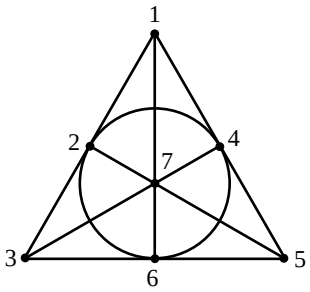
C-UPPSATS 2002:02

TFM,
851 70 Sundsvall

Mid Sweden University
Tel: 060-14 86 00

# On Projective Planes




The Fano plane, the smallest projective plane.

**By Johan Kåhrström**

**Abstract**

It was long an open question whether or not a projective plane of order 10 existed. It has now been shown, using a computer search, that no projective plane of order 10 exists. This essay introduces the concept of projective planes, and then looks at some of the theory on the existence of certain projective planes. It concludes with a look at the computer search for a projective plane of order 10, and some of the theory behind it.

# Contents

# Acknowledgement

I would like to thank Pia Heidtmann for all her help and support, and for putting up with me taking up much more of her time than I was supposed to (when her time often should have been spent on marking exams). I am also very thankful for her suggestion on the topic for this essay. I had only a vague idea of what I wanted to do, and I feel that projective planes is about as close to this idea as is possible to come.

# Chapter 1

# Introduction - Projective Planes

This essay will give an introduction to a special kind of geometry called a projective plane. In the first two chapters we define projective planes, and go through some of their most important properties. The last two chapters will look at existence questions regarding the finite projective planes. In particular, the last chapter looks at how it was shown that a certain finite plane does *not* exist.

Projective planes are a special case of a more general structure called a *geometry*. As geometries have more in common with our intuitive notion of geometry, we shall start by looking at these.

## 1.1 Geometries

**Definition 1 (Geometry).** *A* **geometry** $S = (P, L)$ *is a non-empty set* $P$ *whose elements are called* **points**, *together with a set* $L$ *of non-empty subsets of* $P$ *called* **lines** *satisfying:*

$G1$: *For any two distinct points* $p_1, p_2 \in P$, *there exists exactly one line* $l \in L$ *such that both* $p_1 \in l$ *and* $p_2 \in l$.

$G2$: *There exists a set of four points, such that given any set of three of these points, no line exists that contains all three points.*

Note that the sets $P$ and $L$ may be either finite or infinite. We say that a point $p$ is *on*, or *incident with*, a line $l$ if $p \in l$. Similarly a line $l$ is *on*, or *incident with*, a point $p$ if $p \in l$. A set of points is called *collinear* if there exists a line such that all points are on the line. If $p$ and $q$ are two points, then $pq$ denotes the unique line on both $p$ and $q$. Obviously, $qp = pq$. If $l_1$ and $l_2$ are lines that intersect in a point, $l_1 l_2$ denotes their point of intersection.

Using this notation, we can write $G1$ and $G2$ in a more straightforward way:

$G1$: Two distinct points are on exactly one line.

$G2$: There exists a set of four points, no three of which are collinear.

A set of four points, no three of which are collinear, is called a *quadrangle*. A line through two points of a quadrangle is called a *diagonal* of the quadrangle.

**Example 2** This first example will assure us that the Euclidean plane is indeed a geometry. Here, $P$ consist of the usual points, and $L$ of the usual lines. It is a well-known fact that two points are on a unique line. The points (0,0), (1,0), (0,1), (1,1) form a quadrangle. Thus, both $G1$ and $G2$ are satisfied, so the Euclidean plane is a geometry.

**Example 3** $S = (P, L)$, where $P = \{1, 2, 3, 4\}$ and $L = \{\{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}\}$ (see Figure 1.1 (a)) is a geometry. It is easy to see that any two points are on exactly one line, and the four points of $P$ make up a quadrangle.

Next follows a lemma that may seem obvious.

**Lemma 4.** *Two distinct lines in a geometry intersect in at most one point.*

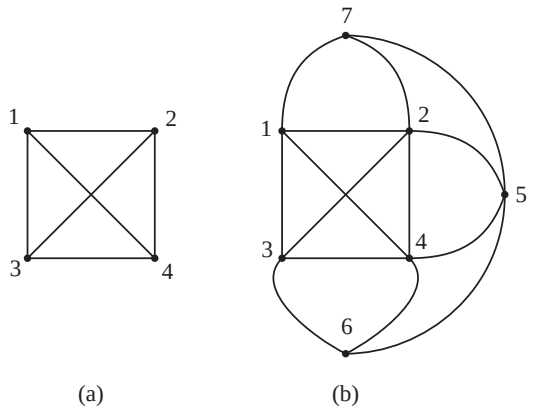



Figure 1.1: Two geometries.

*Proof.* Assume that there are two lines that intersect in at least two points, and let two such points be $p_1$ and $p_2$. But, by $G1$, there is exactly one line on both $p_1$ and $p_2$, and we have a contradiction. □

There are many kinds of geometries, and this essay is mainly about a set of geometries called *projective planes*. However, before we look at those, we shall look briefly at another set of geometries called the *affine planes* as the two are closely related.

**Definition 5 (Affine Plane).** *An* **affine plane** *$A$ is a geometry, that satisfies the following condition:*

*AP: For any line $l$, and any point $p$ not on $l$, there exists a unique line $l'$ on $p$ that does not intersect $l$.*

This is the famous *parallel axiom* of Euclidean geometry. Clearly, the Euclidean plane is an affine plane. The geometry of Example 3 is also easily seen to be an affine plane. For example, if $l = \{1, 4\}$ and $p = 3$, the unique line on $p$ that is not on $l$ is $\{2, 3\}$. The obvious connection to the parallel axiom justifies the following definition.

**Definition 6 (Parallel Lines).** *Two lines in an affine planes are said to be* **parallel** *if they do not intersect. Any line is also said to be parallel to itself. If $l_1$ and $l_2$ are two parallel lines, we write this as $l_1 || l_2$.*

**Lemma 7.** *The relation 'is parallel' on the lines of an affine plane is an equivalence relation.*

*Proof.* Let $l_1, l_2$ and $l_3$ be three distinct lines of $A$. By definition $l_1 || l_1$, so this relation is reflexive. Now, assume that $l_1$ is parallel to $l_2$, that is $l_1$ does not meet $l_2$. Then $l_2$ does not meet $l_1$ either, so $l_2$ is parallel to $l_1$ and the relation is symmetric. To show transitivity, assume that $l_1 || l_2$ and $l_2 || l_3$, but that $l_1$ is not parallel to $l_3$. Then $l_1$ and $l_3$ intersect in a point $p$. But then $p$ is on two lines missing $l_2$, contradicting $AP$. Hence we must have that $l_1 || l_3$, and the relation is transitive. □

The equivalence relation 'is parallel' partitions the set of lines in an affine plane into parallel classes. For a line $l$ in an affine plane, we denote its parallel class by $[l]$. That is, $[l]$ consists of all lines parallel to $l$.

**Lemma 8.** *Let $p$ be a point of an affine plane. For each parallel class of lines, there is exactly one line on $p$ that belongs to the class.*

*Proof.* Let $[l]$ be any parallel class, $l \in L$. If $l$ is not on $p$, by $AP$ there exists a unique line on $p$ parallel to $l$, and we are done. If $l$ is on $p$, we must show that no other line on $p$ is also in $[l]$. But any other line on $p$ meets $l$ in $p$, so the lines are not parallel. □

## 1.2 Projective plane

Now we shall move on to the main subject of this essay, projective planes.

**Definition 9 (Projective plane).** *A* **projective plane** *is a geometry that satisfies the following condition:*

*PP: Any two lines intersect in exactly one point.*

We see that the difference between affine and projective planes is that in a affine plane parallel lines exists, whereas in projective planes lines always meet.

**Example 10** Let $\Pi = (P, L)$ where $P = \{1, 2, 3, 4, 5, 6, 7\}$ and $L = \{l_1, l_2, l_3, l_4, l_5, l_6, l_7\}$, $l_1 = \{1, 2, 3\}$, $l_2 = \{1, 4, 5\}$, $l_3 = \{1, 6, 7\}$, $l_4 = \{2, 4, 6\}$, $l_5 = \{2, 5, 7\}$, $l_6 = \{3, 4, 7\}$ and $l_7 = \{3, 5, 6\}$ (see fig 1.2). Then $\Pi$ is a projective plane. It is easily seen to satisfy G1 and PP, and the set $\{1, 2, 4, 7\}$ is an example of a quadrangle. This plane is called the *Fano* plane .

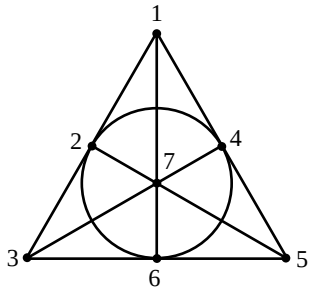



Figure 1.2: The Fano plane

**Example 11** Let $A = (P, L)$ be the Euclidean plane. As we have seen earlier, this is an affine plane. However, there is an easy way to construct a projective plane from the Euclidean plane, by 'tying together' all parallel lines in a point 'at infinity'. It is done as follows.

Let $P' = \{P \cup \mathbb{R} \cup \{\infty\}\}$, where $\infty$ is just a symbol. We shall define the set $L'$. Any line $l$ of $A$ can be written as either the equation $y = kx + m$ or $x = m$, where $k, m \in \mathbb{R}$. If $l$ is of the former form, then let $l' = \{l \cup \{k\}\}$ be an element of $L'$. If $l$ is of the latter form, then let $l' = \{l \cup \{\infty\}\}$ be an element of $L'$. Finally, let $l_\infty = \{\mathbb{R} \cup \{\infty\}\}$ (called the *line at infinity*) be an element of $L'$. A point on the line at infinity will be written as either $(k)$ where $k \in \mathbb{R}$ or as $(\infty)$, and any point in $P$ will be written as $(x, y)$ in the obvious way. A point in $P$ will be called an *ordinary* point, and a point on the line $l_\infty$ will be called an *extended* point.

It should be obvious that two points of $\Pi$ are on a unique line, so $G1$ is satisfied. The four points $(0, 0), (0, 1), (1, 0)$ and $(1, 1)$ still form a quadrangle, so $G2$ is also satisfied. Let $l$ and $l'$ be two lines other than the line at infinity. If $l$ and $l'$ have different slope, then they meet in one point of the ordinary plane (and only there). If they have the same slope, then they meet in a point of the line at infinity (and only there). Finally, $l$ meets the line at infinity in precisely one point. Thus $PP$ is satisfied, so $\Pi = (P', L')$ is a projective plane. This plane is called *the projective real plane*

The previous example suggests a way of turning any affine plane into a projective plane. This is done as follows. Let $A = (P, L)$ be an affine plane. Let $P' = P \cup \{[l] \mid l \in L\}$, that is, $P'$ is $P$ with one point added for each parallel class of $A$. Now, define the set $L'$ as follows. For each line $l \in L$, let $\{l \cup \{[l]\}\}$ be an element of the set $L'$. Finally, let $\{[l] \mid l \in L\}$ be an element of $L'$. Then $\Pi = (P', L')$ is a projective plane. If this is not easy to see, compare with Example 11.

Similarly, any projective plane can be turned into an affine plane by removing one line, and all points on it. $G1$ still holds, as does $G2$. That $AP$ holds can be seen as follows. Let $p$ be any point of the affine plane, let the line removed from the projective plane be $l$, and let $l'$ be any line in the affine plane not on $p$. In the projective plane, $l'$ intersects $l$ in precisely one point, call it $q$. Again,

in the projective plane, there is one unique line on $p$ and $q$. Thus, in the affine plane, the line $pq$ is the only line on $p$ not meeting $l'$, and thus $AP$ holds.

**Example 12** We shall turn the affine plane of Example 3 into a projective plane. As there are three parallel classes, add the points 5, 6 and 7 to get the lines $\{\{1,2,5\}, \{3,4,5\}, \{1,4,6\}, \{2,3,6\}, \{1,3,7\}, \{2,4,7\}, \{5,6,7\}\}$.

**Example 13** Let $\Pi = (P, L)$ where $P$ are the lines of $\mathbb{R}^3$ through the origin and $L$ are the planes of $\mathbb{R}^3$ through the origin. Two distinct lines through the origin define a unique plane through the origin, so $G1$ is satisfied. Furthermore, two distinct planes through the origin intersect in a unique line through the origin, so $PP$ is also satisfied. The axes, together with the line through the origin and (1, 1, 1) is an example of a quadrangle, so $\Pi$ is indeed a projective plane. This example is very important, and we shall use it in the next chapter to construct projective planes.

**Definition 14 (Dual statement).** *If $S$ is a statement on projective planes, then the* **dual statement** *$S'$ of $S$ is the statement where the words* points *and* lines *are swapped.*

**Example 15** The dual statement of "two points are on a line" is "two lines are on a point".

In the definition of a projective plane, there are three statements on points and lines:

$G1$: Two distinct points are on exactly one line.

$G2$: There exists a set of four points, no three of which are collinear.

$PP$: Two distinct lines intersect in exactly one point.

The dual statements of these are:

$G1'$: Two distinct lines are intersect in exactly one point.

$G2'$: There exists a set of four lines, no three of which are on a common point.

$PP'$: Two distinct points are on exactly one line.

We see that $G1' = PP$, and $PP' = G1$. So, if we assume that $G1$, $G2$ and $PP$ hold, then obviously $G1'$ and $PP'$ hold. Also, by $G2$, there exist four points $p_1, p_2, p_3$ and $p_4$, no three collinear. Thus the lines $p_1p_2$, $p_2p_3$, $p_3p_4$ and $p_4p_1$ are four distinct lines (see Figure 1.3 (a)). Obviously, each of the four points $p_1, p_2, p_3$ and $p_4$ are on exactly two of these lines. Now, suppose for a contradiction that three of these lines intersect in a commont point $p$ (which will be different from $p_1, p_2, p_3$ and $p_4$ as each of these are on exactly two of the lines). But this contradicts $PP$, as then there are two distinct points common to two of the three lines. Hence $G2'$ hold.

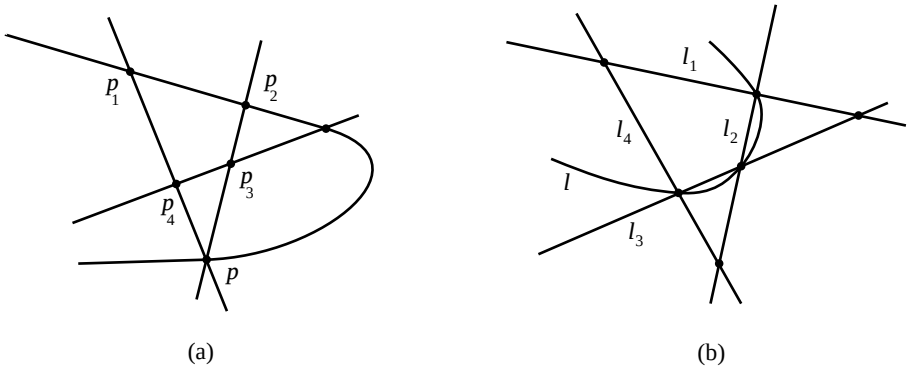



Figure 1.3: (a) If the three lines $p_1p_2$, $p_2p_3$ and $p_4p_1$ would intersect in a common point $p$, the lines $p_1p_2$ and $p_1p_4$ would both contain both $p$ and $p_1$, contradicting $PP$. (b) If there would exist a line $l$ through the points $l_1l_2$, $l_2l_3$ and $l_3l_4$, then there would be two distinct lines containing the two points $l_2l_3$ and $l_3l_4$, contradicting $PP'$.

On the other hand, assume that $G1'$, $G2'$ and $PP'$ hold. Then obviously $G1$ and $PP$ hold. Also, by $G2'$, there exist four lines $l_1, l_2, l_3$ and $l_4$, no three on a common point (see Figure 1.3 (b)). Hence the four points $l_1l_2$, $l_2l_3$, $l_3l_4$ and $l_4l_1$ are all distinct (all these lines intersect by $G1'$). As these are all distinct, each of the four lines $l_1, l_2, l_3$ and $l_4$ are on exactly two of these points. Now suppose, for a contradiction, that three of these points are collinear, say on the line $l$ (which will be different from the lines $l_1, l_2, l_3$ and $l_4$ as these are on only two of the points). But this contradicts $PP'$, as then there are two distinct lines through two of the three points. Hence $G2$ hold.

From the preceding argument, we see that $G1$, $G2$ and $PP$ hold if and only if $G1'$, $G2'$ and $PP'$ hold. Hence, for any statement proved using $G1$, $G2$ and $PP$, the dual statement can be proved using $G1'$, $G2'$ and $PP'$, and vice versa. We have proven the following theorem:

**Theorem 16.** *For any true statement on projective planes, the dual statement is also true.*

This simplifies our work a lot. If we prove a theorem saying something about the points of a projective plane, the dual argument will prove the same thing about lines, and vice versa. This is one of the beautiful symmetric properties of projective planes.

## 1.3 Numeric properties of finite projective planes

We shall now look at properties of the finite projective planes. Here the set $P$ is finite, so $L$ must also be finite. We have previously seen just one finite projective plane (Example 10). Here is another example.

**Example 17** Let $\Pi = (P, L)$, where $P = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13\}$, and

$$\begin{aligned} L = \{ \quad & \{1,2,3,4\}, && \{1,5,9,12\}, && \{1,6,10,13\}, \\ & \{1,7,8,11\}, && \{2,5,10,11\}, && \{2,6,8,12\}, \\ & \{2,7,9,13\}, && \{3,5,8,13\}, && \{3,6,9,11\}, \\ & \{3,7,10,12\}, && \{4,5,6,7\}, && \{4,8,9,10\}, \\ & \{4,11,12,13\}\}. \end{aligned}$$

See figure 1.4. Note that point 4 is on the line $\{1, 2, 3, 4\}$, even though the figure does not show this (this line is represented in the figure by the circle going through points 1, 2 and 3). This is a projective plane.

