The what, how and why of Finite projective planes

Markus Höglin

August 2021

Contents

Abstract

This thesis defines the finite projective plane and the affine projective plane. A method of construction is defined for the field planes by extension of the affine plane constructed from the vector space over a finite field. The thesis explores for which orders planes can and cannot be constructed, in particular, for the prime powers there exist planes. For n=6 a computer search is conducted using a recursive algorithm, which shows that $n = 6$ is not possible as an order for finite projective plane. The thesis then illustrates an application for finite projective planes in the form of a threshold scheme for secret sharing.

Acknowledgements

I would like to express my deepest gratitude to my supervisor,
prof. Victor Ufnarovski for introducting me to the interesting and multifaceted field of finite projective planes, for his guidance and for his boundless patience.

1 Introduction

1.1 Euclidean geometry

Geometry has formed one of the most central fields of mathematics for millenia, it has been explored across countless civilizations, whether it be for architecture, art or physics. At heart of geometry lies one of the most important sets of axioms, Euclid's axioms of geometry:

- E_1. For any two distinct points, there exists a unique line joining them.
- E_2. A straight line can be prolonged indefinitely.
- E_3. A circle can be constructed when radius and center are given.
- E_4. All right angles are equal.
- E_5. For any line l and point p not on this line, there exists a unique parallel line l' through the p which does not intersect the l.

The geometry defined by these axioms is known as "Euclidean" geometry and is exactly what most people think of when they think of the word "geometry": circles, points with lines inbetween them, lines either intersect in one point or are parallel and never intersect. This Euclidean geometry is ubiquitous to our understanding of the world we inhabit, but is it enough? To answer this question, we must turn to a type of geometry inherent to the way we perceive the world: Projective geometry.

1.2 Projective geometry

We can imagine standing between train tracks which stretch to the horizon. When looking straight down, we can recognize familiar shapes from euclidean geometry, we have lines which are parallel that have a constant distance between them, lines which are not parallel intersect and then diverge. We then look up towards the horizon, and see a very different sight. Lines which were just parallel now converge to a point on the horizon, and lines which are not parallel converge to different points. No matter how far we walk along the tracks, the lines will keep a constant distance and be parallel when looking straight down, but will converge to the same point on the horizon.

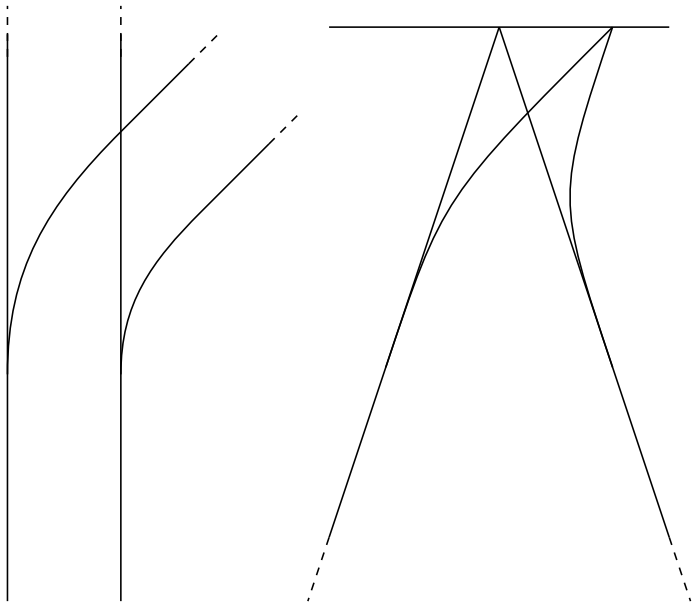

Figure 1: Euclidean and projective train tracks

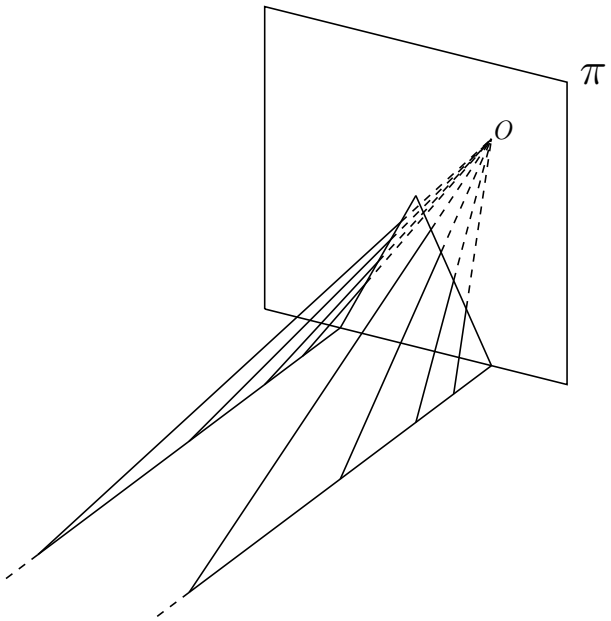

Figure 2: Image projected onto the retina

What has happened is that the image of the train tracks that we can see is created by a projection and obeys projective geometry, rather than Euclidean geometry. Projective geometry was first developed by artists who were searching for techniques for depicting three dimensional objects on a flat plane. The artists had run into the same issue, depicting lines which are parallel in the real world as parallel on a flat surface looks nothing like something which would exist in real world.

We must instead turn to projective geometry which disregards Euclid's fifth axiom, the parallel postulate. In projective geometry, lines cannot be parallel and always intersect at exactly one point. Using this, the Euclidean plane can then be extended to the projective plane by adding a line at infinity, a "horizon" which contains points where parallel lines meet.

Going back to the train tracks, just as artists project three dimensional objects onto surfaces when drawing in perspective, so also does the human eye. We can imagine an idealised human eye as a plane π, as the retina, and a point O as the pupil. An image in the eye is then created when rays of photons are projected through the pupil, onto the retina.

This thesis will present a specific type of projective geometry: the finite projective plane. This type of plane obeys the axioms of projective geometry and only has a finite number of points, unlike the usual idea of a plane. This gives the finite projective plane some unique properties, it is ideal for study using finite fields and algebraic geometry, the specific structure derived from the axioms of projective geometry also yields distinctive combinatorial features. The finite projective plane as a consequence, has applications in for example cryptography and combinatorics.

Finite projective planes, despite following a rather short set of axioms do not have much know about them and are very hard to find, unless specific circumstances are met. Not only are they hard to find, but we do not know even whether they are possible or impossible to create outside these circumstances. The main purpose of this thesis is exploring this question: for which cases is it possible to construct planes and how, as well as proving a specific case as impossible for a plane by a computer search. The thesis also seeks to cultivate a general understanding for these structures by using graphical tools in order to support a visual intuition of these rather abstract objects, as well as by showcasing a potential application in secret sharing.

The primary sources for the theory of finite projective plane in this thesis is Hall, M. (1967). *Combinatorial theory* as well as Dembowski, P. (1968). *Finite Geometries*, proofs of theorems were completed or extended from shorter proofs in these books.

2 Finite Projective Planes

2.1 Definition

A finite projective plane is, as the name suggest a 2-dimensional projective geometry with a finite number of points and lines. Rather than being innately tied to some graphical representation, these geometries are primarily defined axiomatically, through the relation between two "primitive elements". These primitive elements can for example be points and lines but can also be something completely different, this makes the finite projective plane a very flexible structure.

Definition 2.1[Hall, M. (1,p. 173)]: The axioms for projective geometry, when applied to finite projective planes and with *points* and *lines* as primitive elements are as follows:

- A_1. There is one and only one line containing two distinct points.
- A_2. There is one and only one point on two distinct lines.
- A_3. There exists a set of four points, such that no three are on a line.

One can observe that the first two axioms are identical statements with *points* and *lines* interchanged, that is to say they are the *"dual"* of one another, with respect to points and lines. The dual A_3^*, of the third axiom on the other hand, can be shown as a consequence of the other ones. The axioms A_3, A_3^* serve the purpose of disqualifying *"degenerate"* planes, which are too simple to be of interest.

- A_3^*. There exists a set of four lines, such that no three contain the same point.

This *duality* gives a powerful symmetry between points and lines, which are functionally identical.

Theorem 2.2[Hall, M. (1,p. 173)]: A geometry satisfying A_1, A_2, A_3, satisfies A_3^*.

