_2 = 0$, $C : x_0 = x_3 = x_4 = 0$ and $S : x_0 = x_1 = x_3 = 0$ and assigning each of the q^2 symbols to the positions corresponding to each of the affine points on each of the q^2 planes through the line l. In [1] this was shown to always give a soduku latin square. Orthogonal sets of parallel soduku correspond to sets of skew lines in H_∞. So to find a maximal set of $q^2 - q - 1$ MOSLS of order q^2, we actually find a maximal partial spread of $q^2 - q - 1$ lines skew to R, C and S. We then need to check that there are no other extensions possible that are not parallel.

Finding the correct partial spread turns out to be a complicated endeavour, but using GAP [3] soduku were constructed that meet the criteria laid out in [1]. In Figure 1 five soduku of order $q^2 = 9$ are constructed using the techniques outlined in [1].

To verify that the set of mutually orthogonal soduku in Figure 1 are not extendable, a constraint satisfaction problem solver was employed. Constraint satisfaction problem solvers take in a set of constraint on a defined set of variables and attempts to find any assignments to the set of variables that satisfy all the given constraints. In this case, the set of variables are the positions of the final soduku, and the constraints are the soduku latin square constraints plus all the orthogonality constraints implied by the other soduku latin squares. The particular solver chosen was Minion [4], for its fast and scalable constraint solver with particular emphasis on its table based constraints. Not only can minion show that indeed there are no extensions of the soduku given in Figure 1, but in Figure 2 we have a near miss, an orthogonal array that satisfies the subsquare and column constraints but not row constraints of a soduku. In terms of near miss soduku, Figure 2 is probably the closest one can come to extending the orthogonal set.

1	2	3	4	5	6	7	8	9
8	9	7	2	3	1	5	6	4
6	4	5	9	7	8	3	1	2
2	3	1	5	6	4	8	9	7
9	7	8	3	1	2	6	4	5
4	5	6	7	8	9	1	2	3
3	1	2	6	4	5	9	7	8
7	8	9	1	2	3	4	5	6
5	6	4	8	9	7	2	3	1

1	2	3	4	5	6	7	8	9
4	5	6	7	8	9	1	2	3
7	8	9	1	2	3	4	5	6
9	7	8	3	1	2	6	4	5
3	1	2	6	4	5	9	7	8
6	4	5	9	7	8	3	1	2
5	6	4	8	9	7	2	3	1
8	9	7	2	3	1	5	6	4
2	3	1	5	6	4	8	9	7

1	2	3	4	5	6	7	8	9
9	7	8	3	1	2	6	4	5
5	6	4	8	9	7	2	3	1
7	8	9	1	2	3	4	5	6
6	4	5	9	7	8	3	1	2
2	3	1	5	6	4	8	9	7
4	5	6	7	8	9	1	2	3
3	1	2	6	4	5	9	7	8
8	9	7	2	3	1	5	6	4

1	2	3	4	5	6	7	8	9
6	4	5	9	7	8	3	1	2
8	9	7	2	3	1	5	6	4
5	6	4	8	9	7	2	3	1
7	8	9	1	2	3	4	5	6
3	1	2	6	4	5	9	7	8
9	7	8	3	1	2	6	4	5
2	3	1	5	6	4	8	9	7
4	5	6	7	8	9	1	2	3

1	2	3	4	5	6	7	8	9
5	6	4	8	9	7	2	3	1
9	7	8	3	1	2	6	4	5
3	1	2	6	4	5	9	7	8
4	5	6	7	8	9	1	2	3
8	9	7	2	3	1	5	6	4
2	3	1	5	6	4	8	9	7
6	4	5	9	7	8	3	1	2
7	8	9	1	2	3	4	5	6

Figure 1: Five MOSLS of order $q^2 = 9$ that cannot be extended to six MOSLS of order 9.

1	2	3	1	2	3	1	2	3
4	5	6	4	5	6	4	5	6
7	8	9	7	8	9	7	8	9
8	9	7	8	9	7	8	9	7
2	3	1	2	3	1	2	3	1
5	6	4	5	6	4	5	6	4
6	4	5	6	4	5	6	4	5
9	7	8	9	7	8	9	7	8
3	1	2	3	1	2	3	1	2

Figure 2: A near miss extension of the MOSLS in Figure 1

References

[1] Jozefien D'haeseleer, Klaus Metsch, Leo Storme, and Geertrui Van de Voorde. "On the maximality of a set of mutually orthogonal Sudoku Latin Squares". In: *Designs, Codes and Cryptography* 84.1 (July 2017), pp. 143–152. ISSN: 1573-7586. DOI: `10.1007/s10623-016-0234-3`. URL: `https://doi.org/10.1007/s10623-016-0234-3`.

[2] John T. Ethier, Gary L. Mullen, Daniel Panario, Brett Stevens, and David Thomson. "Sets of orthogonal hypercubes of class r". In: *Journal of Combinatorial Theory, Series A* 119.2 (2012), pp. 430–439. ISSN: 0097-3165. DOI: `https://doi.org/10.1016/j.jcta.2011.10.001`. URL: `https://www.sciencedirect.com/science/article/pii/S0097316511001609`.

[3] *GAP – Groups, Algorithms, and Programming, Version 4.11.0.* The GAP Group. 2020. URL: `https://www.gap-system.org`.

[4] Ian Gent, Christopher Jefferson, and Ian Miguel. "Minion: A Fast Scalable Constraint Solver." In: vol. 2006. May 2006, pp. 98–102.

[5] Charles F. Laywine and Gary L. Mullen. *Discrete mathematics using Latin squares.* Wiley-Interscience Series in Discrete Mathematics and Optimization. A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York, 1998, pp. xviii+305. ISBN: 0-471-24064-8.

[6] Ilene H. Morgan. "Complete sets of mutually orthogonal hypercubes and their connections to affine resolvable designs". In: *Ann. Comb.* 5.2 (2001), pp. 227–240. ISSN: 0218-0006. DOI: `10.1007/s00026-001-8009-5`. URL: `https://doi.org/10.1007/s00026-001-8009-5`.