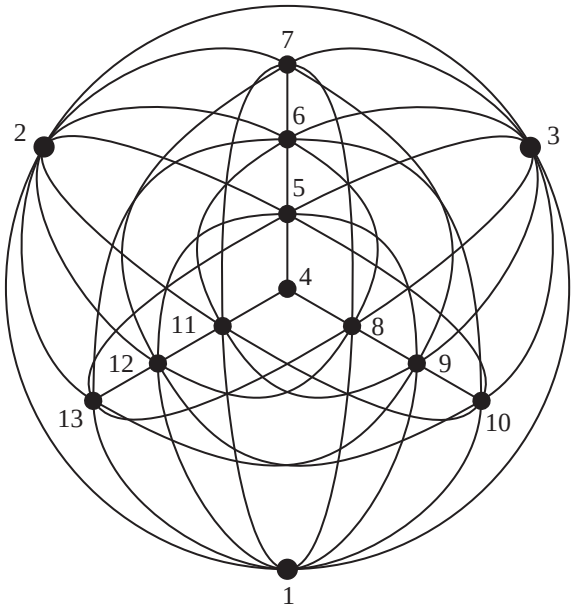



Figure 1.4: A finite projective plane. Note that $\{1, 2, 3, 4\}$ is a line even though this is not clear from the picture.

If you look at our two examples of finite projective planes, they are both very symmetrical. In the Fano plane, each line is on three points, and each point is on three lines. In the last example each line is on four points, and each point is on four lines.

**Lemma 18.** *Let $l$ be any line of a projective plane $\Pi$, and $p$ any point not on $l$. Then the line $l$ has exactly $n+1$ points for some positive integer $n$, if and only if there are $n+1$ lines on $p$.*

*Proof.* Assume that the line $l$ has $n+1$ points. Then each of these points are on exactly one line that is also on $p$, so there are at least $n+1$ lines on $p$. Since any line on $p$ intersects $l$ in exactly one point, there are no other lines on $p$, so there are exactly $n+1$ lines on $p$. The dual argument shows the converse. □

**Theorem 19.** *Let $\Pi$ be a finite projective plane. Then there exists an integer $n > 1$, such that each point is on $n+1$ lines, and dually, each line has $n+1$ points.*

*Proof.* We will prove the first part, and the second part will follow from the dual argument. Let $p_1$, $p_2$, $p_3$, $p_4$, be the points of a quadrangle in $\Pi$. Each of these points is certainly on at least three lines (the lines on the point and the other points of the quadrangle). Let $n > 1$ be the number such that $p_1$ is on $n+1$ lines.

Now, the lines $p_2p_3$, $p_3p_4$ and $p_2p_4$ are each on exactly $n+1$ points, by Lemma 18. For each point $q$ in $\Pi$, at least one of the lines $p_2p_3$, $p_3p_4$, $p_2p_4$ misses $q$. Again, by Lemma 18, there are exactly $n+1$ lines on $q$, and we have proven the theorem. □

**Definition 20 (Order of a finite projective plane).** *The* **order** *of a finite projective plane is the integer $n$ such that each point is on $n+1$ lines, and each line is on $n+1$ points.*

By looking at our previous examples, we see that the Fano plane has order 2, as does the plane of Figure 1.1 (b). The plane in Figure 1.4 has order 3. The following theorem counts the total number of points, and lines, of a finite projective plane.

**Theorem 21.** *The number of points in a projective plane $\Pi$ of order $n$ is $n^2+n+1$, and dually the number of lines is also $n^2+n+1$.*

*Proof.* Let $p$ be any point of $\Pi$. Now, there are $n+1$ lines on $p$. Each of these lines have $n$ points other than $p$. All of these points are distinct, as otherwise two different lines would have two points in common, which violates G1. Thus, the number of points of $\Pi$ other than $p$ is $n(n+1) = n^2+n$, so the total number of points is $n^2+n+1$. □

By this theorem, the Fano plane should contain $2^2+2+1 = 7$ points and lines, which it does. Also, The plane of example 17 should have $3^2+3+1 = 13$ points and lines, which it indeed does.

**Theorem 22.** *The projective plane of order 2 is unique (up to renumbering of the points).*

*Proof.* Let the plane be $\Pi$. We know that $\Pi$ has 7 points, which we will denote by 1, 2, 3, 4, 5, 6 and 7. There should be three lines on the point 1, and we may, without loss of generality, assume that these are $l_1 = \{1,2,3\}, l_2 = \{1,4,5\}$ and $l_3 = \{1,6,7\}$. Now, there are two more lines on the point 2. One of these must be on point 4, and we may, again without loss of generality, assume that this line is $l_4 = \{2,4,6\}$. Then the other line on 2 must be $l_5 = \{2,5,7\}$. Now, 4 is on one more line. The only points that 4 is not already on a line with are 3 and 7, and thus $l_6 = \{3,4,7\}$. Now all points except 3, 5 and 6 are on three lines, and no two of these points are already on a line, so $l_7 = \{3,5,6\}$ is a line. We have now constructed a projective plane of order 2, and this was possible in essentially one way (up to renumbering of the points), so there is only one projective plane of order 2. □

From the previous theorem we see that the projective planes of Figures 1.1 (b) and 1.2 are actually the same. This can be seen by renumbering the points of Figure 1.1 (b) to

$$\begin{array}{lll} 1 \to 1 & 4 \to 4 & 7 \to 6 \\ 2 \to 2 & 5 \to 3 & \\ 3 \to 7 & 6 \to 5. & \end{array}$$

So, why do we use the word *planes* for these object. Well, this is because they are, in a sense, two-dimensional. In linear algebra, we say that two vectors *span* a plane, or equivalently that three points not on a line define a plane. The next theorem shows, that for finite projective planes, by selecting three points, not on a line, we can generate the entire plane.

**Theorem 23.** *Let $\Pi$ be a finite projective plane of order $n$. Let $p$, $q$ and $r$ be three points of $\Pi$, not on a line. Then the lines $pp'$, where $p'$ is any point on the line $qr$ contains all points of $\Pi$.*

*Proof.* The line $pq$ has $n+1$ points. The $n+1$ lines through $r$ and these points are all distinct. Counting the points of these lines, we get $n(n+1)+1 = n^2+n+1$, which are all the points of $\Pi$. □

**Example 24** Let $p = 1$, $q = 3$ and $r = 7$ of the Fano plane, figure 1.2. The line $pq$ is $\{1, 2, 3\}$. The lines through these points and $r$ are the lines $\{1, 6, 7\}$, $\{2, 4, 7\}$ and $\{3, 5, 7\}$. By theorem 23 any point of the Fano plane should be in at least one of these lines, which is easily seen to be true.

## 1.4 Incidence matrices

A very convenient way of representing projective planes is by using matrices.

**Definition 25 (Incidence matrices).** *Let $\Pi$ be a finite projective plane of order $n$. The* **incidence matrix** *$A$ of $\Pi$ is the $(n^2+n+1) \times (n^2+n+1)$-matrix, where the lines are represented by the rows and the points are represented by the columns, such that row $i$ has a 1 in column $j$ if the line corresponding to row $i$ contains the point corresponding to column $j$, and a 0 otherwise.*

**Example 26** The incidence matrix of example 10 is the $7 \times 7$ matrix

$$A = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{bmatrix}.$$

The following lemmas will be useful when proving the Bruck-Ryser theorem in chapter 3. Please use the incidence matrix of the previous example to check their validity.

**Lemma 27.** *Let $A$ be the incidence matrix of a finite projective plane $\Pi$ of order $n$. Let $u_i$, be the rows of $A$. Then:*

$$u_i \cdot u_j = \begin{cases} 1 & \text{if } i \neq j \\ n+1 & \text{if } i = j \end{cases}$$

*The same holds for inner products of rows of $A$.*

*Proof.* Let $N = n^2+n+1$ be the number of lines/points of $\Pi$, or equivalently the number of columns/rows of $A$. Let $[a_{i1}, a_{i2}, \ldots, a_{iN}]$ be the row $u_i$, and $[a_{j1}, a_{j2}, \ldots, a_{jN}]$ be the row $u_j$.

If $i \neq j$, these rows represent two different lines. These two lines have one unique point in common, which means that there is exactly one $m$, $1 \leq m \leq N$ such that both $a_{im}$ and $a_{jm}$ are one. Hence the product of $a_{im}$ and $a_{jm}$ is one. For all $k$, $1 \leq k \leq N$ and $k \neq m$, at least one of $a_{ik}$ or $a_{jk}$ is zero, which means that their product is zero. By this we see that the inner product of these rows (which is the sum of all these products) are exactly one.

If $i = j$, these rows represent the same line. Then it is easy to see that their inner product is exactly the sum of the ones in the row. Since there are $n+1$ ones in any row, this sum is $n+1$. □

**Lemma 28.** *Let $A$ be the incidence matrix of a projective plane $\Pi$ of order $n$. Then $AA^T = nI+J$, where $I$ is the $(n^2+n+1) \times (n^2+n+1)$ identity matrix and $J$ is the $(n^2+n+1) \times (n^2+n+1)$ matrix having all entries equal to one.*

*Proof.* Let $a_{ij}$ be the entry of $AA^T$ on row $i$ and column $j$. This is equal to the inner product of rows $i$ and $j$ of $A$. By Lemma 27, $a_{ij} = 1$ if $i \neq j$, and $a_{ij} = n+1$ if $i = j$. Thus the diagonal of $AA^T$ will equal $n+1$, and all other entries will equal 1. In short, this can be written as $AA^T = nI + J$, using the notation of the lemma. □

**Lemma 29.** *Let $A$ be the incidence matrix of a projective plane $\Pi$ of order $n$. Then*

$$\det A = \pm(n+1)n^{(n^2+n)/2}.$$

*Proof.* Let $B = AA^T$. Then $\det B = \det(AA^T) = \det A \det A^T = (\det A)^2$. As $\det B$ is a square, it is non-negative. By Lemma 28 $B$ has all entries 1, except for the diagonal, which has all entries $n+1$. Subtract the first row from all other rows, and then add all columns to the first column. As all these operations preserve the absolute value of the determinant, this gives us

$$\det B = \begin{vmatrix} n+1 & 1 & \cdots & 1 \\ 1 & n+1 & & \vdots \\ \vdots & & \ddots & 1 \\ 1 & \cdots & 1 & n+1 \end{vmatrix} = \pm \begin{vmatrix} n+1 & 1 & \cdots & 1 \\ -n & n & & 0 \\ \vdots & & \ddots & \vdots \\ -n & 0 & \cdots & n \end{vmatrix}$$

$$= \pm \begin{vmatrix} (n+1)^2 & 1 & \cdots & 1 \\ 0 & n & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & \cdots & 0 & n \end{vmatrix}$$

As this is a triangular matrix, the determinant is just the product of the elements of the diagonal. All the elements of the diagonal are positive, so

$$\det B = (n+1)^2 n^{n^2+n}.$$

As $(\det A)^2 = \det B$, it follows that $\det A = \pm(n+1)n^{(n^2+n)/2}$. □

# Chapter 2

# Collineations and Constructions of Projective Planes

We will start this chapter with a section that shows how we can construct projective planes using fields. We will then turn to the important concept of collineations (or automorphisms) of projective planes.

## 2.1 Constructing projective planes using fields

We saw in Example 13 that a three-dimensional vector space over $\mathbb{R}$ could be used to construct a projective plane. We will now generalize this idea to construct projective planes using three-dimensional vector spaces over any field $F$.

Let $F$ be a field, and let $F^3$ denote a three-dimensional vector space over $F$. We shall now construct a projective plane $\Pi$. The points of $\Pi$ are the lines of $F^3$ through the origin, that is, the sets of the form $\{\alpha v \mid \alpha \in F\}$, where $v$ is in $F^3$. The lines of $\Pi$ are the planes of $F^3$ through the origin, that is, the sets of the form $\{\alpha v + \beta w \mid \alpha, \beta \in F\}$, where $v$ and $w$ are in $F^3$. As a non-zero vector in $F^3$ spans a line in $F^3$, we can use the non-zero vectors in $F^3$ to represent the points of $\Pi$. To distinguish the two, $v$ denotes the vector in $F^3$, and $[v]$ denotes the point in $\Pi$. If $v = (x, y, z)$, then we write $[x, y, z]$ instead of $([x, y, z])$.

Two non-zero vectors $v$ and $w$ span the same line if and only if there exists an element $\alpha$ in $F$ such that $v = \alpha w$. As two non-zero vectors $v$ and $w$ of $F^3$ represent the same point in $\Pi$ (i.e. $[v] = [w]$) if and only if they span the same line in $F^3$ we see that $[v] = [w]$ if and only if $v = \alpha w$ for some $\alpha$ in $F$. Let $v = (x, y, z)$. If $x \neq 0$, then

$$[v] = [x^{-1}v] = [1, x^{-1}y, x^{-1}z] = [1, y', z'].$$

If $x = 0$, then $y$ and $z$ can not both be zero (as $v$ is a non-zero vector). Then, if $y \neq 0$ then $[v] = [y^{-1}v] = [0, 1, z']$, but if $y = 0$ then $[v] = [z^{-1}v] = [0, 0, 1]$.

Any plane through the origin can be represented with an equation of the form $ax + by + cz = 0$, where a point $(x, y, z)$ is on the plane if it satisfies this equation. We will use the notation $\langle a, b, c\rangle$ to denote the line of $\Pi$ corresponding to this plane. As in the case for vectors, $[a, b, c] = [a', b', c']$ if and only if $a = ra', b = rb'$ and $c = rc'$ for some non-zero element $r \in F$. Using this notation, we se that the point $[x, y, z]$ is on the line $\langle a, b, c\rangle$ if and only if

$$\langle a, b, c\rangle \cdot \begin{bmatrix} x \\ y \\ z \end{bmatrix} = 0$$

The fact that $\Pi$ constructed in this way is a projective plane follows easily from elementary linear algebra. Two lines with exactly one point in common are contained in exactly one plane in $F^3$, and as the point in common is the origin, the plane passes through the origin. Hence the two distinct lines of $F^3$ corresponding to two distinct points of $\Pi$ lie in exactly one plane through the origin, which thus define a unique line through the two points of $\Pi$. Hence $G1$ is satisfied. The four points $[1, 0, 0]$, $[0, 1, 0]$, $[0, 0, 1]$ and $[1, 1, 1]$ are an example of a quadrangle, so $G2$ is satisfied. In fact, we may always assume that the four points of a quadrangle has these co-ordinates. Finally, two

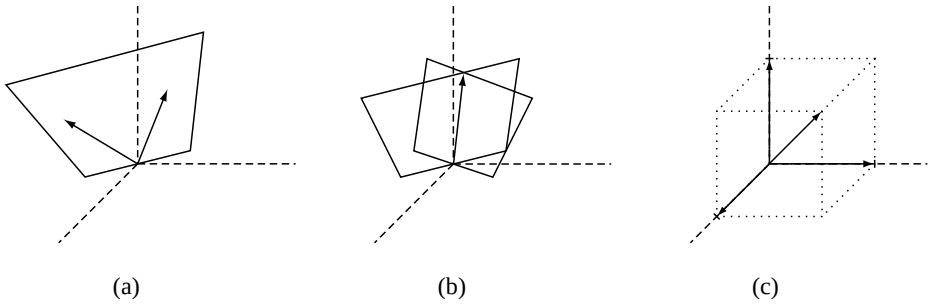



Figure 2.1: (a) Two points are on one unique line. (b) Two lines intersect in exactly one point. (c) There exists a set of four points, no three of which are collinear.

planes through the origin in $F^3$ intersect in exactly one line through the origin, so the two lines of $\Pi$ corresponding to the planes meet in a unique point, and thus $PP$ is satisfied, and we have shown that $\Pi$ is a projective plane (see figure 2.1). The plane constructed in this way using the field $F$ is usually denoted by $PG(2, F)$ (meaning the projective geometry of dimension 2 constructed from the field $F$).

It is very important to know when three points are on the same line, which the following Lemma tells us.

**Lemma 30.** *Let $p_1 = [v_1] = [x_1, y_1, z_1], p_2 = [v_2] = [x_2, y_2, z_2]$ and $p_3 = [v_3] = [x_3, y_3, z_3]$ be three points of the projective plane $PG(2, F)$. Then the three points are collinear if and only if*

$$\det \begin{bmatrix} x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \\ x_3 & y_3 & z_3 \end{bmatrix} = 0.$$

*Proof.* The three points are on a line if and only if $v_1 = \alpha v_2 + \beta v_3$ for some $\alpha$ and $\beta$ in $F$. But it is precisely when this holds that the above determinant is zero. □

As we are mostly interested in finite projective planes here, the following theorem is very important. When $F$ is a finite field, it is customary to write $PG(2, q)$ where the prime power $q$ is the order of the field, as opposed to writing $PG(2, \mathbb{F}_q)$ (where $\mathbb{F}_q$ denotes the finite field of order $q$).

**Theorem 31.** *The projective plane $PG(2, q)$ has order $q$.*

*Proof.* We will prove this by counting the number of points of any line in $PG(2, q)$. Any line of $PG(2, q)$ corresponds to a plane through the origin of $\mathbb{F}_q^3$, that is a set of the form $L = \{\alpha v + \beta w \mid \alpha, \beta \in \mathbb{F}_q\}$, where $v$ and $w$ are vectors of $\mathbb{F}_q^3$. Let this set correspond to the line $l$. The points of $PG(2, q)$ that are on $l$ are the points of the form $[\alpha v + \beta w]$, $\alpha$ and $\beta$ not both zero. As before, $[\alpha v + \beta w] = [\alpha' v + \beta' w]$ if and only if $\alpha = r\alpha'$ and $\beta = r\beta'$ for some $r \in \mathbb{F}_q$. So, if $\alpha \neq 1$, we have $[\alpha v + \beta w] = [v + \beta' w]$ where $\beta' = \beta\alpha^{-1}$, and each distinct $\beta'$ corresponds to a distinct point of $l$. Thus there are $q$ points that can be written in this way. If $\alpha = 0$ then $[\alpha v + \beta w] = [0 \cdot v + \beta\beta^{-1} w] = [w]$, which is just one point. Since all points of $l$ are accounted for in this way, we conclude that $l$ has $q + 1$ points and $PG(2, q)$ is thus of order $q$. □

**Example 32** We will construct the projective plane of order 2 from $\mathbb{F}_2$, i.e. the plane $PG(2, 2)$. $\mathbb{F}_2^3$ consists of the 8 vectors $(0, 0, 0)$, $(0, 0, 1)$, $(0, 1, 0)$, $(0, 1, 1)$, $(1, 0, 0)$, $(1, 0, 1)$, $(1, 1, 0)$ and $(1, 1, 1)$. Any line through the origin consist of just two points, of which the origin is one. We can thus identify the lines through the origin with this point, and we can identify any point of $PG(2, 2)$ with the non-zero vector spanning the corresponding line.