Proof. A_3 gives that there exist four points $1, 2, 3, 4$ where no three have a line in common. The axiom A_1 therefore gives that we can define lines containing the six combinations of any two of these points:

$$\{1, 2, ...\}, \{1, 3, ...\}, \{1, 4, ...\}, \{2, 3, ...\}, \{2, 4, ...\}, \{3, 4, ...\}$$

A_2 requires that each pair of lines have a unique point in common. Using this we define α, β, γ as the points of intersection, of the lines which do not have one of the points $1, 2, 3, 4$ in common:

$$\{1, 2, \alpha, ...\}, \{1, 3, \beta, ...\}, \{1, 4, \gamma, ...\}, \{2, 3, \gamma, ...\}, \{2, 4, \beta, ...\}, \{3, 4, \alpha, ...\}$$

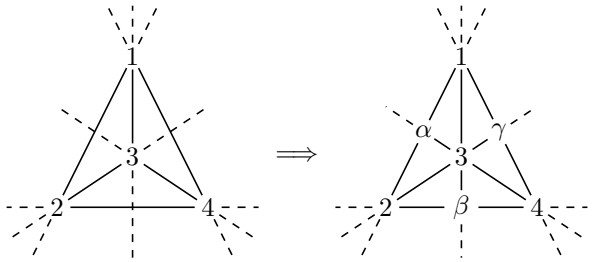

Figure 3: Lines joining $1, 2, 3$ and 4, intersecting in α, β, and γ

We can also define three lines using A_1, joining the points α, β, and γ. These three lines are not necessarily distinct however, as α, β, and γ may all have a single line in common.

$$\{\alpha, \beta, ...\}, \{\alpha, \gamma, ...\}, \{\beta, \gamma, ...\}$$

We can now pick four lines such that no three have a point in common, we begin by picking the lines which join three of the points 1,2,3 and 4. There cannot be any more points in common between these lines, besides the ones defined here, as all points share a line. This means that we can add to these three lines, one of the lines joining α, β, and γ, this line cannot contain any of the points 1,2,3 and 4.

No point lies on more than two of these lines, and so this is a set of four lines, such that no three have a point in common, showing that A_3^* holds. Creating such a set of lines by picking the lines between 1,2 and 3 as well as the line containing α and β yields the following:

$$\{1, 2, \alpha, ...\}, \{1, 3, \beta, ...\}, \{2, 3, \gamma, ...\}, \{\alpha, \beta, ...\}$$

□

We can observe that a plane with fewer than three points on it's lines is an example of a *degenerate plane*, which is too small to be of interest and is disqualified by A_3 and A_3^*. This is the case as some lines joining the points 1,2,3 and 4 could not possibly have any point in common, and so would not fulfill A_2.

Given these axioms, there are some fundamental properties one can show for finite projective planes. One important property is the number of points on a line, lines containing a point, the total number of points in the plane and the relation between these. To this end, these properties are shown for a finite projective plane which is assumed to have a line with $n+1$ points. Building on this we then define "*order*", a natural notion to classify finite projective planes.

Theorem 2.3[Hall, M. (1,p. 173)]: If a finite projective plane contains a line with exactly $n+1$ points, then every line contains exactly $n+1$ points, every point is on exactly $n+1$ lines and in total there are n^2+n+1 points and lines each in the plane. Conversely, if there are n^2+n+1 points and lines in a plane, then every point is on $n+1$ lines and every line contains $n+1$ points.

Proof. Let L_0 be a line containing exactly $n+1$ points, A_3 gives that there exists a point $p \notin L_0$. The point p is on the $n+1$ lines $pp_j : p_j \in L_0$. These lines are all distinct, if there were some line containing two distinct points of L_0 then both points would be contained by two distinct lines, breaking A_1.

These lines are the only lines through p, if there existed another line $L^* : p \in L^*$, then in order to not break A_2 this line needs to contain one of the points of L_0. L^* containing one of the points of L_0, leads to this point being on two distinct lines with p, breaking A_1. It has been shown that any point not on L_0 is on exactly $n+1$ lines.

Starting instead with a point p_0 on $n+1$ lines, by A_3^* there exists some line $L : p_0 \notin L$. There are $n+1$ points on the line L, determined by the intersections of the lines $l : p_0 \in l$ with L, using the previous argument showing that any point not on L_0 is on exactly $n+1$ lines, we can show that any line not through p_0 contains exactly $n+1$ points.

Now, to show that every line contains $n+1$ points we have to find three points that do not lie on the same line which are all on $n+1$ lines. Given such a configuration, every line must not through one of these points, and would therefore contain $n+1$ point. To find such a set of lines we begin by observing that A_3 guarantees that there exists at least two points α and β, not on L_0, we then let ξ and η be two points on L_0.

There are $n+1$ lines through α and β, the only line which could possibly not contain $n+1$ points is the line $\alpha\beta$, which is through both points. We can observe however, that the line $\alpha\xi$ is not through β and must contain $n+1$ points, the point η which is not on $\alpha\xi$ must then also have $n+1$ lines through it. The point η is not on $\alpha\beta$, so this line, and every line must contain $n+1$ points. The fact that every point is on $n+1$ points also follows from this argument, as we found three lines with $n+1$ points, not through a single point.

Since every two points in the plane are on one line and only one line, this gives that every point is on one of the $n+1$ lines p_0 is on. Knowing that every line contains exactly $n+1$ points, each line contains n points distinct from p_0. As a result, the plane has $n(n+1)+1 = n^2+n+1$ points in total, repeating this argument for L_0 in place of p_0 yields that the plane also has n^2+n+1 lines in total.

To show the converse we suppose that there is a plane with a line containing $k+1$ points and $k^2+k+1 = n^2+n+1$, this only has solution $k=n$ in the positive integers and so a plane with n^2+n+1 points and lines must have that every line contains $n+1$ points, every point is on $n+1$ lines. $\square$

Using these results we define a finite projective plane of order n as such a plane that has a line that contains $n+1$ points and so, every line contains $n+1$ points, every point is contained by $n+1$ lines, and so on.

Definition 2.4[Hall, M. (1,p. 175)]: Let $n > 1$ be an integer, a finite projective plane is said to be of order n if a line contains exactly $n+1$ points.

The finite projective plane has now been defined and some elementary properties have been shown, but this does not answer the question whether such a plane even exists or how to construct it. In order to answer this, we will explore how and when finite projective planes can be contructed.

Since the definition would lose any usefulness if it is not possible to construct what it defines, we will attempt to see if there exists any finite projective plane. We can note that a plane of order $n = 1$ would have 3 points, and would not fulfill A_3 and therefore $n = 1$ does not produce a plane. The plane of order $n = 2$ does not immediately break any axioms and could be a valid order for a plane. For plane of order 2 there are not many points, so it is not difficult to check manually that there exists a plane P(2).

Recalling that in a plane of order n, every line contains exactly $n+1$ points, every point is exactly on $n+1$ lines and the plane has n^2+n+1 lines and points in total.

So, P(2) has 7 points and lines in total with 3 points contained by a line and a point is on 3 lines. We can recall the geometry created for the proof of theorem 2.2, this geometry can be extended to define P(2).

This geometry contains 7 points and 6 lines, each of the points 1,2,3 and 4 have exactly one line in common with every other point, the lines between these points also have exactly one point in common. This means that we can define a line which contains each of the points α, β, and γ to get 7 lines. Adding this lines gives that each point has exactly one line in common, and since each other line contains exactly one of α, β, and γ, each line also has exactly one point in common.

Completing the geometry in this way yields the following:

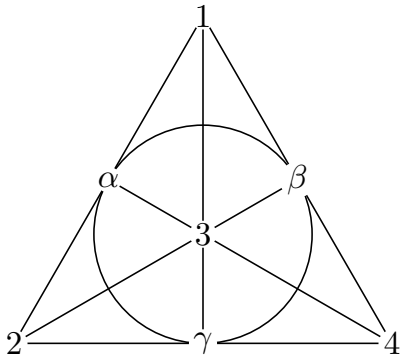

Figure 4: P(2)

This is the smallest possible finite projective plane, which is known as the Fano plane. This also illustrates the fact that lines in a finite projective plane do not need to be straight.