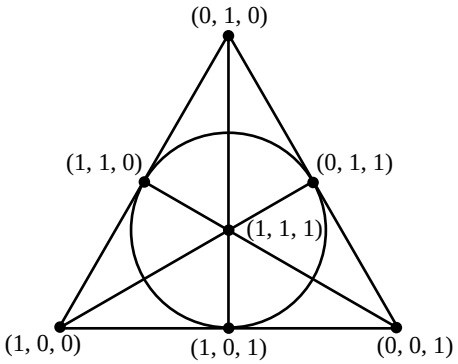



Figure 2.2: The projective plane of order 2 constructed from the finite field of order 2.

The planes of $\mathbb{F}_2^3$ through the origin are

$$\{(0,0,0),(0,0,1),(0,1,0),(0,1,1)\},$$
$$\{(0,0,0),(0,0,1),(1,0,0),(1,0,1)\},$$
$$\{(0,0,0),(0,0,1),(1,1,0),(1,1,1)\},$$
$$\{(0,0,0),(0,1,0),(1,0,0),(1,1,0)\},$$
$$\{(0,0,0),(0,1,0),(1,0,1),(1,1,1)\},$$
$$\{(0,0,0),(0,1,1),(1,0,0),(1,1,1)\},$$
$$\{(0,0,0),(1,0,1),(1,1,0),(0,1,1)\}.$$

Note that in a given plane, the sum of two of the non-zero vectors is the third non-zero vector. As we have identified the points of $PG(2,2)$ with the non-zero vectors of $\mathbb{F}_2^3$, we see that the a line of $PG(2,2)$ consists of the three non-zero elements of the corresponding plane (see figure 2.2).

**Theorem 33.** *There exists a projective plane of order $q$ for each prime power $q$.*

*Proof.* By Theorem 31 the projective plane constructed from the finite field of order $q$ has order $q$. Furthermore, as there exists a finite field for each prime power, the result follows. □

## 2.2 Collineations of projective planes

**Definition 34 (Collineation).** *Let $\Pi = (P, L)$ be a projective plane. A* **collineation** *of $\Pi$ is a bijective function $\phi : P \to P$ which preserves incidence, that is, $\phi(l) \in L$ for any $l \in L$.*

**Example 35** The identity function is obviously always a collineation.

**Example 36** Let $\Pi$ be the Fano plane of Example 10. An example of a collineation of $\Pi$ is $\phi$, defined by

$$\begin{array}{lll} \phi(1) = 2 & \phi(4) = 7 & \phi(7) = 4 \\ \phi(2) = 1 & \phi(5) = 5 & \\ \phi(3) = 3 & \phi(6) = 6 & \end{array}$$

**Example 37** Let $\Pi$ be the projective plane of Example 11. Define $\phi$ by $\phi(x, y) = (x + k, y)$ for any ordinary point $(x, y)$, where $k$ is a non-zero real number, and $\phi(z) = z$ for points on the line at infinity. Then $\phi$ is a collineation of $\Pi$.

**Theorem 38.** *The set of collineations of a projective plane* $\Pi = (P, L)$ *form a group under composition.*

*Proof.* First we must show that the composition of two collineations is again a collineation. So, let $\phi$ and $\theta$ be two collineations of $\Pi$, and let $l \in L$ be any line of $\Pi$. Then, as $\phi$ is a collineation, $\phi(l) \in L$. Again, as $\theta$ is a collineation and $\phi(l) \in L$ we have that $\theta(\phi(l)) \in L$, so $\theta \circ \phi$ is indeed a collineation. Let $\phi$, $\theta$ and $\rho$ be three collineations of $\Pi$, and let $p$ be any point of $\Pi$. Then

$$(\phi \circ \theta) \circ \rho(p) = \phi \circ \theta(\rho(p)) = \phi(\theta(\rho(p))) = \phi(\theta \circ \rho(p)) = \phi \circ (\theta \circ \rho)(p),$$

so composition is associative. Now, $\phi$ be any collineation of $\Pi$, let $\iota$ be the identity collineation, and let $p$ be any point of $\Pi$. Then

$$\phi \circ \iota(p) = \phi(\iota(p)) = \phi(p) = \iota(\phi(p)) = \iota \circ \phi(p),$$

so $\iota$ works as an identity. Finally, as any collineation is bijective, each collineation $\phi$ has an inverse $\phi^{-1}$. We have, for all points $p$ of $\Pi$,

$$\phi \circ \phi^{-1}(p) = \phi(\phi^{-1}(p)) = p = \iota(p)$$
$$\phi^{-1} \circ \phi(p) = \phi^{-1}(\phi(p)) = p = \iota(p).$$

But we must also show that $\phi^{-1}(l) \in L$ for any line $l$, i.e. that $\phi^{-1}$ is indeed a collineation. So, let $p_1$ and $p_2$ be any two points of $l$, and let $p_1' = \phi^{-1}(p_1)$, $p_2' = \phi^{-1}(p_2)$ and let $l'$ be the line $p_1'p_2'$. As $\phi$ is a collineation, we must have $\phi(l') = l$. But then

$$\phi^{-1}(l) = \phi^{-1}(\phi(l')) = l',$$

and $\phi^{-1}$ is a collineation. Hence $\phi^{-1}$ acts as an inverse of any collineation $\phi$ of $\Pi$, and the set of collineations of $\Pi$ form a group under composition. □

**Example 39** We shall determine the order of the collineation group of the Fano plane. We will do this by counting the ways of defining a bijection $\phi$ of the points of the plane such that it is a collineation. First of all, there are 7 ways of choosing $\phi(1)$, and once that is done there are 6 ways of choosing $\phi(2)$. Now, as $\phi$ should be a collineation, $\phi(3)$ must be the third point on the line determined by $\phi(1)$ and $\phi(2)$. As there are 4 points left, there are 4 ways of choosing $\phi(4)$. $\phi(5)$ must be remaining point on the line determined by $\phi(1)$ and $\phi(4)$, $\phi(6)$ must be the remaining point on the line determined by $\phi(2)$ and $\phi(4)$, and $\phi(7)$ must be the remaining point on the line determined by $\phi(3)$ and $\phi(4)$. Hence there are $7 \times 6 \times 4 = 168$ ways of choosing $\phi$, and the order of the collineation group is 168.

**Definition 40 (Central collineation).** *A collineation* $\phi$ *of a projective plane* $\Pi$ *is called a* **central** *collineation if there exists a point* $c$ *in* $\Pi$ *called the* **center** *of the collineation such that* $\phi(c) = c$ *and* $\phi$ *fixes all lines on* $c$*. That is, for any point* $p$ *other than* $c$*, the line* $cp$ *is the same as the line* $c\phi(p)$*.*

**Definition 41 (Axial collineation).** *A collineation* $\phi$ *of a projective plane* $\Pi$ *is called an* **axial** *collineation if there exists a line* $l$ *in* $\Pi$ *called the* **axis** *of the collineation such that* $\phi(l) = l$ *and* $\phi$ *fixes all points on* $l$*. That is, for any line* $l'$ *other than* $l$*,* $l'$ *intersects* $l$ *in the same point as* $\phi(l')$*.*

The two preceding definitions are easily seen to be dual statements. The collineation of Example 36 is a central collineation with center 3, and the collineation of Example 37 is an axial collineation with the line at infinity as axis.

**Theorem 42.** *Any central collineation of a projective plane having more than one center is the identity collineation, and dually any axial collineation having more than one axis is the identity collineation.*

*Proof.* Let $\phi$ be a central collineation having two centers, $c_1$ and $c_2$. Let $p$ be any point not on the line $c_1c_2$. As both lines $pc_1$ and $pc_2$ are fixed by $\phi$, and $p$ is on both these lines, it follows that $p$ is fixed by $\phi$. Thus any point not on the line $c_1c_2$ are fixed by $\phi$. Now, let $p$ be any point on the line $c_1c_2$, and let $l$ be any line on $p$ different from $c_1c_2$. Then, as all points different from $p$ on $l$ are fixed by $\phi$, it follows that $p$ is also fixed by $\phi$. But then $\phi$ fixes all points of $\Pi$, and is thus the identity collineation. □

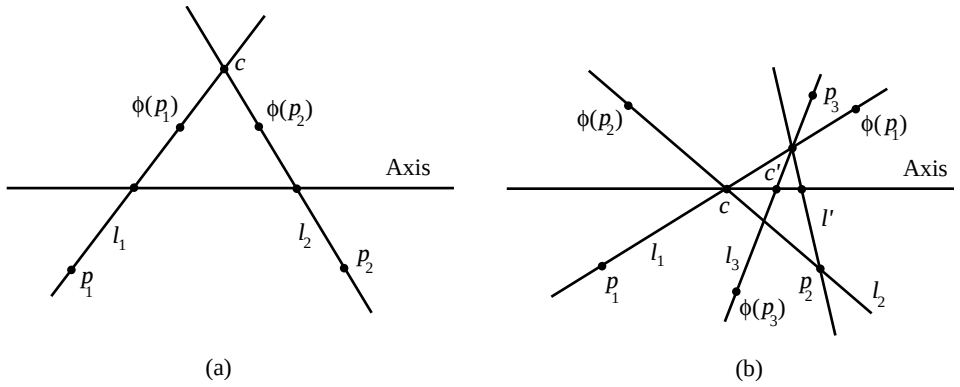



Figure 2.3: (a) Every axial collineation has a center. (b) Assuming that there is a point $p_3$ such that the line on both $p_3$ and $\phi(p_3)$ does not contain $c$ yields that the point $p_2$ is fixed.

**Lemma 43.** *Let $\phi$ be an axial collineation. Suppose that $\phi$ fixes a point $p$ that is not on the axis. Then $\phi$ is also a central collineation with $p$ as center. Dually, if a central collineation fixes a line not on the center, it is also an axial collineation.*

*Proof.* We must show that each line on $p$ is fixed by $\phi$. Any line on $p$ intersects the axis in precisely one point, and both this point and $p$ are fixed, so the line must also be fixed. Thus any line on $p$ is fixed by $\phi$ and $\phi$ is a central collineation. □

**Theorem 44.** *A collineation $\phi$ of a projective plane $\Pi$ is a central collineation if and only if it is an axial collineation.*

*Proof.* The identity collineation is obviously both central and axial, so suppose that $\phi$ is an axial collineation that is not the identity collineation. We must show that $\phi$ has a center, that is, a point whose lines are fixed by $\phi$.

Let $p_1$ and $p_2$ be two points not on the axis. If either $p_1$ or $p_2$ are fixed by $\phi$, the by Lemma 43 $\phi$ is a central collineation. So suppose that $\phi(p_1) \neq p_1$ and $\phi(p_2) \neq p_2$. Let the line on $p_1$ and $\phi(p_1)$ be called $l_1$, and the line on $p_2$ and $\phi(p_2)$ be called $l_2$ (see figure 2.3 (a)). As the point where $l_1$ intersects the axis is fixed by $\phi$, $l_1$ must also be fixed by $\phi$. Similarly $l_2$ is fixed by $\phi$. Let $c$ be the point of intersection of $l_1$ and $l_2$. As both $l_1$ and $l_2$ are fixed by $\phi$, $c$ must also be fixed by $\phi$. If $c$ is not on the axis, by Lemma 43 $\phi$ is a central collineation.

So suppose that $c$ is on the axis. If all lines on $c$ are fixed, $\phi$ is a central collineation with center $c$. So, for a contradiction, suppose that there is a line on $c$ that is not fixed by $\phi$, and let $p_3$ be a point on this line different from $c$. If $p_3$ is fixed by $\phi$ then $\phi$ is a central collineation by Lemma 43, so assume that $p_3$ is not fixed by $\phi$. Let the line on $p_3$ and $\phi(p_3)$ be $l_3$, and the point where $l_3$ intersects the axis be $c'$ (see figure 2.3 (b)). As $c'$ is fixed by $\phi$ the line $l_3$ is fixed by $\phi$, as above. As the line $l_1$ is also fixed by $\phi$, the point of intersection of $l_1$ and $l_3$ (which is not on the axis) is fixed by $\phi$. Let $l'$ be the line on $p_2$ and $l_1 l_3$. As the point $l_1 l_3$ is fixed by $\phi$, and the point where $l'$ intersects the axis is fixed by $\phi$, $l'$ must also be fixed by $\phi$. But then, as $l_2$ is fixed by $\phi$, $p_2$ is fixed by $\phi$, contradicting our previous assumption that $p_2$ was not fixed. Hence all lines on $c$ are fixed by $\phi$ so $\phi$ is a central collineation, which completes the proof. □

The axis of Example 36 is the line $\{3, 5, 6\}$, and the center of Example 37 is the point (0). In both these cases the center is a point on the axis. As was hinted in the proof of Theorem 44 this is not always the case. For example, the collineation $\theta$ of the projective plane of Example 11 defined by $\theta(x, y) = (kx, ky)$ for any ordinary point, where $k \in \mathbb{R}$, and $\theta(z) = z$ for any point on the line at infinity has the line at infinity as axis, and the origin as center.

A collineation with center $c$ and axis $l$ is called a $(c, l)$-collineation. Is a $(c, l)$-collineation uniquely determined by its center and axis? The answer is no. For example, the collineation of Example 37 has the same center and axis for any value of $k$. However, the following theorem does say when a $(c, l)$-collineation is completely determined.

**Theorem 45.** *A $(c, l)$-collineation is completely determined by its center, its axis and its action on one point not on the axis or the center.*

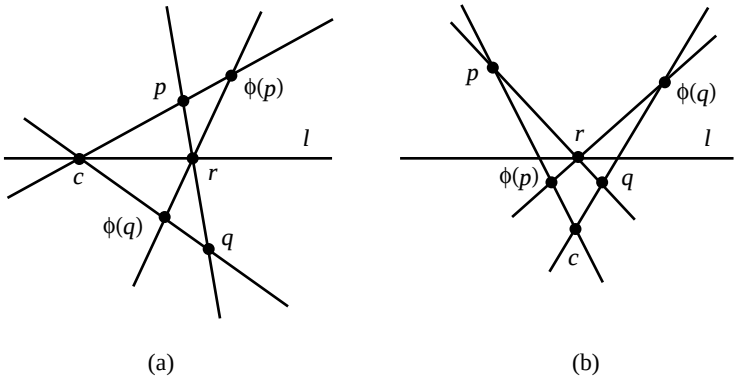



Figure 2.4: (a) The center is on the axis. (b) The center is not on the axis.

*Proof.* Let $\phi$ be a $(c, l)$-collineation and let $p$ be any point other than the center not on the axis such that $\phi(p)$ is known. Let $q$ be any point other than the $p$, $\phi(p)$, the center, and not on the axis. Let $r$ be the point of intersection of the line $pq$ and the axis. As $r$ is fixed by $\phi$, the line on $\phi(p)$ and $\phi(q)$ is on $r$. The line $cq$ is also fixed by $\phi$, as $c$ is the center. Hence $\phi(q)$ is the point of intersection of the lines $cq$ and $r\phi(p)$, which are both known, and we are done (see figure 2.4). □

**Corollary 46.** *A $(c, l)$-collineation $\phi$ that fixes any point other than $c$, not on the axis, is the identity collineation.*

*Proof.* Suppose there is a point $p$ other than $c$ not on the axis, that is fixed by $\phi$. Let $q$ be any other point different from $c$ not on the axis. Then, as there are two fixed point on the line $qp$ ($p$ and the point of intersection with the axis), the line $qp$ is fixed. Then $q$ is mapped to the point of intersection of $qp$ and $cq$, which are both fixed. Hence $q$ is fixed, and $\phi$ is the identity function. □

**Theorem 47.** *The set of all $(c, l)$-collineations of a projective plane form a group under composition of functions.*

*Proof.* The set of $(c, l)$-collineations of a projective plane $\Pi$ is obviously a subset of the set of all collineations of $\Pi$, which by Theorem 38 is a group under composition of functions.

The identity is certainly a $(c, l)$-collineation. If two collineations $\phi$ and $\theta$ fix all lines on $c$ and all points of $l$, then it is obvious that $\phi \circ \theta$ and $\theta \circ \phi$ also fix all lines on $c$ and all points of $l$.

Finally, we need to show that the inverse of a $(c, l)$-collineation is again a $(c, l)$-collineation. So, let $\phi$ be a $(c, l)$-collineation. As $\phi$ is bijective, and fixes $c$ and all points of $l$, $\phi^{-1}$ also fixes $c$ and all points of $l$. We must also show that $\phi^{-1}$ fixes all lines on $c$.

So suppose, for a contradiction, that there is a line $l'$ on $c$ such that $\phi^{-1}(l') \neq l'$. But then, as $l'$ is fixed by $\phi$,

$$l' = \phi^{-1}(\phi(l')) = \phi^{-1}(l') \neq l',$$

a contradiction. Hence $\phi^{-1}$ fixes all lines on $l$ and is indeed a $(c, l)$-collineation, which completes the proof. □

**Example 48** The only $(c, l)$-collineation of the Fano plane where $c \notin l$ is the identity. This follows from the fact that any line on the center is also on the axis. Thus any line on the center has two of its points fixed, which implies that the third point of this line is also fixed. As all points are on a line on the center, all points of the plane must be fixed. Thus the group of $(c, l)$-collineations of the Fano plane where $c \notin l$ is the trivial group, consisting of only the identity.

The group of $(c, l)$-collineations of the Fano plane where $c \in l$ however is not trivial. Any point not on the axis can either be fixed by the collineation (in which case the collineation is the identity), or it can be mapped to the third point of the line on this point and the center. Hence there are only two elements in this group and it is thus isomorphic to $\mathbb{Z}_2$.

**Definition 49 ($(c,l)$-transitive).** *A projective plane $\Pi$ is said to be* **$(c,l)$-transitive** *if, for any to points $p$, and $p'$ such that neither is in $\{c\} \cup l$ and $p'$ is on the line $cp$, there exists a $(c,l)$-collineation mapping $p$ to $p'$.*

The Fano plane is easily seen to be $(c,l)$-transitive.

**Example 50** Let $\Pi$ be the projective real plane, and let $c = (0)$ and $l$ be the line at infinity. We shall show that $\Pi$ is $(c,l)$-transitive. We must construct a $(c,l)$-collineation which, for any two points $p$ and $p'$ different from $c$ and not on $l$ such that $p'$ is on the line $cp$, maps $p$ to $p'$.

So, let $p$ and $p'$ be any two points such that $p'$ is on the line $cp$. Then both $p$ and $p'$ are on a line with equation $y = m$, with the point (0) added. Thus, if $p = (x, y)$, then $p' = (x + n, y)$ for some $n \in \mathbb{R}$. Hence, any point $q = (x', y')$ is mapped to $(x' + n, y')$. As all points on the line at infinity are fixed, the collineation is now defined for all points of $\Pi$, and we know from Example 37 that this is indeed a collineation. Thus $\Pi$ is $(c,l)$-transitive.

**Definition 51 (Complete set of central collineations).** *A projective plane $\Pi$ is said to have a* **complete set of central collineations** *if $\Pi$ is $(c,l)$-transitive for any $c$ and $l$ of $\Pi$.*

## 2.3 The Desargues configuration

Let $\Pi$ be a projective plane, and let $\phi$ be a non-identity $(c,l)$-collineation of $\Pi$. Let $x, y$ and $z$ be points of $\Pi$ different from $c$ and not on $l$, and let $x' = \phi(x)$, $y' = \phi(y)$ and $z' = \phi(z)$ (see Figure 2.5). Let $u$ be the point of intersection of the lines $xy$ and $x'y'$. As we have seen earlier, for any line $l'$ other than the axis, the point of intersection of $l'$ and $\phi(l')$ is the point where $l'$ intersects the axis. Thus the point $u$ is on the axis.

Now, let $v$ be the point of intersection of the lines $xz$ and $x'z'$, and let $w$ be the point of intersection of the lines $yz$ and $y'z'$. As above, both $v$ and $w$ are on the axis. Thus the three points $u$, $v$ and $w$ are collinear.

Any set of 10 points configured as in Figure 2.5 are called a *Desargues* (or *Desarguesian*) configuration. That is, a set of 10 points $c, x, x', y, y', z, z', u, v$ and $w$ such that $c, x$ and $x'$ are collinear, as are $c, y, y'$ and $c, z, z'$. Furthermore the points $x, y$ and $z$ are not collinear, nor are $x', y', z'$. The points $u$, $v$ and $w$ are the intersection points of lines $xy$ and $x'y'$, $xz$ and $x'z'$, and $yz$ and $y'z'$ respectively. Finally, the points $u$, $v$ and $w$ are collinear. The following theorem follows directly from the first paragraph of this section.

**Theorem 52.** *Let $\Pi$ be a projective plane not of order 2 (it does not have to be finite), and let $\phi$ be a non-identity $(c,l)$-collineation. Let $x, y$ and $z$ be three points different from $c$ and not on the axis, that are not collinear. Then $\phi$ together with the three points $x, y$ and $z$ gives rise to a Desargues configuration.*

The reason why the order 2 case is excluded from the previous theorem is because there are no three points $x, y, z$ satisfying the give condition.

If for any set of points $c, x, x', y, y', z, z'$ chosen in the required way the three points $u$, $v$ and $w$ are always collinear, then the plane is said to be *Desarguesian* . We can now see the Fano plane to be Desarguesian in a vacuous sense; there is no way of choosing the 7 points in the desired way, and hence there is no way of choosing them such that the points $u, v$ and $w$ are *not* collinear.

It can be shown that a projective plane is Desarguesian if and only if it has a complete set of central collineations. We will only prove this one way, the reader is referred to [1] for the other.

**Theorem 53.** *If projective plane $\Pi$ has a complete set of central collineations, then it is Desarguesian.*

*Proof.* Let $c, x, x', y, y', z$ and $z'$ be chosen appropriately (see Figure 2.5). Now, let $u$ be the intersection of $xy$ and $x'y'$, $v$ the intersection of $xz$ and $x'z'$ and let $w$ be the intersection of $yz$ and $y'z'$. As $\Pi$ has a complete set of central collineations, there is a $(c, uv)$-collineation $\phi$ that takes $x$ to $x'$. As $u$ is fixed by $\phi$, we see that $\phi(ux) = ux'$. By the definition of $u$ we have that $y' \in ux'$, and also $y' \in cy$, as $\phi$ has center $c$. From this it follows that $\phi(y) = y'$. Similarly, $\phi(z) = z'$. It remains to show that $w \in uv$. As $\phi(w)$ is on both $cw$ and $y'z'$, and as these points intersect in $w$, we see that $w$ is fixed by $\phi$. As $\phi$ is not the identity, it follows from Corollary 46 that $w$ is either the center or a point of the axis. If $w$ is on the axis, the proof is complete. So suppose that $w = c$. As $c$ then is on both $zz'$ and $yz$, this implies that $c = z$, which yields a contradiction. □

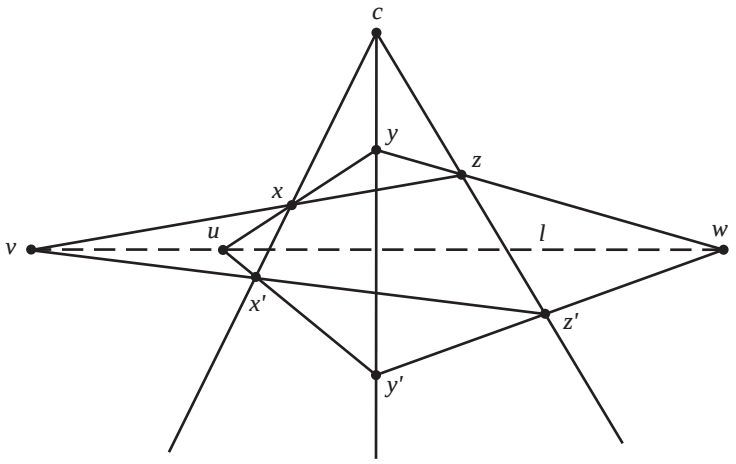



Figure 2.5: A Desargues configuration.

We will conclude this chapter with a theorem that shows that projective planes constructed from fields are in fact always Desarguesian.

**Theorem 54.** *Any projective plane $PG(2, F)$ constructed from a field $F$ is Desarguesian.*

*Proof.* As was noted previously, $PG(2, 2)$ is Desarguesian, so we can assume that $F \neq \mathbb{F}_2$ and we can choose the 10 points as required. Let $\Pi = PG(2, F)$. Let $c, x, x', y, y', z, z', u, v$ and $w$ be chosen as in Figure 2.5. We must show that $u$, $v$ and $w$ are collinear. The four points $c, x, y$ and $z$ form a quadrangle of $\Pi$, and as was noted in the beginning of this chapter these can be assumed to have coordinates $[1, 1, 1], [1, 0, 0], [0, 1, 0]$ and $[0, 0, 1]$ respectively.

As $x'$ is on the line $cx$, we have that $x' = \alpha[1, 1, 1] + \beta[1, 0, 0] = [\alpha + \beta, \alpha, \alpha] = [r, 1, 1]$ for some $r \in F$, as $\alpha$ is not zero (since $x' \neq c$). Similarly, $y' = [1, s, 1]$ and $z' = [1, 1, t]$ for some $s, t \in F$.

As $u$ is on the line $xy$, we have that $u = \gamma[1, 0, 0] + \delta[0, 1, 0] = [1, a, 0]$ for some $a \in F$. On the other hand, $u$ is also on the line $x'y'$, so

$$u = \gamma'[r, 1, 1] + \delta'[1, s, 1] = [\gamma' r + \delta', \gamma' + \delta' s, \gamma' + \delta'].$$

As the third co-ordinate of $u$ should be zero, we see that $\delta' = -\gamma'$ and hence

$$u = [\gamma' r - \gamma, \gamma' - \gamma' s, \gamma' - \gamma'] = [r - 1, 1 - s, 0] = [1, (1 - s)(r - 1)^{-1}, 0].$$

Similarly, $v = [1, 0, (1 - t)(r - 1)^{-1}]$ and $w = [0, 1, (1 - t)(s - 1)^{-1}]$. Now,

$$\begin{aligned}
\begin{vmatrix} u \\ v \\ w \end{vmatrix} &= \begin{vmatrix} 1 & (1-s)(r-1)^{-1} & 0 \\ 1 & 0 & (1-t)(r-1)^{-1} \\ 0 & 1 & (1-t)(s-1)^{-1} \end{vmatrix} \\
&= 1 \begin{vmatrix} 0 & (1-t)(r-1)^{-1} \\ 1 & (1-t)(s-1)^{-1} \end{vmatrix} - 1 \begin{vmatrix} (1-s)(r-1)^{-1} & 0 \\ 1 & (1-t)(s-1)^{-1} \end{vmatrix} \\
&= -(1-t)(r-1)^{-1} - (1-s)(r-1)^{-1}(1-t)(s-1)^{-1} \\
&= -(1-t)(r-1)^{-1} + (s-1)(s-1)^{-1}(1-t)(r-1)^{-1} \\
&= -(1-t)(r-1)^{-1} + (1-t)(r-1)^{-1} = 0.
\end{aligned}$$

By Lemma 30, $u$, $v$ and $w$ are thus collinear, and we are done. □

# Chapter 3

# The Bruck-Ryser Theorem

In the last chapter we saw that fields can be used to construct projective planes. If the field is finite the projective plane is also finite, and the order of the plane is the same as the order of the field. Thus by Galois' Theorem, there exists a projective plane of order $q$ for any primer power $q$.

The purpose of this essay is to consider for which orders projective planes exist. This would be an easy task if all projective planes could be constructed from fields. Then there would exist a unique projective plane for each prime power, and no other finite plane would exist. However, this is not the case. For example, it is known that there exist four non-isomorphic projective planes of order nine (see, for example [4]).

The strongest known theorem on the existence of projective planes is Theorem 33. The strongest theorem on *non-existence* is the Bruck-Ryser theorem. This chapter will be entirely devoted to the proof of this theorem. The proof relies on the algebraic properties of the incidence matrix of a projective plane, and not so much on the geometric properties of projective planes. This makes this proof a lot different from the proofs seen earlier in this essay.

For the proof, we will need some results from number theory, so we will start with those. The proofs of the first two are basically just long calculations. They can be found in Appendix A. The proof of Lemma 58 is similar to the proof of Lemma 57, but is a bit more complex, so to not get stuck on all this number theory, its proof can be found in Appendix B.

**Lemma 55 (The Four-Squares Identity).** *If $b_1, b_2, b_3, b_4, x_1, x_2, x_3, x_4$ are integers, then*

$$(b_1^2 + b_2^2 + b_3^2 + b_4^2)(x_1^2 + x_2^2 + x_3^2 + x_4^4) = y_1^2 + y_2^2 + y_3^2 + y_4^2 \tag{3.1}$$

*where the y's are integers and*

$$\begin{aligned} y_1 &= b_1x_1 + b_2x_2 + b_3x_3 + b_4x_4 \\ y_2 &= -b_2x_1 + b_1x_2 - b_4x_3 + b_3x_4 \\ y_3 &= -b_3x_1 + b_4x_2 + b_1x_3 - b_2x_4 \\ y_4 &= -b_4x_1 - b_3x_2 + b_2x_3 + b_1x_4. \end{aligned} \tag{3.2}$$

*There is also a similar* two-squares identity*: If $b_1, b_2, x_1, x_2$ are integers, then*

$$(b_1^2 + b_2^2)(x_1^2 + x_2^2) = y_1^2 + y_2^2 \tag{3.3}$$

*where the y's are integers and*

$$\begin{aligned} y_1 &= b_1x_1 - b_2x_2 \\ y_2 &= b_1x_2 + b_2x_1. \end{aligned} \tag{3.4}$$

By letting $\mathbf{x} = (x_1, x_2, x_3, x_4), \mathbf{y} = (y_1, y_2, y_3, y_4)$, we can represent equation (3.2) by $\mathbf{y} = \mathbf{x}B$, where

$$B = \begin{bmatrix} b_1 & b_2 & b_3 & b_4 \\ -b_2 & b_1 & -b_4 & b_3 \\ -b_3 & b_4 & b_1 & -b_2 \\ -b_4 & -b_3 & b_2 & b_1 \end{bmatrix}. \tag{3.5}$$

**Lemma 56.** *Let $B$ be the $4 \times 4$ matrix determined by (3.5). Then det(B) $= (b_1^2 + b_2^2 + b_3^2 + b_4^2)^2$, and hence $B$ is invertible if and only if at least one of the b's is different from zero.*

This means that if not all the $b$'s are zero, we can solve equation (3.2) for the $x$'s.

**Lemma 57.** *If $p$ is an odd prime, and there exists integers $x_1$ and $x_2$ such that $x_1^2+x_2^2 \equiv 0 \pmod{p}$, then $p$ is the sum of two integer squares.*

*Proof.* Since $x_1^2 + x_2^2 \equiv 0 \pmod{p}$, we have that $rp = x_1^2 + x_2^2$ for some positive integer $r$. Take such an expression that makes $r$ the smallest such number. The lemma is proven if we can show that $r = 1$.

We'll use contradiction, so assume that $r > 1$. Now choose $u_1$ and $u_2$ such that $u_1 \equiv x_1 \pmod{r}$, $u_2 \equiv -x_1 \pmod{r}$ and $|u_i| \leq r/2$ for $i = 1, 2$. This can be done, as of all integers $n$, $-r/2 \leq n \leq r/2$, one has to equal $x_1 \pmod{r}$, and one has to equal $-x_2 \pmod{r}$.

Then

$$u_1^2 + u_2^2 \equiv x_1^2 + x_2^2 \equiv 0 \pmod{r},$$

so $rs = u_1^2 + u_2^2$ for some positive integer $s$. Since

$$s = \frac{rs}{r} = \frac{u_1^2 + u_2^2}{r} \leq \frac{(r/2)^2 + (r/2)^2}{r} = r/2,$$

we have that $s < r$. Now,

$$r^2sp = (rp)(rs) = (x_1^2 + x_2^2)(u_1^2 + u_2^2) = (x_1u_1 - x_2u_2)^2 + (x_1u_2 + x_2u_1)^2 \tag{3.6}$$

by the two-squares identity. By the way $u_1$ and $u_2$ were defined, we also have

$$x_1u_1 - x_2u_2 \equiv x_1^2 + x_2^2 \equiv 0 \pmod{r}$$

and

$$x_1u_2 + x_2u_1 \equiv -x_1x_2 + x_2x_1 \equiv 0 \pmod{r},$$

so both terms of the right side of (3.6) has a factor $r^2$. Hence,

$$sp = y_1^2 + y_2^2,$$

where $y_1 = (x_1u_1 - x_2u_2)/r$, $y_2 = (x_1u_2 + x_2u_1)/r$. Hence, $s$ is an integer less than $r$, such that $sp$ is the sum of two integer squares. But $r$ was assumed to be the least such integer, hence we have a contradiction. Our assumption that $r > 1$ must be false, so $r = 1$. This proves the lemma. □

**Lemma 58 (Lagrange).** *Any positive integer can be written as the sum of four squares.*

As was pointed out before, the proof of the Theorem of Lagrange can be found in Appendix B.

**Lemma 59.** *For any integer $n$, if the equation $x^2 + y^2 = nz^2$ has an integer solution with $x, y, z$ not all zero, then $n$ is the sum of two squares.*

*Proof.* Suppose that there exists integer $x, y, z$ and satisfying the equation. We may assume that $x, y$ and $z$ has no common factors, as any common factor can be canceled from the equation. We will first prove it in the case where $n$ is a square free integer, as the general case then easily follows. So, assume that $n$ is a square free number, say $n = p_1p_2 \cdots p_k$, where each $p_i$ are distinct. No $p_i$ divides both $x$ and $y$, as then either $n$ would be divisible by $p_i^2$ (which it is not), or $z$ would be divisible by $p_i$ (which contradicts the fact that $x, y$ and $z$ has no common factors). Now, as we can rewrite the equation as

$$x^2 + y^2 = p_1p_2 \cdots p_kz^2,$$

we see that $x^2 + y^2 \equiv 0 \pmod{p_i}$ for all $p_i$. Then, by Lemma 57, all $p_i$ are sums of two squares. Let $p_i = x_i^2 + y_i^2$, then

$$n = p_1p_2 \cdots p_k = (x_1^2 + y_1^2)(x_2^2 + y_2^2) \cdots (x_k^2 + y_k^2).$$

By successively using the two-squares identity $k - 1$ times, we can reduce the right hand side to a sum of two integer squares. Hence the Lemma holds when $n$ is square free.

Now, assume that $n$ is not a square free integer, say $n = mu^2$, where $m$ is square free. Then we can rewrite the equation as

$$x^2 + y^2 = m(uz)^2.$$

As $m$ is square free, by what we previously proved, $m$ can be written as the sum of two integer squares, say $m = r^2 + s^2$. Then $n = mu^2 = (r^2 + s^2)u^2 = (ru)^2 + (su)^2$, so $n$ is the sum of two integer squares, and the proof is complete. □

Now we have all the number theoretic machinery needed to prove the Bruck-Ryser theorem. The theorem itself may seem rather technical, but it has an important corollary, given after the proof.

**Theorem 60 (Bruck-Ryser).** *If a projective plane of order $n$ exists, then the equation*

$$z^2 = nx^2 + (-1)^{n(n+1)/2}y^2$$

*has a solution in integers $x$, $y$ and $z$ not all zero.*

*Proof.* Suppose a projective plane of order $n$ exists. Let $N = n^2 + n + 1$ be the number of points and lines in the plane. Let the incidence matrix of this plane be $A$, which is a $N \times N$-matrix.