Since we have now found that there exists a plane P(2), we can now continue exploring when there exists a plane by increasing the order to 3. While it is possible to manually construct the planes for very small orders such as 3, it quickly becomes unfeasible. Here one solution for P(3) is presented, while why we can arrange points and lines in this particular way to create a finite projective plane, will be shown later. The plane P(3) must have 13 points and lines, so we define it by arranging the points $p_1, ..., p_{13}$ into lines in the following way:

$$\{p_1, p_2, p_3, p_{12}\}, \{p_4, p_5, p_6, p_{12}\}, \{p_7, p_8, p_9, p_{12}\}$$

$$\{p_1, p_5, p_9, p_{11}\}, \{p_3, p_4, p_8, p_{11}\}, \{p_2, p_6, p_7, p_{11}\}$$

$$\{p_1, p_6, p_8, p_{13}\}, \{p_2, p_4, p_9, p_{13}\}, \{p_3, p_5, p_7, p_{13}\}$$

$$\{p_1, p_4, p_7, p_{10}\}, \{p_2, p_5, p_8, p_{10}\}, \{p_3, p_6, p_9, p_{10}\}$$

$$\{p_{10}, p_{11}, p_{12}, p_{13}\}$$

So, the plane exists for both order 2 and 3, the plane that was created now, P(3) can be graphed as follows:

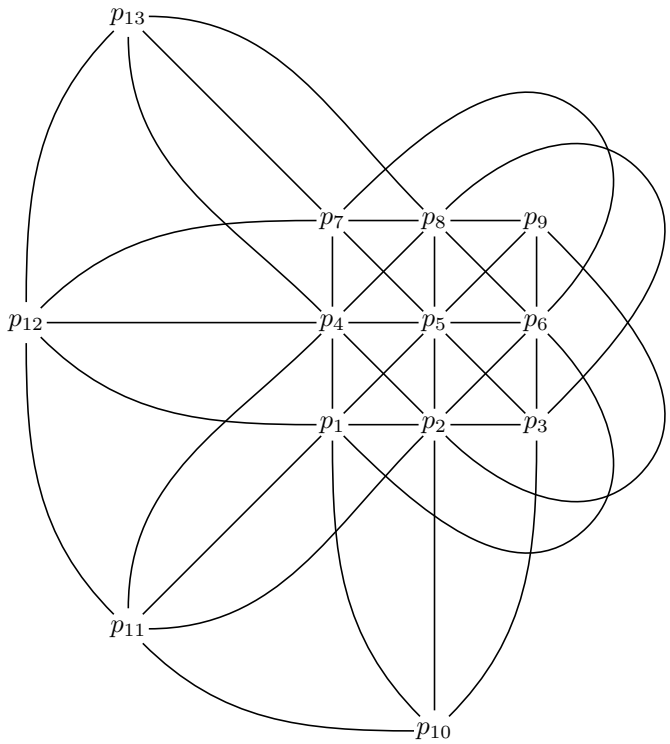

Figure 5: P(3)

2.2 Constructing field planes

We have now shown that there exists a projective plane for both order 2 and 3, so we know that there exists planes for some n at least, but does there exist some plane for finitely many n, infinitely many n or perhaps for every n? Manually creating the plane of order n by trying to combine the points into lines by following the axioms also becomes increasingly unfeasible. To solve this, we will define a general method of construction for a specific class of finite projective planes.

To define this system we shall first define another concept, the affine plane denoted as A(n). Just like the projective plane, the affine plane has an order n and can be obtained from the projective plane of the same order. For a projective plane of order n, if a line L_∞ *"at infinity"* is removed along with removing the points on this line from every other line the affine plane of the same order is obtained.

This plane has $n^2 + n$ lines and n^2 points, the removal of L_∞ creates $n + 1$ sets of n lines with no points in common, corresponding to the set of lines through a given point on L_∞. Using this structure inherited from the projective plane we can define the affine plane.

Definition 2.5[Dembowski, P. (2,p. 115)]: The affine plane with *points* and *lines* as primitive elements is a geometry satisfying the following axioms:

- AG_1. There is one and only one line containing two distinct points.
- AG_2. For a line and a point not on it, there is one and only one line with no point in common to the first that contains the point. Two such lines are referred to as being "*parallel*", this relation is transitive: if l_1 is parallel to l_2, and l_2 to l_3 then l_1 is parallel to l_3.
- AG_3. There exist three points which are not on a line.

Theorem 2.6[Dembowski, P. (2,p. 117)]: Any finite projective plane can be restricted to an affine plane by removing a line and all points on it, inversely any affine plane can be extended to a projective plane by adding a line at infinity to it, and points at infinity to each family of parallel lines.

Proof. Let π_p and π_a be projective and affine planes. We let π_p^* be π_p with a line L_∞, along with it's points removed. Each point in π_p is on $n+1$ lines and each pair of lines both contain one and only one point. When L_∞ is removed from π_p, for each of the $n+1$ points in L_∞ a family of n mutually parallel lines is created from the lines that had that point in common.

Each family contains each point once and each pair of lines from different families have one and only one point in common. Picking a line l and a point p not on that line, each line containing p from another family will have some point in common with l, while the line of the same family containing p has no points in common with l, AG_2 is valid for π_p^*.

For AG_1 we can observe that none of the points of π_p^* were on L_∞, so the line connecting any pair of points in π_p^* is also in π_p^*, AG_1 is valid for π_p^*.

Finally, for AG_3 we use the set of four points $1, 2, 3, 4$, no three on a line given by A_3, as well as the points α, β, γ connecting the lines defined by the pairs of $1, 2, 3, 4$ with no point in common.

$$\{1, 2, \alpha, ...\}, \{1, 3, \beta, ...\}, \{1, 4, \gamma, ...\}, \{2, 3, \gamma, ...\}, \{2, 4, \beta, ...\}, \{3, 4, \alpha, ...\}$$

From these lines, any can be removed along with it's points and there still exists three points where no three are on a line. So π_p^* is an affine plane by these axioms.

We now let π_a^* be the affine plane with a line added to it, and each point of this line added to every line in a parallel family of π_a.

Now to show that any affine plane can be extended to a projective plane, we observe that the line defined by a pair of points p_ip_j must be one of the lines, or parallel to a unique line through a point p_0. If this pair of points p_ip_j does not define a line through p_0, then there must be a unique line p_0p^* parallel to it which contains p_0. p_ip_j will then define the unique line parallel to p_0p^*, through any point of p_ip_j. We can now divide all lines of π_a into families of parallel lines, for each line p_0p_i we define the family F_i by p_0p_i and all lines parallel to this line through all points not on it.

No pair of lines in a given family have any points in common, as p_0p_i would not have a unique parallel through this point. Each point in the plane is contained on a unique line of each family and each line in the plane is contained in a unique family as the line defined by any two points which is parallel to a unique line through p_0. A pair of lines with a line parallel to both are also parallel as this line would have multiple parallels through the point which the pair has in common, this gives that every pair of lines from different families have a unique point in common.

We now define a new line L_∞ with one point for each family, and to each line in a parallel family we add a point of L_∞. By doing this, each pair of lines meet in a unique point, and each pair of points are on a unique line. This means that π_a^* fulfills A_1 and A_2, for A_3 we add L_∞ to the three points given by AG_3:

$$\{1, 2, \alpha, ...\}, \{1, 3, \beta, ...\}, \{2, 3, \gamma, ...\}, \{\alpha, \beta, \gamma, ...\}$$

From these points, one can pick four such that none are on the same line, π_a^* fulfills A_3 and so is a projective plane. □

It is quite easy to see this extension in figure 5, for P(3) where the square of nine points is the affine plane A(3) and the line $\{p_10, p_{11}, p_{12}, p_{13}\}$ is the line added to create the projective plane.

Through extension of the affine plane, we can define a general method of construction for a large set of projective planes: the field planes.

Theorem 2.7[Hall, M. (1,p. 177)]: There exists a finite projective plane for every prime power order, $n = p^k$.

To prove this, we define and prove the construction of the affine plane for $n = p^k$:

This construction of the affine plane of order $n = p^k$ resembles the euclidean plane in many ways. We begin by constructing a vector space V over the finite field of order $n = p^k$:

$$V = \mathbb{F}_{p^k}^2$$

The points and lines of the affine plane can now be defined inside this vector space, just as in the euclidean plane:

$$a, b, c \in \mathbb{F}_{p^k} \quad x, y \in V$$

$$\begin{aligned} p &\iff (x, y) \\ l &\iff ax + by = c \end{aligned}$$

In this construction, a point is defined as a vector (x, y) of V and a line as a particular linear equation in V defined by the scalars a, b, c, and the solution set for (x, y) representing the point contained by this line. We should note however, that two different sets of scalars a', b', c' can represent the same line if $ka = a'$, $kb = b'$, and $kc = c'$, $k \neq 0$. To circumvent this, lines can instead be defined as equivalence classes of equations:

$$l \iff [a, b, c] = \{kax + kby = kc : \forall k \in \mathbb{F}_{p^k} \setminus \{0\}\}$$

At this point, we can also note that $[0, 0, c]$ is an invalid line as this does not have a solution set.

For the sake of intuition, we can use this to redefine l in terms of the usual equation for a line in the euclidean plane. Given that $b \neq 0$, we can always multiply by $k^{-1}b^{-1}$, as all non-zero elements have inverses in a field. We can then set $\alpha = -b^{-1}a$, and $\beta = b^{-1}c$:

$$\begin{aligned}(x,y) \in l &\iff kax + kby = kc \\ &\iff b^{-1}ax + y = b^{-1}c \\ &\iff -\alpha x + y = \beta \\ &\iff y = \alpha x + \beta\end{aligned}$$

In this view, we can see that a line can be defined by a slope α and a constant term β. This holds under the assumption that $b \neq 0$, when $b = 0$ however, we can multiply by $k^{-1}a^{-1}$ and set $a^{-1}c = \beta$. In this case the line is equal to some constant β with respect to x:

$$\begin{aligned}l &\iff kax + kby = kc \\ &\iff kax = kc \\ &\iff x = \beta\end{aligned}$$

Using this concept of slope, we can define the parallel families of lines in an intuitive way as sets of lines with equal slope, just as in the euclidean plane.

$$(a', b') = (ka, kb) \iff a'b'^{-1} = ab^{-1}$$

To conclude the construction of the affine plane, we can define the set of points $\mathcal{P}$ and the set of lines $\mathcal{L}$ and so, the plane π_a:

$$\begin{gathered}\mathcal{P} = \{(x,y) \in V\} \\ \mathcal{L} = \{[a,b,c] : a,b,c \in \mathbb{F}_{p^k}\} \setminus \{[0,0,c]\} \\ \pi_a = \mathcal{P} \cup \mathcal{L}\end{gathered}$$

We can now move on to show that this construction defines an affine plane, proving theorem 2.7:

Proof. To begin, we can simply show that this gives the correct number of points and lines. We can see that for the set of points that there are n^2 vectors $(x, y) \in \mathbb{F}_n^2$, which is the number of points in $\mathrm{A}(n)$.

Computing the total number of equivalence classes gives that the number of lines is:

$$\frac{n^3 - n}{n - 1} = n^2 + n$$

n^3 possible permutations of $[a, b, c],\ a, b, c \in \mathbb{F}_n$, n invalid permutations $[0, 0, c]$ and $n - 1$ lines in each equivalence class, the number of lines in $\mathrm{A}(n)$.

To show AG_1 we must show that there is exactly one line between a pair of points. We begin by showing that there is some line between any two points: we let $(x_1, y_1) \neq (x_2, y_2)$ be two distinct points, the line connecting two points (x_1, y_1) and (x_2, y_2) is equal to the following system of equations.

$$\begin{aligned} l : (x_1, y_1), (x_2, y_2) \in l &\iff \begin{cases} kax_1 + kby_1 = kc \\ kax_2 + kby_2 = kc \end{cases} \\ &\implies ax_1 + by_1 = ax_2 + by_2 \\ &\iff a(x_2 - x_1) = -b(y_2 - y_1) \end{aligned}$$

$$\begin{aligned} x_2 - x_1 \neq 0 &\implies a = -b(y_2 - y_1)(x_2 - x_1)^{-1} \\ &\implies -kb(y_2 - y_1)(x_2 - x_1)^{-1}x_1 + kby_1 = kc \\ k = b^{-1} \implies l &\iff -(y_2 - y_1)(x_2 - x_1)^{-1}x + y = -(y_2 - y_1)(x_2 - x_1)^{-1}x_1 + y_1 \\ &\iff (y - y_1) = (y_2 - y_1)(x_2 - x_1)^{-1}(x - x_1) \end{aligned}$$

$$\begin{aligned} x_2 - x_1 = 0 &\implies 0 = b \\ &\implies kax_1 = c \\ &\implies l \iff x = x_1 \end{aligned}$$

We find that a line containing both (x_1, y_1) and (x_2, y_2) yields a unique solution for $[a, b, c]$ exactly when these two points are distinct, and so there is exactly one line containing both points.

Now, to show AG_2 we have to show that for any line l and a point, there exists a unique parallel line l' which contains the point and does not intersect l. We begin by letting $l,\ l'$ be two distinct lines and (x, y) the intersection between the two lines. We then use systems of linear equations and the fact that these have a unique solution exactly when it's determinant is non-zero:

$$\begin{aligned} l &\iff ax + by = c \\ l' &\iff a'x + b'y = c' \end{aligned}$$

$$\begin{aligned} (x, y) \in l, l' &\iff \begin{cases} ax + by = c \\ a'x + b'y = c' \end{cases} \\ &\iff \begin{bmatrix} a & b \\ a' & b' \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} c \\ c' \end{bmatrix} \end{aligned}$$

$$\begin{aligned} \exists!(x, y) : (x, y) \in l, l' &\iff \begin{vmatrix} a & b \\ a' & b' \end{vmatrix} \neq 0 \\ &\iff ab' - a'b \neq 0 \\ &\iff (a', b') \neq (ka, kb) \end{aligned}$$

We find the intersection has a unique solution for (x, y) exactly when the determinant is non-zero and so, the lines have a unique solution when they are not parallel. When the determinant is zero however, we can see that the lines have (x, y) in common only if $l = l'$. We can therefore use the fact that distinct parallel lines have no intersection, and now need to show that for any line there exists a unique parallel line which contain any point not on it.

To complete the proof of AG_2, we must show that there exist, for every line l and point (x, y) not in l a unique parallel line l' which contains the point:

$$\begin{aligned} l &\iff ax + by = c \\ l' &\iff ax + by = c' \end{aligned}$$

$$(x, y) \notin l, (x, y) \in l' \iff \begin{cases} ax + by = \gamma \neq c \\ ax + by = c' \end{cases}$$

$$\implies l' \iff [a, b, \gamma]$$

We can see here that there exists a unique parallel line l', which contains the point (x, y) and has no points in common with l.

Finally, to prove AG_3 we can pick the three points $(0, 0),\ (1, 0),\ (0, 1)$ these points will always exist as 0 and 1 are included in all fields:

$$l \iff ax + by = c$$

$$\begin{aligned} (0,0), (1,0), (0,1) \in l &\iff \begin{cases} a0 + b0 = c \\ a1 + b0 = c \\ a0 + b1 = c \end{cases} \\ &\iff \begin{cases} 0 = c \\ a = c \\ b = c \end{cases} \end{aligned}$$

$$\implies l \iff [0, 0, 0]$$

This is not a valid solution for a line, so these three points are not on a line. This concludes the proof as all axioms of affine planes hold for this construction. $\square$

We have now defined a general method of construction of an affine plane over a field, this affine plane can then be extended to a projective plane. We have found as a result that there exist planes for all prime power orders, as there exist finite fields for all prime power orders.

The affine plane is extended to a projective plane as defined in theorem 2.6: a new line with $n+1$ points is added, each point is added to every line in one of the parallel families. The way this can be done is quite arbitrary, one simple way is to add a line containing the points $(0), (1), ..., (n), (\infty)$. The point (k) is added to the parallel family with slope α, that is to say $\{ax + by = c : ab^{-1} = \alpha\}$. The point (∞) is added to the family with "infinite" slope where x is constant, $\{ax = c\}$.

We can also extend the affine plane in a way that connects to the projective nature of the plane, we view the affine plane as a plane, π in $\mathbb{F}^3$ disjoint from the origin. We view the points and lines as the projection of one- and two-dimensional subspaces through the origin onto the π. To extend the affine plane to the projective plane we add points and a line at infinity, these are the one- and two-dimensional subspaces through the origin parallel to π. Picking $\pi \iff z = 1$ we can see that the equation for a line and plane through the origin in $\mathbb{F}^3$ reduces to that of lines and points which we defined:

$$ax + by + cz = 0 \overset{z=1}{\iff} ax + by + c = 0$$
$$(x, y, z) \overset{z=1}{\iff} (x, y, 1)$$

The line at infinity is then defined as $z = 0$ and points at infinity as the unique one-dimensional subspaces obtained from $k(x, y, 0)$.