Now choose $\mathbf{x} = (x_1, \ldots, x_N)$ where $x_i \in \mathbb{Q}$ for $1 \leq i \leq N$, and let $\mathbf{z} = (z_1, \ldots, z_N)$ where $\mathbf{z} = A\mathbf{x}$, which expresses the $z$'s as a linear combination of the $x$'s. By Lemma 28 we have that

$$\mathbf{z}^T\mathbf{z} = \mathbf{x}^T A^T A\mathbf{x} = \mathbf{x}^T(nI + J)\mathbf{x} = \mathbf{x}^T nI\mathbf{x} + \mathbf{x}^T J\mathbf{x} = n\mathbf{x}^T\mathbf{x} + \mathbf{x}^T J\mathbf{x}. \tag{3.7}$$

We note that

$$\mathbf{z}^T\mathbf{z} = (z_1, \ldots, z_n)\begin{pmatrix} z_1 \\ \vdots \\ z_N \end{pmatrix} = z_1^2 + \cdots + z_N^2,$$

$$n\mathbf{x}^T\mathbf{x} = n(x_1, \ldots, x_N)\begin{pmatrix} x_1 \\ \vdots \\ x_N \end{pmatrix} = n(x_1^2 + \cdots x_N^2)$$

and

$$\begin{aligned}\mathbf{x}^T J\mathbf{x} &= (x_1, \ldots, x_N)\begin{pmatrix} 1 & \ldots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \ldots & 1 \end{pmatrix}\begin{pmatrix} x_1 \\ \vdots \\ x_N \end{pmatrix} \\ &= (x_1 + \cdots + x_N, \ldots, x_1 + \cdots + x_N)\begin{pmatrix} x_1 \\ \vdots \\ x_N \end{pmatrix} \\ &= (x_1 + \cdots + x_N)^2.\end{aligned}$$

Now we can write (3.7) as

$$z_1^2 + \cdots + z_N^2 = n(x_1^2 + \cdots + x_N^2) + \omega^2 \tag{3.8}$$

where $\omega = x_1 + \cdots + x_N$ and the $z$'s are integer linear combinations of the $x$'s. By Lemma 58, $n$ can be written as the sum of four squares, so we can write $n = b_1^2 + b_2^2 + b_3^2 + b_4^2$ where the $b$'s are integers. Now we can use Lemma 55 on the $b$'s and the $x$'s, four at a time, but this may leave som $x$'s if $N$ is not divisible by four. What possibilities do we have for $N$? We get two cases: if $n = 0, 4 \pmod 4$ then $N = 1 \pmod 4$, if $n = 1, 2 \pmod 4$ then $N = 3 \pmod 4$. We start by looking at the latter case.

So, suppose that $n = 1, 2 \pmod 4$ so that $N = 3 \pmod 4$. Choose $x_{N+1}$ to be a rational number, and add $nx_{N+1}^2$ to both sides of equation (3.8). We then get

$$z_1^2 + \cdots + z_N^2 + nx_{N+1}^2 = (b_1^2 + b_2^2 + b_3^2 + b_4^2)(x_1^2 + \cdots + x_N^2 + x_{N+1}^2) + \omega^2. \tag{3.9}$$

Note that $N + 1 = 0 \pmod 4$, so we can use Lemma 55 on the $b$'s and $x$'s four at a time to get

$$z_1^2 + \ldots + z_N^2 + nx_{N+1}^2 = y_1^2 + \ldots + y_{N+1}^2 + \omega^2, \tag{3.10}$$

where the $y$'s are integer linear combinations of the $x$'s. Let $\mathbf{y} = (y_1, \ldots, y_{N+1})$ and let $\mathbf{x}' = (x_1, \ldots, x_N, x_{N+1})$. As the $y$'s are integer linear combinations of the $x$'s, there exists a $(N + 1) \times (N + 1)$-matrix $B$ with integer entries such that

$$\mathbf{y} = B\mathbf{x}'. \tag{3.11}$$

By Lemma 56, $B$ is invertible. Thus, $\mathbf{x}' = B^{-1}\mathbf{y}$. Let $A'$ be the matrix $A$ with one more columna at the far right with all entries zero. $A'$ is then a $N \times (N+1)$-matrix such that $A'\mathbf{x}' = A\mathbf{x}$. Then

$$\mathbf{z} = A\mathbf{x} = A'\mathbf{x}' = A'B^{-1}\mathbf{y} = C\mathbf{y}, \tag{3.12}$$

where the matrix $C$ has rational entries. As the $x$'s were chosen arbitrarily, and there is a one-to-one correspondence between the $x$'s and the $y$'s by the matrix $B$, we could see it instead of as choosing the $y$'s. Furthermore, as the $z$'s are linear combinations of the $y$'s, the following way of choosing the $y$'s enables us to cancel most of the terms in equation (3.10).

As the $z$'s are rational linear combinations of the $y$'s, $z_1 = c_{11}y_1 + \cdots + c_{1(N+1)}y_{N+1}$ for some rational numbers $c_{11}, \ldots, c_{1(N+1)}$. If $c_{11} \neq 1$ we can set

$$y_1 = \frac{1}{1-c_{11}}(c_{12}y_2 + \cdots + c_{1(N+1)}y_{N+1})$$

so that

$$\begin{aligned} z_1 &= \frac{c_{11}}{1-c_{11}}(c_{12}y_2 + \cdots + c_{1(N+1)}y_{N+1}) + c_{12}y_2 + \cdots + c_{1(N+1)}y_{N+1} \\ &= \Big(\frac{c_{11}}{1-c_{11}} + 1\Big)(c_{12}y_2 + \cdots + c_{1(N+1)}y_{N+1}) \\ &= \frac{1}{1-c_{11}}(c_{12}y_2 + \cdots + c_{1(N+1)}y_{N+1}) = y_1. \end{aligned}$$

If $c_{11} = 1$ we can set

$$z_1 = -\frac{1}{2}(c_{12}y_2 + \cdots + c_{1(N+1)}y_{N+1})$$

so that

$$\begin{aligned} z_1 &= -\frac{1}{2}(c_{12}y_2 + \cdots + c_{1(N+1)}y_{N+1}) + c_{12}y_2 + \cdots + c_{1(N+1)}y_{N+1} \\ &= \frac{1}{2}(c_{12}y_2 + \cdots + c_{1(N+1)}y_{N+1}) = -y_1. \end{aligned}$$

In any case, $y_1$ is expressed in terms of the other $y$'s, and $z_1^2 = y_1^2$. By continuing like this, we can choose the $y$'s such that $y_i^2 = z_i^2$ for $i = 1, \ldots, N$. Equation (3.10) is then reduced to

$$nx_{N+1}^2 = y_{N+1}^2 + \omega^2, \tag{3.13}$$

where $x_{N+1}$ and $\omega$ are rational linear combinations of $y_{N+1}$, i.e. $x_{N+1} = ky_{N+1}$ and $\omega = k'y_{N+1}$ for some rational numbers $k$ and $k'$. So, by letting $y_{N+1}$ equal the least common multiple of the denominators of $k$ and $r$ we see that $x_{N+1}$ and $\omega$ are integers. Hence, equation (3.13) has an integer solution.

Now let's consider the case $n = 0, 3 \pmod 4$, so that $N = 1 \pmod 4$. As $N - 1 \equiv 0 \pmod 4$, we can use lemma 55 on the $b$'s and $x$'s four at a time and get one $x$ left.

$$z_1^2 + \cdots + z_N^2 = (b_1^2 + b_2^2 + b_3^2 + b_4^2)(x_1^2 + \cdots + x_{N-1}^2) + nx_N^2 + \omega^2 \tag{3.14}$$

$$z_1^2 + \cdots + z_N^2 = y_1^2 + \cdots + y_{N-1}^2 + nx_N^2 + \omega^2 \tag{3.15}$$

By proceeding as above, we can choose the $y$'s in such a way that they cancel the first $N-1$ $z$'s. We then get

$$z_N^2 = nx_N^2 + \omega^2, \tag{3.16}$$

where $z_N$ and $\omega$ are rational linear combinations of the independent $x_N$. As before, we can choose an integer value of $x_N$ such that both $z_N$ and $\omega$ are integers. Cleaning up the notations a bit, we have found that if a projective plane of order $n \equiv 1, 2 \pmod 4$ then

$$z^2 = nx^2 - y^2 \tag{3.17}$$

has integer solutions not all zero, and if $n \equiv 0, 3 \pmod 4$ then

$$z^2 = nx^2 + y^2 \tag{3.18}$$

has integer solutions not all zero. Noting that if $n \equiv 1, 2 \pmod 4$ then $n(n+1)/2$ is an odd number, and if $n \equiv 0, 3 \pmod 4$ then $n(n+1)/2$ is an even number, we can write equations (3.17) and (3.18) as

$$z^2 = nx^2 + (-1)^{n(n+1)/2} y^2. \tag{3.19}$$

Thus, we have proven that if a projective plane of order $n$ exists, then equation (3.19) has integer solutions, not all zero. □

We now sum up all we know about the existence of projective planes in the following important proposition.

**Proposition 61.** *Let $n$ be a positive integer, then*

*A) if $n$ is a prime power, at least one projective plane of order $n$ exists.*

*B) if $n \equiv 1$ or $2$ (mod 4), and is not the sum of two squares, then no projective planes of order $n$ exists.*

*C) In any other case, a projective plane of order $n$ may or may not exist.*

*Proof.* Part (A) follows from theorem 33. Part (B) is true, since if $n = 1$ or $2 \pmod 4$, then by the Bruck-Ryser theorem the equation

$$nx^2 = y^2 + z^2$$

has integer solutions. By Theorem 59 this implies that $n$ can be written as a sum of two squares. Hence, if $n$ is *not* the sum of two squares, no projective plane of order $n$ exists. Part (C) is obvious. □

It should be noted that the Bruck-Ryser Theorem does not say anything about the existence of projective planes of order $n$ when $n \equiv 0$ or $3 \pmod 4$, since the equation $z^2 = nx^2 + y^2$ always has the solution $x = 0$, $y = z$.

**Example 62** Let us conclude this chapter by using Proposition 61 to see what planes of order less than or equal to 25 does/doesn't/might exist. First of all, by part A of proposition 61, a plane exist for orders 2, 3, 4, 5, 7, 8, 9, 11, 13, 16, 17, 19, 23 and 25, as these are all prime powers.

Now, let's check which orders are excluded by part B of proposition 61. The numbers that are equal to 1 or 2 mod 4 that are not prime powers are 6, 10, 14, 18, 21 and 22. On the other hand, the numbers (greater than one, less than or equal to 25) that are sums of two integer squares are

$$\begin{aligned}
1^2 + 1^2 &= 2 & 1^2 + 2^2 &= 5 \\
1^2 + 3^2 &= 10 & 1^2 + 4^2 &= 17 \\
2^2 + 0^2 &= 4 & 2^2 + 2^2 &= 8 \\
2^2 + 3^2 &= 13 & 2^2 + 4^2 &= 20 \\
3^2 + 0^2 &= 9 & 3^2 + 3^2 &= 18 \\
3^2 + 4^2 &= 25 & 4^2 + 0^2 &= 16 \\
5^2 + 0^2 &= 25
\end{aligned}$$

We see that the numbers that are excluded by part B of Proposition 61 are 6, 14, 21 and 22 as these are not the sums of two integer squares. For all remaining integers, projective planes of that order may, or may not exist. We summarize these results in table 3. In the cases where conclusions can be made on the existence of a projective plane of a certain order, the reason is indicated in the 'Comment' column. 'PP' indicates that the order is a prime power, and 'BR' indicates that no projective plane exist due to the Bruck-Ryser Theorem.

| $n$ | Conclusion made by Proposition 61 | Comment |
|---|---|---|
| 2 | Exist | PP |
| 3 | Exist | PP |
| 4 | Exist | PP |
| 5 | Exist | PP |
| 6 | Does not exist | BR |
| 7 | Exist | PP |
| 8 | Exist | PP |
| 9 | Exist | PP |
| 10 | May exist | |
| 11 | Exist | PP |
| 12 | May exist | |
| 13 | Exist | PP |
| 14 | Does not exist | BR |
| 15 | May exist | |
| 16 | Exist | PP |
| 17 | Exist | PP |
| 18 | May exist | |
| 19 | Exist | PP |
| 20 | May exist | |
| 21 | Does not exist | BR |
| 22 | Does not exist | BR |
| 23 | Exist | PP |
| 24 | May exist | |
| 25 | Exist | PP |

Table 3.1: What can be said on the existence of projective planes of small order by Proposition 61.

# Chapter 4

# The Search for a Projective Plane of Order 10

The final proposition of the last chapter sums up our results so far regarding the existence/nonexistence of finite projective planes. As we saw in Example 62 there are a lot of orders for which we have no way of telling whether or not a plane of that order exists. The first such order is 10. It was an open question for a long time, but in 1989 it was shown by Lam, Thiel and Swiercz [13] [16] using an extensive computer search that such a plane does not exist.

This final chapter will look at how this search was done, and what mathematical ideas was used. We will start by looking at some theory needed to understand this.

## 4.1 The connection with coding theory

**Definition 63 (Binary code of a projective plane).** *Let* $\Pi$ *be a finite projective plane. The* **binary code** $C$ *of* $\Pi$ *is the vector space over* $\mathbb{F}_2$ *spanned by the rows of the incidence matrix of* $\Pi$*. An element of* $C$ *is called a* **code word**.

If we let $N = n^2 + n + 1$ we see that $C$ is a subspace of $\mathbb{F}_2^N$.

**Example 64** The binary code of the Fano plane of Example 10 is the vector space spanned by $[1,1,1,0,0,0,0]$, $[1,0,0,1,1,0,0]$, $[1,0,0,0,0,1,1]$, $[0,1,0,1,0,1,0]$, $[0,1,0,0,1,0,1]$, $[0,0,1,1,0,0,1]$ and $[0,0,1,0,1,1,0]$. Examples of code words are

$$\begin{aligned}
[0,0,0,0,0,0,0] &= [1,1,1,0,0,0,0] + [1,1,1,0,0,0,0],\\
[0,0,0,1,1,1,1] &= [0,0,1,1,0,0,1] + [0,0,1,0,1,1,0],\\
[0,1,1,1,1,0,0] &= [1,1,1,0,0,0,0] + [1,0,0,1,1,0,0],\\
&\text{and}\\
[1,1,0,1,0,0,1] &= [1,0,0,0,0,1,1] + [0,1,0,1,0,1,0].
\end{aligned}$$

Since the binary code of the Fano plane is a vector space, it is vital to investigate its dimension. We shall return to this example later, when we have developed some more machinery. We will then, among other things, determine its dimension.

Note that all operations are done in $\mathbb{F}_2$. As all code words are linear combinations of the rows of the incidence matrix, and all operations are in $\mathbb{F}_2$, we can always assume that each row occurs at most once in the sum.

Another observation that can be made is the following. Let $x$ be a code word that is a sum of the rows $r_1, \ldots, r_m$. Let $a_{ij}$ be the value of row $i$ in column $j$, and let $b_j$ be the value of $x$ in column $j$. Then

$$b_j = \sum_{i=1}^{m} a_{ij} \pmod 2.$$

From this we conclude that $x$ has a 1 in column $j$ if and only if an odd number of the rows $r_1, \ldots, r_m$ has a 1 in column $j$, and a 0 otherwise.

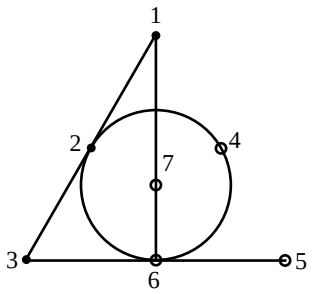



Figure 4.1: $x = l_1 + l_3 + l_4 + l_7$. The points of $x$ are 4, 5, 6, and 7.

In the same way as a point is on a line if the row corresponding to the line has a 1 in the column corresponding to the point, we say that a point is on a code word if the code word has a 1 in the column corresponding to the point. For example, the points on the code word $[0, 1, 1, 1, 1, 0, 0]$ of Example 64 are the points 2, 3, 4 and 5.

Instead of saying that a code word is the sum of a set of rows, we will often say that the code word is the sum of the corresponding set of lines. So, for example, we may write $x = l_1 + l_2 + l_3$, where the $l$'s are lines, which will mean the same as $x = r_1 + r_2 + r_3$, where the $r$'s are the rows corresponding to the lines. By the previous paragraphs, a point will be on $x$ if and only if it is on an odd number of the lines $l_1, l_2$ and $l_3$.

We will sometimes talk about the dot product of two lines, by which we will mean the dot product of the corresponding rows. In the same way, we may talk about the dot product of two code words, or of the dot product of a code word and a line. Note that the dot product of two code words counts the number of columns that both code words has a 1 in, mod 2.

**Example 65** Let $C$ be the code of Example 64. Let $x = l_1 + l_3 + l_4 + l_7$. In figure 4.1 the points of the Fano plane has been drawn, together with the lines in the sum making up $x$. We easily see that the points with an odd number of lines on them are 4, 5, 6 and 7, so $x = [0, 0, 0, 1, 1, 1, 1]$. The reader is advised to check that indeed you get the same result when actually doing the calculation. Note that there are other ways of writing $x$ as a sum of lines. For example, $x = l_2 + l_3 = l_6 + l_7$.

**Definition 66 (Weight).** *The* **weight** $w(x)$ *of a code word* $x$ *is the number nonzero entries in* $x$*.*

**Example 67** If $x_1 = [1, 1, 1, 0, 0, 0, 0]$, $x_2 = [0, 0, 0, 0, 0, 0, 0]$ and $x_3 = [0, 0, 0, 1, 1, 1, 1]$ then $w(x_1) = 3$, $w(x_2) = 0$, $w(x_3) = 4$.

As each code word can be identified with the points on it, each code word of weight $i$ corresponds to a set of $i$ points. The code word of example 65 has weight 4, and as we have seen it corresponds to the four points 4, 5, 6 and 7.

**Lemma 68.** *Let* $x$ *be a code word, and* $l$ *any line of* $\Pi$*. Then* $w(x + l) = w(x) + n + 1 - 2k$*, where* $n$ *is the order of the plane and* $k$ *is the number of points where* $l$ *intersects* $x$*.*

*Proof.* Since $l$ has weight $n + 1$, the total number of nonzero columns of $x$ and $l$ is $w(x) + n + 1$. However, in the code word $x + l$, each of the columns that $x$ and $l$ has a 1 in common will have a 0, and these columns correspond precisely to the points of intersection of $x$ and $l$. So each of these points will 'remove' one 1 from $x$ and one 1 from $l$, and we get the formula. □

**Lemma 69.** *Let* $x = l_1 + \cdots + l_k$ *be a code word in the binary code of a projective plane* $\Pi$*, where the* $l_i$*'s are lines of* $\Pi$*, and let* $l$ *be any line of* $\Pi$*, different from the* $l_i$*'s. If* $k$ *is even then* $l$ *intersects* $x$ *in an even number of points, and if* $k$ *is odd then* $l$ *intersects* $x$ *in an odd number of points.*

*Proof.* Suppose that $x = l_1 + \cdots + l_k$, where, as noted earlier, each $l_i$ can be assumed to be distinct. Let $l$ be a line, where $l \neq l_i, 1 \leq i \leq k$, that is, $l$ is not one of the lines that make up $x$. Let $p_1, \ldots, p_m$ be the points where $l$ intersects the lines $l_1, \ldots, l_k$, where each point is unique (that is, if $l$ intersects $l_1$ and $l_2$ in the same point, this point occurs only once, say as point $p_1$). For each point $p_i$, let $L(p_i)$ denote the number of the lines $l_1, \ldots, l_k$ that is on $p_i$. Since each line is on exactly one of the points $p_1, \ldots, p_m$, we see that

$$\sum_{1}^{m} L(p_i) = k. \tag{4.1}$$

Also, as we have argued earlier, the line $l$ intersects $x$ in a point $p_i$ if and only if $L(p_i)$ is odd. Furthermore, $l$ does not intersect $x$ in any other points, by the way we have defined $p_i$.