Using this extension in a vector space means that we can create a representation of the plane in $\mathbb{F}^3$. For the smaller planes, this can give a good visual intuition of the relation between the affine, and projective plane and for finite projective planes as a whole. To this end we create such a representation of P(3) where each parallel family of lines in A(3) has been assigned a color to make them distinguishable:

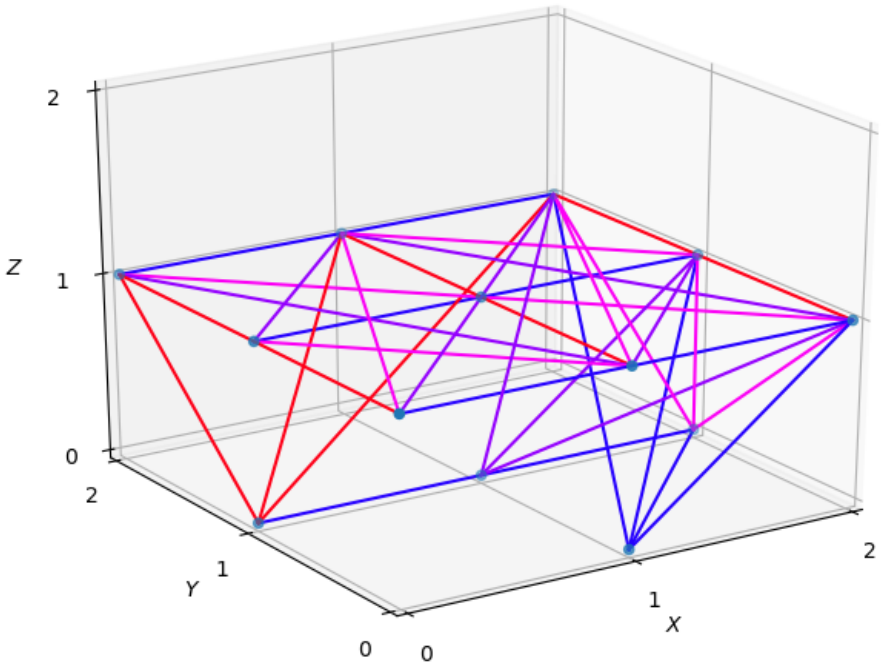

Figure 6: P(3) in $\mathbb{F}^3$

Here we can see the affine plane at $z = 1$ and the line at infinity at $z = 0$.

While it can be difficult to connect the intuition of adding points at infinity to families of parallel lines in the affine plane to the graphs, as the lines which are parallel sometimes cross each other. This is due to the modular arithmetic of fields, this means a line loops back to $y = k$ when it reaches $y = np + k$. Here it is useful to instead imagine the affine plane as F_p^2 tiled indefinitely, here we let the line go to $y = k$ of the next tile instead of looping back. When viewing A(3) like this we can see that parallel lines all have the same slope, and never cross:

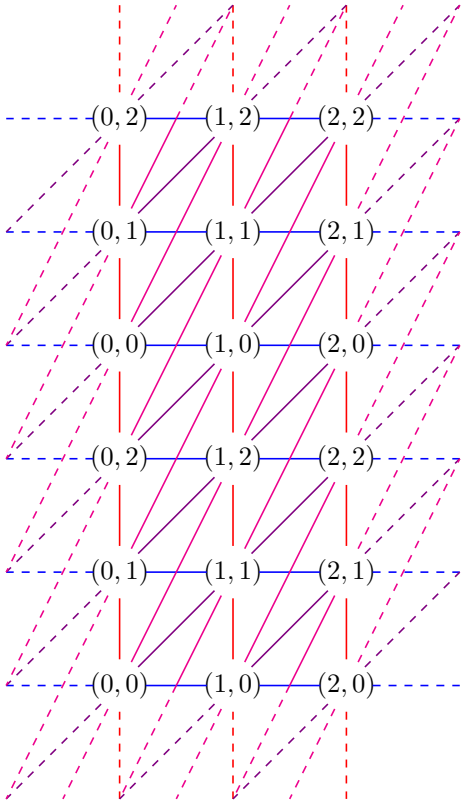

Figure 7: A(3)

We can now use this method of extending affine planes to create the finite projective planes for the next two orders, $n = 4, 5$ and for all prime power orders $n = p^k$. Starting by picking the next prime, we will try to construct the plane of order 5 over the vector space $\mathbb{F}_5^2$:

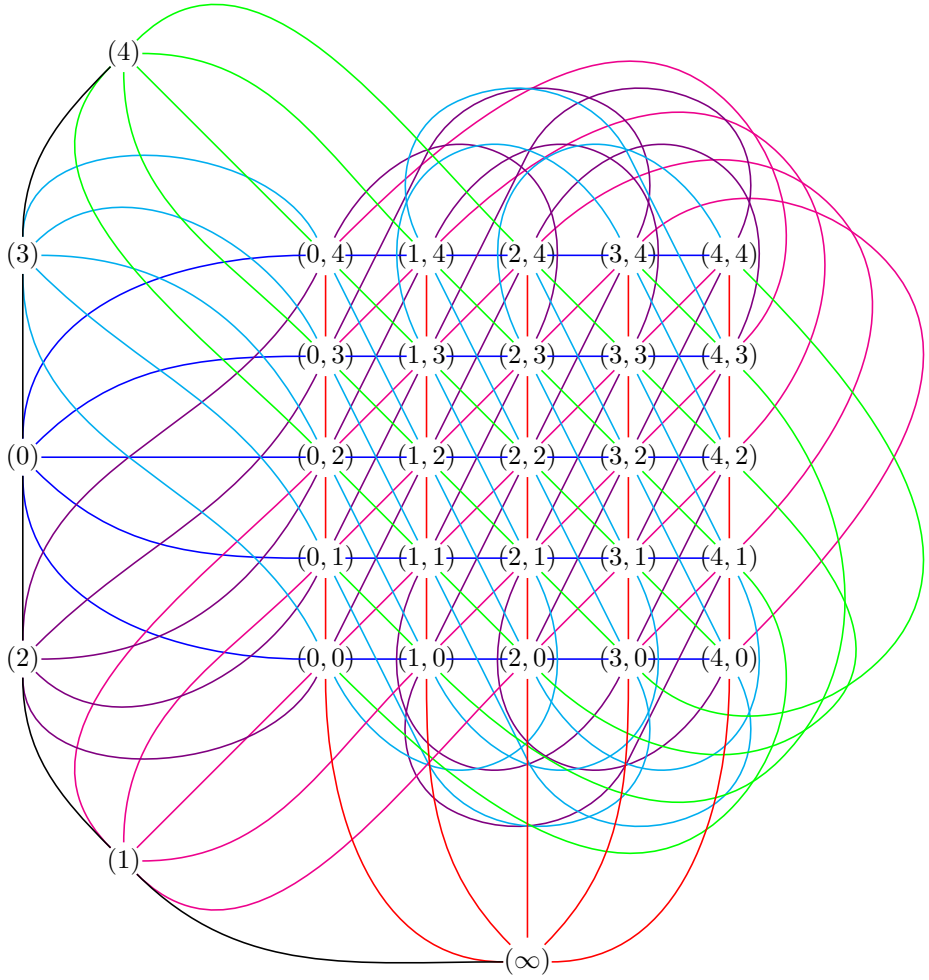

Figure 8: P(5)

We will now create the plane for the first prime power p^k where $k > 1$, once again we can obtain this plane by construction over the vector space $\mathbb{F}_4^2$. This case however differs somewhat from the previous cases where the orders are p, as these planes are the integers with multiplication and addition modulo p. For the prime power fields, the elements are polynomials with multiplication and addition modulo some irreducible polynomial of order k over $\mathbb{F}_p$. Picking the polynomial $X^2 + X + 1$ over $\mathbb{F}_2$ and defining "a" as a root of this polynomial in $\mathbb{F}_4$ yields the following multiplication:

$\times$	0	1	a	$a+1$
0	0	0	0	0
1	0	1	a	$a+1$
a	0	a	$a+1$	1
$a+1$	0	a+1	1	a

We then use this operation in the vector space, with the scalar field $\mathbb{F}_4 = \{0, 1, a, a+1\}$ to create the projective plane of order 4. In the graph we let $a + 1$ be denoted by b in order to save space, constructing the plane using this we obtain:

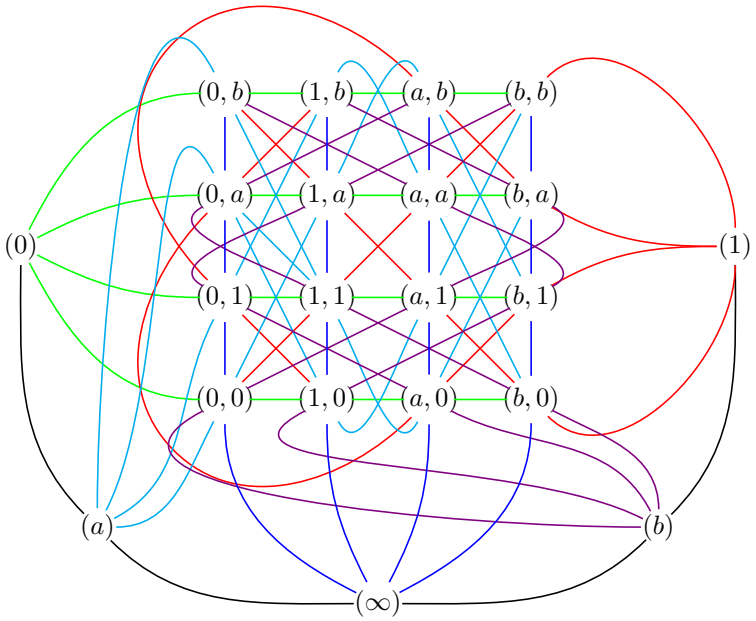

Figure 9: P(4)

2.3 Isomorphic planes

We have now constructed finite projective planes for a few orders and found an infinite class of planes. So we now have a basis to explore the algebraic structures of these planes. To begin studying these structures, we will define "*incidence preserving maps*" of geometries. These serve as useful tools for generalising the structures of planes.

We let a geometry of points and lines V be defined by a triple $V = (\mathcal{P}, \mathcal{L}, \mathcal{I})$. Here $\mathcal{P}$ is the set of points of V, $\mathcal{L}$ the lines and we have that the $(p, l) \in \mathcal{I}$, for $p \in \mathcal{P},\ l \in \mathcal{L}$ if the point p lies on the line l and. We call this relationship $(p, l) \in \mathcal{I}$ "*incidence*", where $\mathcal{I}$ is the set of incidences of points and lines.

We let $V = (\mathcal{P}, \mathcal{L}, \mathcal{I}),$ and $W = (\mathcal{P}^*, \mathcal{L}^*, \mathcal{I}^*)$ be two such sets of points and lines, we are interested in finding mappings $\phi : V \to W$ which preserve the structure of V.

Such a mapping ϕ, which preserves structure can be defined as a mapping where the following relation holds:

$$(p, l) \in \mathcal{I} \implies (\phi(p), \phi(l)) \in \phi(\mathcal{I})$$

We can now define some properties which determine different types of such a mapping ϕ defined by Dembowski, P.[2,p. 8].

$$\phi : \mathcal{P} \to \mathcal{P}^*,\ \mathcal{L} \to \mathcal{L}^* \tag{1}$$

$$\phi : X \to \mathcal{P}^*, Y \to \mathcal{L}^* \implies \phi(X) = \mathcal{P}^*,\ \phi(Y) = \mathcal{L}^* \tag{2}$$

$$(p^*, l^*) \in \mathcal{I}^* \implies (\phi^{-1}(p^*), \phi^{-1}(l^*)) \in \phi^{-1}(\mathcal{I}^*) \tag{3}$$

$$\phi : V \to V \tag{4}$$

For such a mapping ϕ, we can classify it based on which of the relations $(1), (2), (3), (4)$ hold. A mapping ϕ, fulfilling (1) is a "*Homomorphism*", a mapping fulfilling $(1), (3)$ is an "*Epimorphism*", a homomorphism where the image of $\mathcal{P}$, $\mathcal{L}$ under ϕ is equal to $\mathcal{P}^*,\ \mathcal{L}^*$ respectively. A one-to-one mapping ϕ fulfilling $(1), (2), (3)$ is an "*Isomorphism*", a one-to-one epimorphism, which preserves structure under inversion. An isomorphisms which fulfills (4), mapping V to itself, is an "*Automorphism*".

From these mappings we can find useful ways of classifying and relating different finite projective planes. We can say that two planes V, W are isomorphic if there exists an isomorphism between them, this means that the incidences of the primitive elements of the planes are structurally identical.

This a vital tool for answering several important questions regarding these planes. Isomorphisms can be used to determine whether the field planes we've created uniquely determine the projective plane of their respective order. We can see that a geometry failing to satisfy the axioms of a projective plane, means also that any isomorphic geometries also fail. This can be used when searching for finite projective planes as only structurally distinct geometries have to be searched.

3 Existence of planes of order n

One of the most important questions regarding finite projective planes is that of the existence of planes of order n. This question has been alluded to throughout this thesis, and will be explored more thoroughly in this section. One of the most important tasks of this thesis, was creating a program which can find any plane of any order. The section will thus be concluded with a section on a computer search undertaken in order to determine the uniqueness of the solutions that we have already found using fields, and to determine the existence and non-existence of a non-prime plane.

There is very little known about the existence of P(n) for an arbitrary order n, so far we can only say with certainty that there exist planes for the orders $n = p^k,\ k > 1$ when p is a prime. This is due to the construction defined over a field, since there exists a finite field for all prime power orders.

3.1 The finite projective plane of order 6

The first order which is not included in the prime power planes is the plane of order 6, P(6). This plane is therefore the first whose existence we are not able to determine as of yet. This was an important open problem in finite geometry, until it was showed by Raj Chandra Bose in 1938 that the existence of the plane of order 6 implied the "thirty-six officers problem". The thirty-six officers problem is the combinatorial problem of arranging officers from six regiments and six ranks, one officer of each rank from each regiment, in a 6×6-square such that each column and each row contains exactly one officer of each rank, and one from each regiment, this had been proven impossible and so P(6) must not exist.

3.1.1 Orthogonal latin squares

This connection between the thirty-six officers problem and finite projective planes is the equivalence of a P(n) to a set of $n-1$ "*orthogonal latin squares*". These latin squares are $n \times n$ arrays of n symbols such that each row and each column contains each symbol exactly once. Two latin squares are orthogonal if each pair of symbols appear exactly once when superimposed, and a set of latin squares is orthogonal if each square in the set is mutually orthogonal.

To illustrate, we'll explore a solution to a hypothetical "nine officers problem", where one square is representing the red, green and blue regiments with the colors $\{R, G, B\}$ and the other representing ranks with the numbers $\{1, 2, 3\}$. This gives a solution to the problem, where the nine officers are represented with a rank and a regiment in the third square created by superimposing the first two.

$$\begin{array}{|ccc|} \hline 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \\ \hline \end{array} \quad \begin{array}{|ccc|} \hline R & G & B \\ B & R & G \\ G & B & R \\ \hline \end{array} \quad \Longrightarrow \quad \begin{array}{|ccc|} \hline 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \\ \hline \end{array}$$

Having defined the latin square, we can move on to showing the connection between the squares and the finite projective plane.

Theorem 3.1[Hall, M. (1,p. 177)]: Each projective plane is equivalent to a set of $n-1$ orthogonal latin squares.

Proof. To show the connection between the latin squares and the finite projective plane, it is useful to recall the affine form of a finite projective plane and the extension of the $n+1$ parallel families of an affine plane to the projective one. Here we pick two families which are denoted as $F_c,\ F_r$, the other families are denoted as $F_1, F_2, ..., F_{n-1}$. The families F_c and F_r will essentially serve as indices for the latin squares while each family F_k serves as a latin square. This is accomplished by letting the entry in the i-th column and j-th row of a latin square associated with the family F_k be ξ if the intersection of the i-th line of F_c and j-th line of F_r is on the ξ-th line of F_k.

Using the properties of affine planes we can show that this construction is equivalent to an $n-1$ set of orthogonal latin squares. Each line in a parallel family of lines in an affine plane intersects each line in every other family exactly once, furthermore each pair of points is contained in exactly one line. We can see from this that for any given family, we can create a latin square as two points on the same line ξ in F_k will not be on the same line in either F_c or F_r and therefore ξ will never appear twice in a given column or line.

Let (ξ, η) be a pair from the latin squares created from these two families, if (ξ, η) is found in multiple indices, then this would imply that the points represented by those indices are all contained by both the ξ-th line of the first family and the η-th line of the second, which breaks the axioms of an affine plane. So we have that any pair of squares constructed in this manner will be orthogonal. Finally, since there are $n+1$ parallel families in total and two of these fill the role of F_c and F_r, this leaves a total of $n-1$ orthogonal latin squares.

To show the converse we must show that a set of $n-1$ orthogonal latin squares satisfies the axioms of an affine plane. We first define two indexing families of parallel lines, F_c and F_r, we let the index ij in the latin squares define the point at the intersection of the i-th line of F_c and j-th line F_r. Each latin square then represents a family of parallel lines, where an ξ in the k-th latin square indicates that the point at this index is on the ξ-th line of F_k.

To show AG_1, we must then show that there is a line from the point at the index ij to any other index ij^*. We begin by denoting the entry at ij in each family by ξ, the two points being on the same line would mean that the entry at ij^* also is ξ. We recall that each symbol must be in each row and each column exactly once, and also that squares must not have duplicate pairs of symbols when superimposed. This means that if the two indices lie on the same row or column, then none of the squares can have ξ at both indices these two points would then be on one of the lines of F_c of F_r. If the indices are not on the same row or column however, we see that there are $n-1$ possible indices to enter ξ in the i^*-th column. This means that exactly one square must have ξ at the index ij^* since there are $n-1$ squares in total, and none of the squares can have ξ at the same index, this means that there is exactly one line between two points.

To show AG_2, we simply observe that each point is contained by exactly one line in a parallel family, since each index in a square has exactly one entry. We also have the for the squares to be orthogonal, a line must intersect each line in every other parallel family exactly once. This means that for a line and a point not on it, there exists exactly one parallel line which contains the point.

Finally, to show AG_3 we can pick the points at the indices (1,1), (1,2) and (2,1), these indices cannot all contain the same symbol, as each row and each column must contain each symbol exactly once. □

This result is a powerful tool for determining the existence of finite projective planes. The equivalence of a projective plane to a set of mutually orthogonal latin squares enables the use of results on latin squares to be used when constructing projective planes. While also providing a natural setting for algorithmic construction of projective planes.

We can use orthogonal latin squares together with isomorphisms to provide a simple generalisation of the structure of a set of orthogonal latin squares and so, also the structure of finite projective planes. This general form of a set of orthogonal latin squares is know as the *"standard form"* of such a set:

Theorem 3.2[Hall, M. (1,p. 178)]:

1. Applying a row or column permutation on each square in a set of orthogonal latin squares yields an isomorphic set of orthogonal latin squares.
2. Replacing the k symbols of any square in a set of orthogonal latin squares with k new symbols yields an isomorphic set of orthogonal latin squares.
3. Any set of k orthogonal latin squares is isomorphic to a set of orthogonal latin squares in standard form: where the first row of each square is $\{1, 2, ..., k\}$ and the first column of exactly one square is $\{1, 2, ..., k\}$.

Proof. We can begin by observing that the ordered pairs of of elements created by the i-th and j-th column or row of each square in a set of orthogonal latin squares remain unchanged. This gives that the mappings π_r and π_c defined by $\pi : i \to j,\ j \to i,\ k \to k,\ k \neq i, j$ are isomorphisms, using composition this can be extended to any permutation of rows or columns applied to each square in the set.

Similarly, the pairs of any two latin squares A and B when superimposed can be given by:

$$\{(a_i, b_j) : a_i \in \alpha, b_j \in \beta\}$$

This will be the cartesian product of the sets of symbols of the two squares, A and B when the squares are orthogonal. Mapping the symbols
$a_i \to a_i^*,\ a_i \in \alpha,\ a_i^* \in \alpha^*$ gives the that the latin squares A^* and B yield the pairs $\{(a_i^*, b_j) : a_i^* \in \alpha^*, b_j \in \beta\}$ when superimposed, this set is the cartesian product of α^* and β exactly when A and B are orthogonal. So this mapping preserves the orthogonality, and these two sets of latin squares are also isomorphic as the mapping $a_i \to a_i^*$ is an isomorphism.

Finally, the third statement is simply a matter of combining the first two. Using the fact that we can replace the symbols of any square in the set independently of the other, we can pick a mapping of the symbols of each square such that the first row is mapped to $\{1, 2, ..., k\}$. Then we pick one of the squares to which we will apply a permutation to the $2, ..., k$-th rows of this square such that the row with j as it's first symbol is permuted to the j-th row. This is only possible to do for one square as any other square containing j as the entry in the first column and the j-th row would mean that the set of squares would have the pair (j, j) multiple times. □

we can now illustrate the construction of an affine plane using latin squares. For $n = 3$ construct a set of 2, 3×3 orthogonal latin squares, to construct a plane from these we define the lines of F_r and F_c.

We can for instance, define F_r and F_c as follows:

$$F_r = \{\{p_1, p_2, p_3\}, \{p_4, p_5, p_6\}, \{p_7, p_8, p_9\}\}$$

$$F_c = \{\{p_1, p_4, p_7\}, \{p_2, p_5, p_8\}, \{p_3, p_6, p_9\}\}$$

The lines of F_1 and F_2 are then defined by the two latin squares, where ${}_il_j$ is the j-th line of the i-th family:

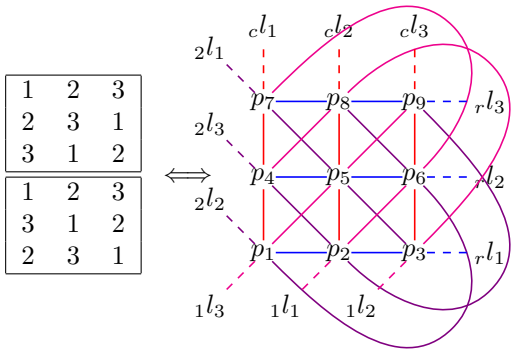

Figure 10: P(3) from latin squares

3.1.2 Computer search for plane of order $n = 6$

We can now use these results to construct any plane without using a field. By iterating through every possible configuration of $n-1$ orthogonal latin squares, we can determine the existence and uniqueness of any plane. This means that constructing a set of 5 6×6 latin squares would mean proving the existence of the plane of order 6, while showing the impossibility of this proves it's non-existence.

For small planes it is not very difficult, however as the order increases this quickly becomes unfeasible as the number of possible configurations becomes very large. To overcome this we must reduce the number of cases by excluding configurations without loss of generality, this can be achieved by excluding only configurations which are isomorphic to some configuration still included in the search.

The first method of managing the number of cases is by putting the latin squares in to standard form. The second method is by utilising a search algorithm which extends the partially completed configuration in steps. The search extends the partial solution either until completed or until it is conclusively impossible to complete to a full set of orthogonal latin squares, at which point any configuration which could be extended from this one can be disregarded.

The method used for the computer search for finite projective planes in this theses is a recursive search algorithm, which ranges over all possible configurations. The algorithm will be briefly outlined here:

The algorithm first checks whether an exit condition is true, whether the algorithm has been able complete all squares. If this condition is true, the algorithm appends this solution to a list of solutions. If the exit condition is not true, then the solution is complete, the algorithm then checks and saves all the pairs that were added by the previous step in the algorithm, then searches the possible columns which can be added. The method used for determining which columns can be used is only allowing columns which do not break latinity of the square or orthogonality of the set of squares. The algorithm will then call itself recursively for each possible column, and then removes the column and pairs added by it's children and finally ends the function call. The algorithm is written in python using the numpy library, the code for the algorithm is included in the appendix.

Starting out with the smaller planes in order to determine the uniqueness of the solutions for $n = 2, 3, 4, 5$, we get that the solutions for $n = 2, 3$ are unique trivially as there exists only one set of orthogonal latin squares in standard form for these orders. For $n = 4, 5$ there exist multiple solutions, however using the operations which leave the squares structurally identical: permuting rows and columns of all squares, changing the symbols of any square we can determine that all solutions are isomorphic.