Now suppose that $k$ is even. Then by equation (4.1) an even number of the $L(p_i)$'s must be odd. As $l$ intersects $x$ in precisely the points where $L(p_i)$ is odd, $l$ intersects $x$ in an even number of points.

Now suppose that $k$ is odd. Then by equation (4.1) an odd number of the $L(p_i)$'s must be odd. As above, $l$ intersects $x$ in an odd number of points. □

Lemma 69 can quite readily be extended to the case where the line is actually one of the lines in the sum of the code word.

**Corollary 70.** *Let $x$ be a code word in the binary code of a finite projective plane $\Pi$, and let $l$ be any line of $\Pi$. Then if $x$ is the sum of an odd number of lines, $l$ intersects $x$ in an even number of points, and if $x$ is the sum of an odd number of lines, $l$ intersects $x$ in an odd number of points.*

*Proof.* The case we need to consider here, which is not covered by Lemma 69, is the case where $l$ is one of the lines in the sum for $x$. So suppose that $x = l_1 + \cdots + l_k$, and let $l = l_i$ for some $i, 0 \leq i \leq k$. Let $x' = l_1 + \cdots + l_{i-1} + l_{i+1} + \cdots + l_k$. Then $x = x' + l$, and the points of $l$ that is on $x$ is precisely those points of $l$ that is *not* on $x'$. As any line of a projective plane always has an odd number of points, $l$ is on an odd number of points of $x$ if and only if $l$ is on an even number of points of $x'$, and vice versa.

As $x'$ is the sum of $k-1$ lines, and none of these are $l$, Lemma 69 shows that $l$ intersects $x'$ in an odd number of points if $k$ is even, and an even number of points if $k$ is odd. Hence $l$ intersects $x$ in an odd number of points if $k$ is odd, and an even number of points if $k$ is even, and the corollary is proven. □

**Corollary 71.** *Let $x$ be a code word of the binary code of a finite projective plane $\Pi$. Then either all sums of lines that equal $x$ are sums of an even number of lines, or all sums are sums of an odd number of lines.*

*Proof.* If $x$ could be written as both the sum of an even number of lines and an odd number of lines, by Corollary 70 any line would intersect $x$ in both an odd and an even number of points, which is impossible. □

**Definition 72 (Orthogonal dual code).** *Let $C$ be the binary code of a projective plane $\Pi$ of order $n$. The* **orthogonal dual code** *$C^\perp$ is the subspace of $\mathbb{F}_2^N$ such that*

$$C^\perp = \{u \in \mathbb{F}_2^N \mid u \cdot v = 0 \text{ for all } v \in C\},$$

*where $N = n^2 + n + 1$.*

From linear algebra, we know that $\dim(C^\perp) = N - \dim(C)$.

**Lemma 73.** *Let $C$ be the binary code of a finite projective plane $\Pi$. The elements of $C$ that are also in $C^\perp$ are precisely the code words $x$ that is a sum of an even number of lines.*

*Proof.* First, let $x'$ be the sum of two lines. Let $l$ be any line of $\Pi$. Then, by Lemma 69 $l$ intersects $x'$ in an even number of points, i.e. the number of columns that both has a 1 in is even. Hence $x' \cdot l = 0$. Now let $y = l_1 + \cdots + l_k$ be any code word of $C$. Then

$$x' \cdot y = x' \cdot (l_1 + \cdots + l_k) = x' \cdot l_1 + \cdots + x' \cdot l_k = 0 + \cdots + 0 = 0,$$

so $x' \in C^\perp$. Hence any code word of $C$ that is the sum of two lines is in $C^\perp$.

Now, let $x$ be a code word that is the sum of an even number of lines. then we can write $x = x_1 + \cdots x_m$, where each $x_i$ is the sum of two lines. Let $y$ be any code word of $C$. Then

$$x \cdot y = (x_1 + \cdots + x_m) \cdot y = x_1 \cdot y + \cdots + x_m \cdot y = 0 + \cdots + 0 = 0,$$

so $x \in C^\perp$.

Now, on the other hand, let $x$ be the sum of an odd number of lines. We can write $x = x' + l$ where $x'$ is a code word that is the sum of an even number of lines, and $l$ is a line. Let $l'$ be any line of $\Pi$ other than $l$. Then, we get

$$x \cdot l' = (x' + l) \cdot l' = x' \cdot l' + l \cdot l' = 0 + 1 = 1,$$

so $x \notin C^\perp$ and we are done. □

**Lemma 74.** *Let $C$ be the binary code of a finite projective plane $\Pi$. Then $C \cap C^\perp$ is of codimension 1 in $C$, that is,* $\dim(C \cap C^\perp) = \dim(C) - 1$.

*Proof.* First of all we note that, for any two lines $l, l'$ of $\Pi$ we have $l \cdot l' = 1$ as they intersect in one point. So for any line $l$ of $\Pi$ we have that $l \notin C^\perp$. Hence $\dim(C \cap C^\perp) < \dim(C)$.

Now, suppose that $\dim(C) = k$. As the lines of $\Pi$ span $C$ there exists a subset of $k$ lines that is a base for $C$. Let this base be $B = \{l_1, \ldots, l_k\}$. Consider the set $D = \{l_1 + l_2, l_1 + l_3, \ldots, l_1 + l_k\}$. Note that $|D| = k - 1$. As $B$ is linearly independent (as it is a base), and

$$\alpha_2(l_1 + l_2) + \alpha_3(l_1 + l_3) + \cdots + \alpha_k(l_1 + l_k) = (\alpha_2 + \cdots + \alpha_k)l_1 + \alpha_2 l_2 + \cdots + \alpha_k l_k,$$

we see that

$$\alpha_2(l_1 + l_2) + \alpha_3(l_1 + l_3) + \cdots + \alpha_k(l_1 + l_k) = 0$$

if and only if $\alpha_i = 0$ for $2 \leq i \leq k$. Thus $D$ is also linearly independent. Hence $D$ is a base for a vector space of dimension $k - 1$, that we will call $L$. Obviously, $L \subseteq C$, and as each element of $L$ is the sum of an even set of lines $L \subseteq C^\perp$ by Lemma 73. So, $L \subseteq C \cap C^\perp$.

Thus, $\dim(L) = k - 1 \leq \dim(C \cap C^\perp) < \dim(C) = k$, and this inequality can only be satisfied if $\dim(C \cap C^\perp) = \dim(C) - 1$, and we are done. □

**Lemma 75.** *Let $C$ be the binary code of a projective plane $\Pi$ of order $n$, where $n$ is divisible by 2 exactly once. Then $C^\perp \subset C$ and*

$$\dim(C) = \frac{n^2 + n + 2}{2}$$

*and*

$$\dim(C^\perp) = \frac{n^2 + n}{2}.$$

*Proof.* Let $A$ be the incidence matrix of $\Pi$. Let $N = n^2 + n + 1$ be the number of lines/points of $\Pi$. By Lemma 29

$$\det(A) = \pm(n + 1)n^{(n^2+n)/2}.$$

Add each column $j$ of $A$, $j = 1, \ldots, N - 1$, to column $N$ to obtain the matrix $A_1$. Every entry of column $N$ of $A_1$ is then $n + 1$. Subtract the last row of $A_1$ from all the other rows of $A_1$ to obtain the matrix $A_2$. We now have the matrix

$$A_2 = \left[\begin{array}{ccc|c} & & & 0 \\ & & & 0 \\ & B_2 & & \vdots \\ & & & 0 \\ \hline * & \cdots & * & n+1 \end{array}\right].$$

The operations used to transform $A$ into $A_2$ has all been elementary operations that preserve the absolute value of the determinant, so $|\det(A)| = |\det(A_2)|$. Furthermore, by cofactor expanding $A_2$ about the rightmost column, we see that $\det(A_2) = (n + 1)\det(B_2)$.

As $A_2$ is invertible, $B_2$ must also be invertible. We can thus act on $B_2$ using the elementary operations to put it in diagonal form, such that its determinant is preserved. We get

$$A_3 = UAV = \left[\begin{array}{cccc|c} h_1 & & & 0 & 0 \\ & h_2 & & & 0 \\ & & \ddots & & \vdots \\ 0 & & & h_{N-1} & 0 \\ \hline * & \cdots & \cdots & * & n+1 \end{array}\right],$$

where $U$ and $V$ are unimodal matrices, that is, matrices with determinant $\pm 1$. The absolute value of the determinant is still preserved, so we have $|\det(A)| = |\det(A_3)|$. Furthermore, $\det(A_3) = h_1 h_2 \cdots h_{N-1}(n+1)$. As $N - 1 = n^2 + n$, we have

$$h_1 h_2 \cdots h_{n^2+n} = \pm n^{(n^2+n)/2}.$$

As $n$ is divisible by 2 exactly once, it follows that at most $(n^2+n)/2$ of the $h$'s are divisible by 2. Considering $A_3$ as a matrix over $\mathbb{F}_2$, precisely those rows $i$ where $h_i$ is divisible by 2 will consist of only zeros, and the set of all nonzero rows will be linearly independent. Hence the rows of $A_3$ over $\mathbb{F}_2$ spans a vector space of dimension at least $n^2 + n + 1 - (n^2+n)/2 = (n^2+n+2)/2$.

As $U$ and $V$ are unimodal matrices, $A$ has the same rank as $A_3$. Thus

$$\dim(C) = \operatorname{rank}(A) = \operatorname{rank}(A_3) \geq (n^2+n+2)/2.$$

By Lemma 74, $\dim(C^\perp) \geq \dim(C) - 1 = (n^2+n)/2$. Since $\dim(C) + \dim(C^\perp) = n^2 + n + 1$, these inequalities imply that

$$\dim(C) = (n^2+n)/2$$

and

$$\dim(C^\perp) + 1 = (n^2+n+2)/2.$$

By Lemma 74, $\dim(C \cap C^\perp) = \dim(C) - 1$, so in fact $C \cap C^\perp = C^\perp$, which implies that $C^\perp \subset C$, and we are done. □

**Example 76** We can now use Lemma 75 to calculate the entire binary code of the Fano plane. The Fano plane is of order 2, which is divisible by 2 exactly once, so the lemma applies. Hence, $\dim(C) = (4+2+2)/2 = 4$. Thus, each base has four elements, and the number of linear combinations of these over $\mathbb{F}_2$ is $2^4 = 16$, so $|C| = 16$ and there are 16 code words in $C$. Also, $\dim(C^\perp = (4+2)/2 = 3$, so $|C^\perp| = 2^3 = 8$, and these eight code words are also in $C$. We will now calculate them.

A base for $C$ can easily be found, one is $\{l_1, l_2, l_3, l_4\}$, where, as before, $l_1 = [1,1,1,0,0,0,0]$, $l_2 = [1,0,0,1,1,0,0]$, $l_3 = [1,0,0,0,0,1,1]$, $l_4 = [0,1,0,1,0,1,0]$. Using this base we can calculate all code words of $C$. However, we will do it in a slightly different way, that will show us more of the actual structure of $C$. Obviously, the zero code word $\mathbf{0}$ is in $C$, and as the sum of all lines contains all points (as then each point is on three lines, which is odd) the unit vector $\mathbf{1}$ (having all entries 1) is also in $C$. For any line $l$, the code word $\mathbf{1} + l$ will contain precisely the points that is *not* on $l$. As there are seven lines, there are seven such complementary code words. Together with the zero vector and the unit vector, this is 16 code words, so all code words of $C$ is accounted for this way. Hence, any code word of $C$ is either the unit code word, a line, or the complement of any of these.

The following list lists the code words, where the unit code word and the lines are in the left column, and the zero code word and complements of the lines are in the right column.

| | |
|---|---|
| $[1,1,1,1,1,1,1]$ | $[0,0,0,0,0,0,0]$ |
| $[1,1,1,0,0,0,0]$ | $[0,0,0,1,1,1,1]$ |
| $[1,0,0,1,1,0,0]$ | $[0,1,1,0,0,1,1]$ |
| $[1,0,0,0,0,1,1]$ | $[0,1,1,1,1,0,0]$ |
| $[0,1,0,1,0,1,0]$ | $[1,0,1,0,1,0,1]$ |
| $[0,1,0,0,1,0,1]$ | $[1,0,1,1,0,1,0]$ |
| $[0,0,1,1,0,0,1]$ | $[1,1,0,0,1,1,0]$ |
| $[0,0,1,0,1,1,0]$ | $[1,1,0,1,0,0,1]$ |

Eight of these code words are in $C^\perp$. Obviously, $\mathbf{0} \in C^\perp$ and $\mathbf{1} \notin C^\perp$. Furthermore, as each line $l$ is the sum of an odd (1!) number of lines, none of these are in $C^\perp$. As there should be 8 elements in $C^\perp$, the seven code words not yet accounted for must be in $C^\perp$. Thus $C^\perp$ is the zero vector together with the complements of the lines (the right column in the list above).

**Definition 77 (Weight-enumerator).** *Let $C$ be the binary code of a projective plane of order $n$. The* **weight-enumerator** *of $C$ is the polynomial*

$$W_C(x, y) = \sum_{i=0}^{N} A_i x^{N-i} y^i,$$

*where $N = n^2+n+1$, and $A_i$ is the number of code words of weight $i$ in $C$. The weight-enumerator of the orthogonal dual of $C$ is defined in the same way.*

**Example 78** Let us calculate the weight-enumerator of the code $C$ and $C^\perp$ of the Fano plane. By the previous example, we see that $A_0 = A_7 = 1$, $A_1 = A_2 = A_5 = A_6 = 0$ and $A_3 = A_4 = 7$. Hence

$$W_C(x, y) = x^7 + 7x^4y^3 + 7x^3y^4 + y^7.$$

For $C^\perp$, we have $A_0 = 1$, $A_1 = A_2 = A_3 = A_5 = A_6 = A_7 = 0$ and $A_4 = 7$. Thus

$$W_{C^\perp}(x, y) = x^7 + 7x^3y^4.$$

The following important identity will be given without proof, as the proof requires more profound results from Coding Theory. For a proof, see for example Hall [15].

**Theorem 79 (McWilliams identity).** *The weight-enumerator of a binary code $C$ and of its orthogonal dual code $C^\perp$ are related to each other by*

$$W_{C^\perp}(x, y) = \frac{1}{|C|} W_C(x + y, x - y).$$

## 4.2 The code of a projective plane of order 10

We will now look closer at what properties a binary code $C$ of a projective plane of order 10 would have, if one would exist. Throughout this section, $C$ will be the code of a projective plane of order 10, and $\Pi$ will be the plane. We begin by observing that 10 is divisible by 2 exactly once, so by Lemma 75, $\dim(C) = (10^2 + 10 + 2)/2 = 56$, $\dim(C^\perp) = (10^2 + 10)/2 = 55$ and $C^\perp \subset C$.

**Lemma 80.** *Let $x$ be a code word of $C$. Then $w(x) \equiv 0 \pmod 4$ if $x$ is the sum of an even number of lines, and $w(x) \equiv 3 \pmod 4$ if $x$ is the sum of an odd number of lines.*

*Proof.* We will use induction on the number of lines in the sum equal to $x$. We start by observing that the zero code word (which is the sum of an even number of lines) has weight 0 (mod 4), and that any line (which is the sum of an odd number of lines) has weight $11 \equiv 3 \pmod 4$.

Now, suppose that $x$ is the sum of an even number of lines, and that $w(x) \equiv 0 \pmod 4$. We must show that $w(x+l) \equiv 3 \pmod 4$ for any line $l$ in $\Pi$. By Corollary 70, $l$ intersects $x$ in an even number of points, so let this number be $2k$. By Lemma 68 we have that

$$w(x + l) = w(x) + 11 - 4k \equiv 0 + 3 + 0 = 3 \pmod 4.$$

On the other hand, suppose that $x$ is the sum of an odd number of lines, let this number be $2k + 1$, and that $w(x) \equiv 3 \pmod 4$. Then we get

$$w(x + l) = w(x) + 11 - 2(2k + 1) \equiv 3 + 3 - 2 \equiv 0 \pmod 4,$$

and we are done. □

As the code words of weight 0 (mod 4) are sums of even sets of lines, each line intersects such code words in an even number of points, and as the code words of weight 3 (mod 4) are sums of odd sets of lines, each line intersects such code words in an odd number of points.

By Lemma 80 we see that for the coefficients of the weight enumerator $A_{4i+1} = A_{4i+2} = 0$ for $i = 0, \ldots, 27$. Also, the unit code word is in $C$ as the sum of all lines contains all points, so for each code word $x$ of weight $w(x)$ in $C$, there is a code word $x + \mathbf{1}$ of weight $111 - w(x)$ in $C$, so $A_i = A_{111-i}$. Hence the 28 numbers $A_{4i}, i = 1, \ldots, 27$ determines the entire weight enumerator. So

$$W_C(x, y) = \sum_{i=0}^{27} A_{4i} x^{111-4i} y^{4i} + \sum_{i=0}^{27} A_{4i+3} x^{108-4i} y^{4i+3}. \tag{4.2}$$

As $C^\perp$ is precisely the code words of $C$ that is the sum of an even set of lines, they are precisely the code words of even weight. Thus

$$W_{C^\perp}(x, y) = \sum_{i=0}^{27} A_{4i} x^{111-4i} y^{4i}.$$

Now, suppose there exists a code word $x$ of weight 3 or 7. Let $p$ be a point not on $x$. As $p$ is not on $x$, and $x$ has weight less than 11, it follows that there exists a line on $p$ that is not on $x$. But this contradicts the fact that each line intersects $x$ in an odd number of points. We have a contradiction, and thus no code word of weigh 3 or 7 exist, and $A_3 = A_7 = 0$.

Suppose that there exists a code word $x$ of weight 4 or 8, and let $p$ be a point on $x$. Then, as there are 11 lines on $p$, there exists a line on $p$ that is not on any of the other points of $x$. Thus this line intersect $x$ in exactly one point, which contradicts the fact that each line intersects $x$ in an even number of points. Hence no code word of weight 4 or 8 exist, and $A_4 = A_8 = 0$.

Finally, we will determine $A_{11}$. Any line is a code word of weight 11, so $A_{11} \geq 111$. Now, let $x$ be a code word of weight 11, and $p_1$ and $p_2$ be two points of $x$. Let $l$ be the line on $p_1$ and $p_2$. Suppose that there is a point $q$ on $l$ that is not on $x$. As there are at most 9 more points of $x$ not on $l$, and there are 10 other lines through $q$, there must be a line $l'$ on $q$ that contains no point of $x$. But all lines intersects $x$ in an odd number of points, which $l'$ does not, and we have a contradiction. Thus the code words of weight 11 are precisely the lines, and $A_{11} = 111$.

Obviously, the only code word of weight 0 is the zero code word, so $A_0 = 1$. Summing up, we have found that $A_0 = 1, A_1 = A_2 = \cdots = A_{10} = 0$ and $A_{11} = 111$.

Using the McWilliams identity, we find that

$$\begin{aligned} \sum_{i=0}^{27} A_{4i} x^{111-4i} y^{4i} = W_{C^\perp}(x, y) = \frac{1}{|C|} W_C(x + y, x - y) = \\ \frac{1}{|C|} \left( \sum_{i=0}^{27} A_{4i} (x + y)^{111-4i} (x - y)^{4i} + \sum_{i=0}^{27} A_{4i+3} (x + y)^{108-4i} (x - y)^{4i} \right). \end{aligned} \tag{4.3}$$

Now, for any $i$, we can equate the coefficient of $x^{111-4i} y^{4i}$ on the right hand side (when expanded and factored properly) to $A_{4i}$. This yields a linear equation system in the $A_{4i}$'s. This equation system can not explicitly be solved for the $A_{4i}$'s, but using the fact that $A_0, \ldots, A_{12}$ is known it can be shown that each $A_{4i}$ depends on just $A_{12}, A_{15}$ and $A_{16}$. Hence if these three are found, the entire weight-enumerator of $C$ is determined.

This observation was made in 1973 by MacWilliams, Sloane and Thompson [5]. They used a computer to search for possible code words of order 15, but none was found, so $A_{15} = 0$. The method used was to look at how lines of the plane would intersect the code word, and what structure this would give the incidence matrix. They then tried to complete this incidence matrix into a complete incidence matrix of a projective plane. If a code word of order 15 existed in the projective plane, this would be possible (this will all be explained in more detail in the next section). However, no starting incidence matrix could be completed into a plane, and hence $A_{15} = 0$.

As early as 1957, Hughes [2] [3] pointed out that the only possible prime divisors of the order of the collineation group of a projective plane of order 10 were 3, 5 and 11. In 1976, Whitesides showed that 11 does not divide the order of the group [6], and in 1979 he showed that the full collineation group would have order 1, 3 or 5 [7]. In the following year, Anstee, Hall and Thompson [8] showed that the collineation group could not have order 5, and in 1981 Janko and van Trung [9] showed that it could not have order 3. Thus the collineation group of the plane would have order

| Weight | | Number of code words |
|---|---|---|
| 0 | 111 | 1 |
| 11 | 100 | 111 |
| 19 | 92 | 24,675 |
| 20 | 91 | 386,010 |
| 23 | 88 | 18,864,495 |
| 24 | 87 | 78,227,415 |
| 27 | 84 | 2,698,398,790 |
| 28 | 83 | 8,148,873,195 |
| 31 | 80 | 166,383,964,620 |
| 32 | 79 | 415,533,405,150 |
| 35 | 76 | 5,023,148,053,500 |
| 36 | 75 | 10,604,483,511,375 |
| 39 | 72 | 78,347,862,432,300 |
| 40 | 71 | 141,031,595,676,060 |
| 43 | 68 | 653,162,390,747,370 |
| 44 | 67 | 1,009,413,831,402,540 |
| 47 | 64 | 2,982,186,455,878,665 |
| 48 | 63 | 3,976,279,652,851,020 |
| 51 | 60 | 7,582,305,834,092,682 |
| 52 | 59 | 8,748,789,607,170,360 |
| 55 | 56 | 10,841,059,295,003,634 |

Table 4.1: Number of code words of each weight.

1, so it would be trivial. All projective planes we have seen in this essay has been symmetric in all sorts of ways, but if a projective plane of order 10 existed, it would have virtually no symmetry at all. This would indeed be a very strange projective plane.

The idea now, was to calculate $A_{12}$ and $A_{16}$, using similar techniques as those used for calculating $A_{15}$. If a code word of weight 12 or 16 was found to complete to a plane, a plane has been found and existence shown. If on the other hand no such code words was found (and $A_{12} = A_{16} = 0$), the weight-enumerator of $C$ could be calculated. Then a code word that should exist (i.e. $A_i \neq 0$) should be possible to complete into a plane. If this was possible, a plane would be found, but if this was not possible, this would contradict the fact that such a code word should exist. Hence our assumption that a projective plane of order 10 exist must be false, and we have proven that no projective plane of order 10 exist.

In 1983, Lam, Thiel, Swiercz and McKay finished a computer search for code words of weight 12 [10]. None was found, so $A_{12} = 0$. The program used a total of 183 days of CPU time. Three years later, Lam, Thiel and Swiercz finished a search for code words of weight 16 [12]. Again, none was found, so $A_{16} = 0$. Now the entire weight-enumerator was known, so the number of code words was known for each weight. Table 4.1 lists the number of code words of each weight. All weight where the number of code words are zero are excluded from the list. As $A_i = A_{111-i}$, they are listed together.

## 4.3 The search for a projective plane of order 10

From table 4.1 we see that if a projective plane of order 10 exists, it should contain 24,675 code words of weight 19. Let us now look at what properties such a code word would have. We note first, that since the weight is odd, each line intersects the code word in an odd number of points.

From now on, $x$ will be a code word of weight 19. Obviously, no line can intersect $x$ in more than 11 points. Now, suppose that a line $l$ intersects $x$ in 11 points. But then $w(x+l) = 19+11-2\cdot 11 = 8$ and this contradicts the fact that there are no code words of weight 8. Hence, no line can intersect $x$ in 11 points.

Suppose a line $l$ intersects $x$ in 9 points. Then $w(x + l) = 19 + 11 - 2 \cdot 9 = 12$. Since no code word of weight 12 exist, no line can intersect $x$ in 9 points.

Suppose a line $l$ intersects $x$ in 7 points. Then $w(x + l) = 19 + 11 - 2 \cdot 7 = 16$. Since no code

| | | | |
|---|---|---|---|
| 1 1 1 1 1 | 0 0 0 0 0 | 0 0 0 0 0 | 0 0 0 0 |
| 1 0 0 0 0 | 1 1 1 1 0 | 0 0 0 0 0 | 0 0 0 0 |
| 1 0 0 0 0 | 0 0 0 0 1 | 1 1 1 0 0 | 0 0 0 0 |
| 1 0 0 0 0 | 0 0 0 0 0 | 0 0 0 1 1 | 1 1 0 0 |
| 0 1 0 0 0 | 1 0 0 0 1 | 0 0 0 1 0 | 0 0 1 0 |
| 0 0 1 0 0 | 0 1 0 0 0 | 1 0 0 0 0 | 0 0 1 1 |

Table 4.2: One of the $19 \times 6$-incidence matrices found by Lam, Crossfield and Thiel. If a code word of weight 19 corresponding to this matrix would exist in a projective plane of order 10, the top left corner of the incidence matrix for the projective plane could be assumed to look like this.

word of weight 16 exist, no line can intersect $x$ in 7 points.

Assuming that a line $l$ intersects $x$ in 5, 3 or 1 points does not yield a contradiction using this argument, as there should exists a lot of code words of weight 20, 24 and 28. Hence, any of these may be possible. Thus any line intersects $x$ in 1, 3 or 5 points. Let $b_1, b_3$ and $b_5$ be the number of lines that intersect $x$ in 1, 3 and 5 points respectively. We will call a line that intersects $x$ in 1 point a *single* line, a line that intersects $x$ in 3 points a *triple* line and a line that intersects $x$ in 5 points a *heavy* line. Since every line of $\Pi$ intersects $x$ in either 1, 3 or 5 points, and there are 111 lines in $\Pi$, we see that

$$b_1 + b_3 + b_5 = 111. \tag{4.4}$$

As there are 11 lines on each point of $x$, and there are 19 points on $x$, $11 \cdot 19 = 209$ counts each single line one time, each triple line three times and each heavy line five times. Thus we have

$$b_1 + 3b_3 + 5b_5 = 209. \tag{4.5}$$

Finally, each unordered pair of points of $x$ define a line through $x$. There are $\binom{19}{2} = 171$ unordered pairs of points of $x$. No single line is accounted for in this way. As any pair of the three points on $x$ of a triple line defines the line, and there are three such unordered pairs for each triple line, each triple line is accounted for three times. As any pair of the five points on $x$ of a heavy line defines the line, and there are ten such unordered pairs for each heavy line, every heavy line is accounted for ten times. Thus

$$3b_3 + 10b_5 = 171. \tag{4.6}$$

By solving these three equations, we get

$$b_1 = 6 \qquad b_3 = 37 \qquad b_5 = 68. \tag{4.7}$$

Thus there are 6 heavy lines, 37 triple lines and 68 single lines for any code word $x$ of weight 19 in $\Pi$. By permuting the rows and columns of the incidence matrix for $\Pi$, we can assume that the 19 points of the code word are the 19 leftmost columns, the 6 heavy lines are the 6 topmost rows, the 37 triple lines are the next 37 rows, and the 68 single lines are 68 bottom rows (see table 4.3).

The incidence of the 19 points of $x$ with the 6 heavy lines induces an $19 \times 6$-incidence matrix (the sub matrix $B_1$ of table 4.3), where the rows represents the lines and the columns represents the points, as usual. We will call such a $19 \times 6$-matrix a *starting point configuration*. Lam, Crossfield and Thiel found [11], using a computer search, that there are 66 non-isomorphic starting point configurations, where two starting point configurations are isomorphic if one can be produced from the other using only row/column permutations. If a code word of weight 19 exists in $\Pi$, it would be possible to extend at least one of the starting point configurations to a $111 \times 111$-incidence matrix representing the projective plane $\Pi$. Two of these non-isomorphic $19 \times 6$-matrices are given in tables 4.2 and 4.5. These can be seen not to be isomorphic to each other by noting that the one in table 4.2 has one column with four 1's and the one in table 4.5 has no column with four 1's in it. Permuting the rows of the matrix preserves the number of 1's in each column, and permuting columns only moves the columns so there is no way of turning one of the starting point configurations in to the other by permuting the rows and columns. Hence the two starting point configurations are non-isomorphic.

Now, let $p$ be any point of $\Pi$. Let $c_1$, $c_3$ and $c_5$ be the number of single, triple and heavy lines on $p$, respectively. If $p$ is a point of $x$, then the following relations hold.

$$c_1 + c_3 + c_5 = 11, \tag{4.8}$$

| | 19 | 92 |
|---|---|---|
| 6 | $B_1$ | $B_2$ |
| 37 | $B_3$ | $B_4$ |
| 68 | $B_5$ | $B_6$ |

Table 4.3: We can assume that the 19 points of the code word of weight 19 are the leftmost columns in the incidence matrix, that the 6 heavy lines are the topmost rows, the 37 triple lines are the next 37 rows and the 68 single lines are the 68 rows at the bottom.

| $c_1$ | $c_3$ | $c_5$ |
|---|---|---|
| 2 | 9 | 0 |
| 3 | 7 | 1 |
| 4 | 5 | 2 |
| 5 | 3 | 3 |
| 6 | 1 | 4 |

(a)

| $c_1$ | $c_3$ | $c_5$ |
|---|---|---|
| 7 | 4 | 0 |
| 8 | 2 | 1 |
| 9 | 0 | 2 |

(b)

Table 4.4: The solutions to equations (4.8) and (4.9) (a), and equations (4.10) and (4.11) (b).

$$2c_3 + 4c_5 = 18. \tag{4.9}$$

Equation (4.8) holds, as $p$ is on 11 lines. Equation (4.9) counts the number of lines connecting $p$ to the other points of $x$. Table 4.4 (a) lists the integer solutions to these two equations.

Now, if $p$ is *not* a point of $x$, we get the following relations.

$$c_1 + c_3 + c_5 = 11, \tag{4.10}$$

$$c_1 + 3c_3 + 5c_5 = 19, \tag{4.11}$$

where (4.10) counts the number of lines on $p$, and (4.11) counts the number of lines connecting $p$ to points of $x$. Table 4.4 (b) lists the integer solutions to these two equations.

21 of the 66 starting point configurations can be seen not to complete to a projective plane by mere inspection. For example, looking at the starting point configuration of table 4.2, we see that point 1 is on four heavy lines. By table 4.4 (a) we see that point 1 should be on exactly one triple line. As the points $2, 3, \ldots, 17$ are on the heavy lines on point 1, they can not also be on the triple line on point 1. Furthermore, the points 18 and 19 are on a line that is not on 1 (the triple line containing 3, 18 and 19). Thus none of the points $2, 3, \ldots, 19$ can be on a triple line containing point 1, which contradicts the fact that there should be exactly one such line. Hence this starting point configuration can not be completed into a complete plane. Ten other starting point configurations can be shown not to complete into projective planes by similar arguing.

Another method to show that a starting point configuration can not be completed into a projective plane is to see if the starting point configuration implies that a code word of weight 16 is in the plane. Since there are no code words of weight 16 in the code of a projective plane of order 10, we have a contradiction, and the starting point can not be completed to a plane. An example of such a starting point configuration is the one shown in table 4.5.

Here, the rows 4, 5 and 6 are mutually non-intersecting within $x$, that is, no two of the three heavy lines have a point in common in $x$. Hence they must meet in a point outside the code word. Let $l_4, l_5$ and $l_6$ denote the lines corresponding to rows 4, 5 and 6 respectively. All three lines can not meet in a common point, since $c_5$ is less than 2 for any point not on the code word. Let $y = x + l_4 + l_5 + l_6$. The points of $y$ that are in $x$ are the points that are also on an even number of the lines $l_4, l_5$ and $l_6$. These are the four points 1, 5, 9 and 13. Furthermore, the points that are in $y$ that are not in $x$ are the points that are on an odd number of the three lines. These lines each have 6 points that are not in $x$, and two of these points are the points of intersection with the

| | | | |
|---|---|---|---|
| 1 1 1 1 1 | 0 0 0 0 0 | 0 0 0 0 0 | 0 0 0 0 |
| 1 0 0 0 0 | 1 1 1 1 0 | 0 0 0 0 0 | 0 0 0 0 |
| 1 0 0 0 0 | 0 0 0 0 1 | 1 1 1 0 0 | 0 0 0 0 |
| 0 1 0 0 0 | 1 0 0 0 1 | 0 0 0 1 1 | 0 0 0 0 |
| 0 0 1 0 0 | 0 1 0 0 0 | 1 0 0 0 0 | 1 1 0 0 |
| 0 0 0 1 0 | 0 0 1 0 0 | 0 1 0 0 0 | 0 0 1 1 |

Table 4.5: A starting point configuration that can not be completed into a projective plane of order 10 as it implies the existence of a code word of weight 16.

other to lines. Hence there are 4 points on each line that is neither in $x$ nor on any of the other two lines. Summing up, we see that the code word $y$ has 16 points, which contradicts the fact that there are no code words of weight 16. So this starting point configuration can not be completed into a complete plane.

Four other starting point configurations can be eliminated by the same argument. Also, four other starting point configurations can be eliminated using ad hoc arguments. This eliminates 21 of the 66 starting point configurations. This leaves us with 45 remaining starting point configurations that need to be eliminated. This was done using computers as follows.

For each starting point configuration, all possible incidences of the 19 points with the triple lines are found. That is, by looking at table 4.3, to determine all possibilities for $B_3$ once $B_1$ is chosen. $B_2$ is then determined by successively looking at the incidence of the points of the heavy lines that is not in the code word. One would then proceed to determine $B_4$ and so forth. This, however, was never necessary as no starting point configuration could be extended to $B_2$. Checking all cases took about 2 years of CPU time. As no starting point configuration could be completed into a projective plane, we must conclude that no projective plane of order 10 exists.

## 4.4 Possible errors in the search

Unfortunately, there is a small chance that an error occured during the search, resulting in the possibility that a a projective plane of order 10 was in fact missed by the search. However, precautions were made to minimize the probability of errors. There are two types of errors that can occur, hardware and software. Of these two types, the software-errors are by far the most common ones. To avoid these, all computer programs were made in two versions, one that would do the actual search, and one that would do part of the search, for testing that both programs performed as expected.

The hardware errors are a bit harder to avoid. One of the more common hardware errors is the random substitution of two bits, which may result in the program missing several cases that it is supposed to check. One of the computers used in the search is reported do this error on average once every thousand hours of computing. One such error was in fact detected after a hardware failure. When rerunning the last 1,000 cases before the hardware failure and comparing these results to what was reported before the failure differences were found, indicating that a random bit substitution had occurred. However, if a projective plane of order 10 exists, 24,675 extensions of starting point configurations to a $B_3$ can be extended into a complete projective plane. Since isomorphism checking was done, if all these 24,675 extensions are isomorphic they are only checked once. If a hardware error occurred when this extension were checked, the projective plane is missed. However, there were about half a million extensions to $B_3$'s, so the probability that a hardware error occurred when checking this particular extension is about one in half a million. Also, as the plane would have a trivial collineation group, it is likely that there are many non-isomorphic extension, in which case the probability that a plane was missed is virtually zero.