Finding all solutions for the orders $n = 2, 3, 4, 5$ was done in less than a second each. Moving on to $n = 6$, however the computer search took roughly 1300 seconds, or roughly 21 minutes and 40 seconds. The search yielded no solutions, which means that it is impossible to construct a set of 5 6×6 orthogonal latin squares, and so also impossible to construct a finite projective plane of order 6, the algorithm was not able to create even a single pair of orthogonal latin squares. This means also that the problem of arranging the 36 officers has no solution.

3.2 n=10

While there is very little that can be said in general about the existence of finite projective planes, however there exists one such theorem, the Bruck-Ryser theorem:

Theorem 3.3[Hall, M. (1,p. 175)]: A necessary condition for the existence of a finite projective plane of order n is that for $n \equiv 1, 2 (\text{mod } 4)$, then n is the sum of two squares.

This rules out an infinite set of orders, however also leaves an infinite set undetermined. This result rules out the order $n = 6$, which was proven by computer search in the preceding section. The next possible order for a plane is then $n = 10 = 1^2 + 9^2$, this order was only shown to be impossible in 1989, after an intensive computer search by C. W. H. Lam, L. Thiel and S. Swiercz.

The next order $n = 12 \equiv 0 (\text{mod } 4)$ is, as of writing, still undetermined.

4 Applications

While finite projective planes have been mostly theoretical objects so far, it has applications in several fields. It primarily finds use due to its unique combinatorial and geometric propeties, one such application of finite projective planes, and finite projective spaces in general is in the field of secret sharing. Secret sharing refers to schemes where a secret is split into "shares" and distributed in such a way that the secret can be reconstructed with a certain combination of shares.

The value of such a scheme is easy to see, one can imagine for example a bank manager. The bank manager carries the key which accesses the bank's important documents and capital, which are necessary for daily operations. However, the manager often needs to leave the bank and is then faced with a troublesome decision. The manager either shuts down operation at the bank or entrust one of their employees with the key, which could lead to the key falling into the wrong hands.

This underlines two common use cases for secret sharing: need for access which is controlled but independent of the scheme creator and the need for distributing risk. The bank manager could either mitigate or avoid this dilemma altogether by using a secret sharing scheme. One such type of secret sharing scheme is the (k,n)-threshold scheme where the secret is split into n shares, any k out of the n shares can be used to reconstruct the secret.

Projective planes are well suited for implementation in secret sharing schemes in many cases, this due both to their combinatorial and geometric structure. In the case of the bank manager we can construct a threshold scheme where any two participants can gain access, rather than just one. This would allow access when the manager is away while not giving any one person unrestricted access, reducing risk of misuse considerably.

To create this (2,n)-threshold scheme which is outlined by Beutelspacher, A. and Rosenbaum, U. [3,p. 236], we create the finite projective plane P(n). In this plane we pick a line l_p, the *public* line which is released publicly, on l_p we pick a point $S \in l_p$ as the secret. We then pick a line l_h, the *hidden* line, which intersects l_p in S: $l_p \cap l_h = s$, any of the n points $\sigma_1, ..., \sigma_n$ on l_h apart from S can then be used as a share. The secret, S can then be reconstructed by determining l_h, using any two shares and then finding the intersection of l_h and l_p.

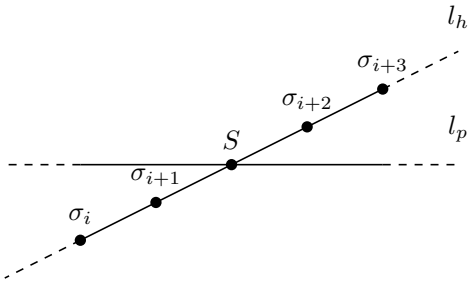

Figure 11: A (2,n)-Threshold scheme

This secret sharing scheme lets the bank manager generate shares equal to any prime power and then give one share to each person in some group of trusted senior employees. This scheme, like any other security system is not impossible to break, but rather serves to mitigate risk and make attacks too costly to be worthwhile. To know the strength of this scheme we can determine the likelihood of an attacker being able to guess the solution without any keys. Since l_p was released to the public, the attacker's best strategy is to guess one of the $n + 1$ points on l_p, this gives a $\frac{1}{n+1}$ chance at guessing S without any shares. A desirable property of this scheme is that possessing only one share gives no additional information regarding S

We can construct planes for any prime power, and we can therefore make guessing the secret arbitrarily difficult by picking a large power of some prime. We can for example pick $n = 2^i$, to make a scheme where the shares are easily represented in binary, and pick the largest possible i without making the shares use too many bits.

References

[1] Hall, M. (1967). *Combinatorial theory*. Waltham, Mass : Blaisdell Pub. Co

[2] Dembowski, P. (1968). *Finite Geometries*. Springer Berlin Heidelberg

[3] Beutelspacher, A. & Rosenbaum, U. (1997). *Projective Geometry: From Foundations to Applications* . Cambridge university press

A Appendix

```
import time as time
import numpy as np
import itertools as it


n = 6
F = np.arange(1,n+1,1,dtype = 'uint8')


Cols = np.array(list(it.permutations(F, n-1)))
idnt = np.identity(n-1)
ColDict = {}
for i in range(n):
    for j in range(n-1):
        ColDict[(i+1,j+1)] = np.invert(np.any((i+1)*idnt[j] == Cols,axis=1))


I = np.stack((np.tile(F,(n,1)).transpose().flat,np.tile(F,(n))))
MOLS = np.vstack((I,np.zeros((n-1,n**2),dtype = 'uint8')))
MOLS[2:,:n] = np.tile(F,(n-1,1))
MOLS[2,:][MOLS[1,:] == 1] =  F
MOLS = MOLS.transpose()


F2 = np.arange(n+1,dtype='uint8')+1
pairIdx = np.array(list(it.combinations(F2,2)))
checkMatrix = np.zeros((int((n*(n+1))/2),n,n),dtype='uint8')
PairDict = {tuple(pairIdx[i]): checkMatrix[i] for i in range(int((n*(n+1))/2))}
PairDict[(1,2)][:,:] = 1
for key in pairIdx[np.any(pairIdx == 1,axis = 1)]:
```

```
    PairDict[tuple(key)][0,:] = 1
for key in pairIdx[np.all(pairIdx != 1,axis = 1)]:
    PairDict[tuple(key)][F-1,F-1] = 1


Soln = []
idx1 = np.array(np.meshgrid(F,0)).transpose().reshape(n,2)-1
def PairCheck(A,i,j):
    PrevCols = (A[F[:-1]*n+F.reshape(-1,1)[j]-1,:i+1]).transpose()
    a = np.take(PrevCols, idx1[:i+1,:], 0).transpose(0,2,1)[:-1]-1
    for k,v in enumerate(a):
        PairDict[(k+1,i+1)][v[:,0],v[:,1]] = 1
    return a

def ColumnSearch(A,i,j):
    PrevCols = (A[(F[:-1])*n+F.reshape(-1,1)[j]-1,:i]).transpose()
    Bool = []
    for k,v in enumerate(PrevCols):
        a = np.take(PairDict[(k+1,i+1)],v-1,0)
        Bool=Bool+[ColDict[(I[1]+1,I[0]+1)]
                   for I in np.array(np.where(a)).transpose()]
    return Cols[np.logical_and.reduce(Bool)]

def Recursion(A,I,k,N):
    if k >= N:
        Soln.append(np.copy(A[:,2:]).transpose().reshape(n-1,n,n))
        return
    else:
```

```
            a = PairCheck(A,I[k,0],I[k,1])
            v = ColumnSearch(A,I[k+1,0],I[k+1,1])
            for i in v:
                A[(F[:-1])*n+F.reshape(-1,1)[I[k+1,1]]-1,I[k+1,0]] = i.transpose()
                Recursion(A, I, k+1, N)
            A[(F[:-1])*n+F.reshape(-1,1)[I[k+1,1]]-1,I[k+1,0]] = 0
            for K,v in enumerate(a):
                PairDict[(K+1,I[k,0]+1)][v[:,0],v[:,1]] = 0
            pass

RecursionIndex = np.fliplr(np.array(
                    np.meshgrid(F-1,F[1:])).reshape(2,n*(n-1)).transpose())
N = RecursionIndex.shape[0]-1

start = time.time()
Recursion(MOLS,RecursionIndex,0,N)
Soln = np.array(Soln)
for i in range(len(Soln)):
    print(Soln[i],"\n\n")
print('Time elapsed:',time.time()-start)
```