# Appendix A

# Proof of the Four-Squares Identity

**Lemma 81 (The Four-Squares Identity).** *If $b_1, b_2, b_3, b_4, x_1, x_2, x_3, x_4$ are integers, then*

$$(b_1^2 + b_2^2 + b_3^2 + b_4^2)(x_1^2 + x_2^2 + x_3^2 + x_4^4) = y_1^2 + y_2^2 + y_3^2 + y_4^2 \tag{A.1}$$

*where the y's are integers and*

$$\begin{aligned} y_1 &= b_1x_1 + b_2x_2 + b_3x_3 + b_4x_4 \\ y_2 &= -b_2x_1 + b_1x_2 - b_4x_3 + b_3x_4 \\ y_3 &= -b_3x_1 + b_4x_2 + b_1x_3 - b_2x_4 \\ y_4 &= -b_4x_1 - b_3x_2 + b_2x_3 + b_1x_4. \end{aligned} \tag{A.2}$$

*There is also a similar* two-squares identity*: If $b_1, b_2, x_1, x_2$ are integers, then*

$$(b_1^2 + b_2^2)(x_1^2 + x_2^2) = y_1^2 + y_2^2 \tag{A.3}$$

*where the y's are integers and*

$$\begin{aligned} y_1 &= b_1x_1 - b_2x_2 \\ y_2 &= b_1x_2 + b_2x_1. \end{aligned} \tag{A.4}$$

*Proof.* Straightforward calculation. The left hand side of equation (A.1), when expanded, is

$$\begin{aligned} (b_1^2 + b_2^2 + b_3^2 + b_4^2)(x_1^2 + x_2^2 + x_3^2 + x_4^2) = \; & b_1^2x_1^2 + b_1^2x_2^2 + b_1^2x_3^2 + b_1^2x_4^2 + \\ & b_2^2x_1^2 + b_2^2x_2^2 + b_2^2x_3^2 + b_2^2x_4^2 + \\ & b_3^2x_1^2 + b_3^2x_2^2 + b_3^2x_3^2 + b_3^2x_4^2 + \\ & b_4^2x_1^2 + b_4^2x_2^2 + b_4^2x_3^2 + b_4^2x_4^2. \end{aligned}$$

For the right hand side, we will expand the $y$:s, one at a time. By the generalized quadratic rule, we have

$$\begin{aligned} y_1^2 = (b_1x_1 + b_2x_2 + b_3x_3 + b_4x_4)^2 = \; & b_1^2x_1^2 + b_2^2x_2^2 + b_3^2x_3^2 + b_4^2x_4^2 + \\ & 2b_1b_2x_1x_2 + 2b_1b_3x_1x_3 + 2b_1b_4x_1x_4 + \\ & 2b_2b_3x_2x_3 + 2b_2b_4x_2x_4 + 2b_3b_4x_3x_4, \end{aligned}$$

$$\begin{aligned} y_2^2 = (-b_2x_1 + b_1x_2 - b_4x_3 + b_3x_4)^2 = \; & b_2^2x_1^2 + b_1^2x_2^2 + b_4^2x_3^2 + b_3^2x_4^2 - \\ & 2b_1b_2x_1x_2 + 2b_2b_4x_1x_3 - 2b_2b_3x_1x_4 - \\ & 2b_1b_4x_2x_3 + 2b_1b_3x_2x_4 - 2b_3b_4x_3x_4, \end{aligned}$$

$$\begin{aligned} y_3^2 = (-b_3x_1 + b_4x_2 + b_1x_3 - b_2x_4)^2 = \; & b_3^2x_1^2 + b_4^2x_2^2 + b_1^2x_3^2 + b_2^2x_4^2 - \\ & 2b_3b_4x_1x_2 - 2b_1b_3x_1x_3 + 2b_2b_3x_1x_4 + \\ & 2b_1b_4x_2x_3 - 2b_2b_4x_2x_4 - 2b_1b_2x_3x_4, \end{aligned}$$

$$\begin{aligned} y_4^2 = (-b_4x_1 - b_3x_2 + b_2x_3 + b_1x_4)^2 = \; & b_4^2x_1^2 + b_3^2x_2^2 + b_2^2x_3^2 + b_1^2x_4^2 + \\ & 2b_3b_4x_1x_2 - 2b_2b_4x_1x_3 - 2b_1b_4x_1x_4 - \\ & 2b_2b_3x_2x_3 - 2b_1b_3x_2x_4 + 2b_1b_2x_3x_4. \end{aligned}$$

This looks rather messy, but we see that $y_1^2+y_2^2+y_3^2+y_4^2$ has summands of the form $b_i^2x_j^2$ exactly once for each $i,j,=1,2,3,4$. Also, each summand of the form $2b_ib_jx_kx_l$ occurs exactly once for each $i,j,k,l=1,2,3,4$ as do the summands of the form $-2b_ib_jb_kb_l$, so these cancel each other. What we are left with is exactly the left hand side of equation (A.1).

To prove the two-squares identity, we do a similar calculation. The left hand side of equation (A.3) is

$$(b_1^2+b_2^2)(x_1^2+x_2^2)=b_1^2x_1^2+b_1^2x_2^2+b_2^2x_1^2+b_2x_2^2.$$

The right hand side of equation (A.3) is

$$\begin{aligned}(b_1x_1^2-b_2x_2)^2+(b_1x_2+b_2x_1)^2&=b_1^2x_1^2+b_2^2x_2^2-2b_1b_2x_1x_2+b_1^2x_2^2+b_2^2x_1^2+2b_1b_2x_1x_2\\&=b_1^2x_1^2+b_2^2x_2^2+b_1^2x_2^2+b_2^2x_1^2\end{aligned}$$

which equals the left hand side, and we are done. □

By letting $\mathbf{x}=(x_1,x_2,x_3,x_4),\mathbf{y}=(y_1,y_2,y_3,y_4)$, we can represent equation (A.2) by $\mathbf{y}=\mathbf{x}B$, where

$$B=\begin{bmatrix}b_1&b_2&b_3&b_4\\-b_2&b_1&-b_4&b_3\\-b_3&b_4&b_1&-b_2\\-b_4&-b_3&b_2&b_1\end{bmatrix}. \tag{A.5}$$

**Lemma 82.** *Let $B$ be the $4\times4$ matrix determined by* (A.5)*. Then $det(B)=(b_1^2+b_2^2+b_3^2+b_4^2)^2$, and hence $B$ is invertible if and only if at least one of the $b$'s is different from zero.*

*Proof.*

$$\begin{aligned}\det(B)&=\begin{vmatrix}b_1&b_2&b_3&b_4\\-b_2&b_1&-b_4&b_3\\-b_3&b_4&b_1&-b_2\\-b_4&-b_3&b_2&b_1\end{vmatrix}\\&=b_1\begin{vmatrix}b_1&-b_4&b_3\\b_4&b_1&-b_2\\-b_3&b_2&b_1\end{vmatrix}+b_2\begin{vmatrix}b_2&b_3&b_4\\b_4&b_1&-b_2\\-b_3&b_2&b_1\end{vmatrix}-\\&\quad b_3\begin{vmatrix}b_2&b_3&b_4\\b_1&-b_4&b_3\\-b_3&b_2&b_1\end{vmatrix}+b_4\begin{vmatrix}b_2&b_3&b_4\\b_1&-b_4&b_3\\b_4&b_1&-b_2.\end{vmatrix}\\&=b_1D_1+b_2D_2-b_3D_3+b_4D_4.\end{aligned}$$

Here we have labeled the four $3\times3$ determinants by $D_1,D_2,D_3$ and $D_4$. Their values are

$$\begin{aligned}D_1&=b_1\begin{vmatrix}b_1&-b_2\\b_2&b_1\end{vmatrix}-b_4\begin{vmatrix}-b_4&b_3\\b_2&b_1\end{vmatrix}-b_3\begin{vmatrix}-b_4&b_3\\b_1&-b_2\end{vmatrix}\\&=b_1(b_1^2+b_2^2)-b_4(-b_1b_4-b_2b_3)-b_3(b_2b_4-b_1b_3),\\D_2&=b_2\begin{vmatrix}b_1&-b_2\\b_2&b_1\end{vmatrix}-b_4\begin{vmatrix}b_3&b_4\\b_2&b_1\end{vmatrix}-b_3\begin{vmatrix}b_3&b_4\\b_1&-b_2\end{vmatrix}\\&=b_2(b_1^2+b_2^2)-b_4(b_1b_3-b_2b_4)-b_3(-b_2b_3-b_1b_4),\\D_3&=b_2\begin{vmatrix}-b_4&b_3\\b_2&b_1\end{vmatrix}-b_1\begin{vmatrix}b_3&b_4\\b_2&b_1\end{vmatrix}-b_3\begin{vmatrix}b_3&b_4\\-b_4&b_3\end{vmatrix}\\&=b_2(-b_1b_4-b_2b_3)-b_1(b_1b_3-b_2b_4)-b_3(b_3^2+b_4^2),\\D_4&=b_2\begin{vmatrix}-b_4&b_3\\b_1&-b_2\end{vmatrix}-b_1\begin{vmatrix}b_3&b_4\\b_1&-b_2\end{vmatrix}+b_4\begin{vmatrix}b_3&b_4\\-b_4&b_3\end{vmatrix}\\&=b_2(b_2b_4-b_1b_3)-b_1(-b_2b_3-b_1b_4)+b_4(b_3^2+b_4^2).\end{aligned}$$

So, we get

$$
\begin{aligned}
\det(B) &= b_1D_1 + b_2D_2 - b_3D_3 + b_4D_4 \\
&= b_1^2(b_1^2+b_2^2) + b_1b_4(b_1b_4+b_2b_3) - b_1b_3(b_2b_4-b_1b_3) + \\
&\quad b_2^2(b_1^2+b_2^2) + b_2b_4(b_2b_4-b_3b_1) + b_2b_3(b_2b_3+b_1b_4) + \\
&\quad b_2b_3(b_1b_4+b_2b_3) - b_1b_3(b_2b_4-b_1b_3) + b_3^2(b_3^2+b_4^2) + \\
&\quad b_2b_4(b_2b_4-b_1b_3) + b_1b_4(b_2b_3+b_1b_4) + b_4^2(b_3^2+b_4^2) \\
&= (b_1^2+b_2^2)(b_1^2+b_2^2) + (b_3^2+b_4^2)(b_3^2+b_4^2) \\
&\quad +2(b_1b_4+b_2b_3)(b_1b_4+b_2b_3) + 2(b_2b_4-b_1b_3)(b_1b_4-b_2b_3) \\
&= (b_1^2+b_2^2)^2 + (b_3^2+b_4^2)^2 + 2(b_1b_4+b_2b_3)^2 + 2(b_2b_4-b_1b_3)^2 \\
&= b_1^4 + 2b_1^2b_2^2 + b_2^4 + b_3^4 + 2b_3^2b_4^2 + b_4^4 + 2b_1^2b_4^2 \\
&\quad +4b_1b_2b_3b_4 + 2b_2^2b_3^2 + 2b_2^2b_4^2 - 4b_1b_2b_3b_4 + 2b_1^2b_3^2 \\
&= \textstyle\sum_{i,j=1}^{4} b_i^2b_j^2 = (b_1^2+b_2^2+b_3^2+b_4^2)^2,
\end{aligned}
$$

and we are done. □

# Appendix B

# Proof of the Theorem of Lagrange

In this appendix we will prove Lagrange's Theorem, that states that any positive integer can be written as the sum of four squares. The proof will be very similar to the proof of Lemma 57. For the proof, we will need the following lemma

**Lemma 83.** *For every odd integer $m$, there exists integers $x, y$ and $n$ such that $x^2 + y^2 + 1 = mn$.*

*Proof.* Let $X = \{x^2 + 1 \pmod m \mid x = 0, \ldots, (m-1)/2\}$. The elements of $X$ are easily seen to be $(m-1)/2$ distinct elements. Let $Y = \{-(y^2) \pmod m \mid y = 0, \ldots (m-1)/2\}$. The elements of $Y$ are also all distinct. Hence, $|X| = |Y| = (m-1)/2$, so $|X| + |Y| = m + 1$. As there are $m$ distinct values (mod $m$), $X$ and $Y$ must have at least one element in common. Hence there must exist $x$ and $y$, $0 \leq x, y \leq (m-1)/2$ such that $x^2 + 1 \equiv -(y^2) \pmod m$, or $x^2 + y^2 + 1 \equiv 0 \pmod m$. Hence, there exists an integer $n$ such that $x^2 + y^2 + 1 = mn$, and we are done.

□

**Theorem 84 (Lagrange).** *Every positive integer can be written as the sum of four squares.*

*Proof.* By the four-squares identity, i suffices to prove that every positive prime $p$ can be written as the sum of four squares. Since $2 = 1^2 + 1^2 + 0^2 + 0^2$, and 2 is the only even prime, we can assume that $p$ is odd.

Let $a, b, c, d$ be integers and $m$ a positive integer such that $a^2 + b^2 + c^2 + d^2 = mp$. Such integers exist by Lemma 83. Take such an expression that minimizes $m$. If we can show that $m = 1$, we have proven the lemma. So, for a contradiction, assume that $m > 1$. Now choose integers $A, B, C, D$ such that $-m/2 < A, B, C, D \leq m/2$, and $A \equiv a, B \equiv b, C \equiv c, D \equiv d \pmod m$. By the same argument as in the proof of Lemma 57 such integers exists.

We have that $A^2 + B^2 + C^2 + D^2 \equiv a^2 + b^2 + c^2 + d^2 \equiv 0 \pmod m$, so $A^2 + B^2 + C^2 + D^2 = rm$ for some non-negative integer $r$. We see that

$$r = \frac{rm}{m} = \frac{A^2 + B^2 + C^2 + D^2}{m} \leq \frac{m^2/4 + m^2/4 + m^2/4 + m^2/4}{m} = m,$$

so $r \leq m$.

Suppose that $r = 0$. This implies that $A = B = C = D = 0$, so $a \equiv b \equiv c \equiv d \equiv 0 \pmod m$. But this means that $a, b, c$ and $d$ are multiples of $m$, so $a^2 + b^2 + c^2 + d^2$ is divisible by $m^2$, and $p$ is divisible by $m$. This contradicts the fact that $m > 1$ and $p$ is prime, so $r$ can not be zero. Thus $r > 0$.

Now, suppose that $r = m$. Then $A = B = C = D = m/2$. Since $A \equiv a \pmod m$, this means that $a = m/2 + um$ for some integer $u$. Then $a^2 = m^2/4 + um^2 + u^2m^2$, so $a^2 \equiv m^2/4 \pmod{m^2}$. The same holds, of course, for $b, c$ and $d$. Then,

$$a^2 + b^2 + c^2 + d^2 \equiv \frac{m^2}{4} + \frac{m^2}{4} + \frac{m^2}{4} + \frac{m^2}{4} \equiv m^2 \equiv 0 \pmod{m^2},$$

so $a^2 + b^2 + c^2 + d^2$ is again divisible $m^2$, which implies that $p$ is divisible by $m$, which contradicts the fact that $p$ is prime. Hence $r < m$.

Now, by the four squares identity,

$$m^2rp = (mp)(mr) = (a^2 + b^2 + c^2 + d^2)(A^2 + D^2 + C^2 + D^2) = e^2 + f^2 + g^2 + h^2,$$

where

$$\begin{aligned} e &= aA + bB + cC + dD \\ f &= -bA + aB - dC + cD \\ g &= -cA + dB + aC - bD \\ h &= -dA - cB + bC + aD. \end{aligned}$$

Furthermore,

$$\begin{aligned} e &\equiv a^2 + b^2 + c^2 + d^2 \equiv 0 \pmod{m} \\ f &\equiv -ba + ab - dc + cd \equiv 0 \pmod{m} \\ g &\equiv -ca + db + ac - bd \equiv 0 \pmod{m} \\ h &\equiv -da - cb + bc + ad \equiv 0 \pmod{m}, \end{aligned}$$

so $e, f, g$ and $h$ all have a factor $m$, and thus $e^2, f^2, g^2$ and $h^2$ are all divisible by $m^2$. But then

$$rp = (e/m)^2 + (f/m)^2 + (g/m)^2 + (h/m)^2,$$

so $rp$ is a sum of four integer squares, and $r < m$, contradicting the fact that $m$ is the smallest such number. Our assumption that $m > 1$ does not hold, so we must have that $m = 1$. □

# Bibliography


[1] Hughes D. R. and Piper F. C. *Projective Planes, second edition.* Springer-Verlag, New York.

[2] Hughes D. R. *Collineations and generalized incidence matrices.* Trans Amer. Math. Soc. No. 86, 1957, pp. 284-296.

[3] Hughes D. R. *Generalized incidence matrices over group algebras.* Illinois J. Math, No 1, 1957, pp. 545-551.

[4] T.G. Room and P.B. Kirkpatrick *Miniquaternion Geometry.* Cambridge Univ. Press, 1971.

[5] MacWilliams F. J., Sloane N. J. A. and Thompson, J. G. *On the existence of a projective plane of order 10.* Journal of Combinatorial Theory, Series A, No. 14, 1973, pp. 66-78.

[6] Whitesides S. H. *Projective planes of order 10 have no collineations of order 11.* Proceedings of the Seventh Southeastern Conference on Combinatorics, Graph Theory, and Computing. Utilias Mathematica, 1976, pp. 515-526.

[7] Whitesides S. H. *Collineations of projective planes of order 10, Parts I & II.* Journal of Combinatorial Theory, Series A, No 26, 1979, pp. 249-277.

[8] Anstee R. P., Hall, M Jr. and Thompson J. G. *Planes of order 10 do not have a collineation of order 5.* Journal of Combinatorial Theory, Series A, No. 29, 1980, pp. 39-58.

[9] Janko Z. and van Trung T. *Projective planes of order 10 do not have a collineation of order 3.* J. Reine Angew. Math, No 325, 1981, pp. 189-209.

[10] Lam C. W. H., Thiel L., Swiercz S. and McKay J. *The nonexistence of ovals in a projective plane of order 10.* Discrete Mathematics No. 45, 1983, pp. 319-321.

[11] Lam C. W. H., Crossfield S. and Thiel L. *Estimates of a computer search for a projective plane of order 10.* Congressus Numerantium, No 48, 1985, pp. 253-263.

[12] Lam C. W. H., Thiel L. and Swiercz S. *The nonexistence of code words of weight 16 in a projective plane of order 10.* Journal of Combinatorial Theory, Series A, No. 42, 1986, pp. 207-214.

[13] Lam C. W. H., Thiel L. and Swiercz S. *The non-existence of finite projective planes of order 10.* Can. J. Math, Vol. XLI, No. 6, 1989, pp. 1117-1123.

[14] Batten, L. M. *Combinatorics of finite geometries.* Cambridge University Press, 1997.

[15] Hall, M. Jr. *Combinatorial Theory, second edition.* John Wiley & Sons Inc., 1998.

[16] Lam, C. W. H. *The Search for a Finite Projective Plane of Order 10.* `http://www.cecm.sfu.ca/organics/papers/lam/`