Master's Thesis

On the prime power conjecture for finite projective planes

Lukas Klawuhn

Matriculation number: 175412

Fakultät für Mathematik
Technische Universität Dortmund

Supervisor: Prof. Dr. Franz Kalhoff

Foreword

It is always something very special when progress is made on a century-old conjecture that has not seen progress for almost 30 years. As such I was immediately intrigued when one of my professors pointed me to an article claiming to have made a new discovery regarding the prime power conjecture for finite projective planes.

The prime power conjecture states that the order of a finite projective plane must always be a prime power. It is a famous problem in finite geometry and combinatorics. The theory of projective planes has a long history, and at the beginning of the 20th century projective planes with order p^n for any prime power p^n became known. However, no one could find a projective plane that had an order that is not a prime power. Thus, it was conjectured that no such plane exists, and (at the time of publishing of this thesis) the conjecture still stands today.

The aim of this thesis is to critically analyse an approach to the prime power conjecture proposed by Mingchun Xu. In chapter 1 we define basic terminology from design theory and collect some results needed in this thesis. Then we will deal with projective planes and their history in chapter 2. Chapter 3 then deals with a class of projective planes called translation planes. The known planes not covered in this chapter are called non-translation planes and we describe all known constructions in chapter 4. In chapter 5 we prove the Bruck-Ryser-Chowla theorem and describe the state of the prime power conjecture at the time of publication of this thesis. After that we will take a look at Xu's attempted generalisation of the Bruck-Ryser-Chowla theorem in chapter 6, explain why it does not work and try to make some progress using a closely related approach. Chapter 7 gives a short overview of projective planes of small order and we look at some other conjectures about projective planes. Finally, in chapter 8 we summarise the results and give some final thoughts.

All computations by the author were done in SageMath [49], and all images in this thesis were drawn by the author using Inkscape [18].

I would like to express my gratitude to Professor Kalhoff for his support and helpful discussions during the writing of this thesis.

Notation:

$\mathbb{N}$ is the set $\{1, 2, 3, \ldots\}$
$\mathfrak{P}(M)$ denotes the power set of a set M
$F^{m \times n}$ denotes the set of all $(m \times n)$-matrices with m rows, n columns and entries in F
a_{ij} denotes the entry in row i and column j of a matrix A
$GL(n, F)$ denotes the set of all invertible $(n \times n)$-matrices with entries in F
If q is a prime power, we write $GL(n, q) = GL(n, \mathbb{F}_q)$
I_n denotes the $(n \times n)$-identity matrix
J_n denotes the $(n \times n)$-matrix where every entry is 1
$\mathbb{F}_q$ denotes the finite field with q elements

Contents

1 Design Theory

Our approach to the prime power conjecture is rooted in design theory. In this chapter basic definitions and theorems are given that will be used throughout this thesis.

1.1 Basic results

This section is based on Chapter 1 from the book “Designs and their Codes“ by Assmus and Key [2] with some definitions simplified or altered to better fit our purpose.
Finite projective planes, which this thesis deals with, are a special case of symmetric designs. In this section we give an introduction into the field of design theory, fixing notation along the way.

Definition. Let $\mathcal{P}$ and $\mathcal{B}$ be (finite) disjoint sets and $\mathcal{I} \subseteq \mathcal{P} \times \mathcal{B}$. Then the triple $\mathcal{S} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ is called a *(finite) incidence structure.* The elements of $\mathcal{P}$ are called *points* (denoted with lower case letters) and the elements of $\mathcal{B}$ are called *blocks* or sometimes *lines* in a geometric context (denoted with upper case letters). If $(p, B) \in \mathcal{I}$, then the point p is said to be *incident* with the block B and the pair (p, B) is called *flag.* We denote this as $p\,\mathcal{I}\,B$. We also say B contains p or p is in B.

This definition is very broad and offers little to work with. However, it is the basis of design theory and using it we can state some definitions to come in an easier way. We are interested in incidence structures exhibiting a certain kind of regularity, called *designs.*

Definition. Let $t, v, k, \lambda \in \mathbb{N}$ with $t \leq k$ be natural numbers. A t-(v, k, λ) *design* (or for short t-*design*) is a pair $D = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ such that

- $|\mathcal{P}| = v$
- Any block $B \in \mathcal{B}$ is incident with precisely k points.
- For any t pairwise distinct points $p_1, \ldots, p_t \in \mathcal{P}$ there exist precisely λ blocks $B_1, \ldots, B_\lambda \in \mathcal{B}$ such that the points $p_1, \ldots, p_t$ are all incident with B_i for every $i = 1, \ldots, \lambda$.

We will call the numbers t, v, k and λ the *parameters* of D.

This definition allows different blocks to be incident with the same set of points. It is an important concept in general, but it is not needed in this thesis. Designs without such repeated blocks are called *simple.* Throughout this thesis we will always mean “simple design“ when writing “design“. This also allows us to simplify the definition of a t-(v, k, λ)

design a bit: We can view the blocks as the set of points incident with it, i.e. as a subset of $\mathcal{P}$. Then the relation $\mathcal{I}$ becomes the membership relation $\in$. Thus, for our purposes if $D = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ is a design, we will assume $\mathcal{B} \subseteq \mathfrak{P}(\mathcal{P})$ and $\mathcal{I} = \in$, and write $D = (\mathcal{P}, \mathcal{B})$ for short. We will also adopt this convention for arbitrary incidence structures: when no incidence relation is mentioned, we will assume $\mathcal{B} \subseteq \mathfrak{P}(\mathcal{P})$ and $\mathcal{I} = \in$.

1.1 Example. Let $v, k \in \mathbb{N}$ be positive integers with $k \leq v$. Let $\mathcal{P}$ be a set with v elements and $\mathcal{B}$ be the set of all subsets of $\mathcal{P}$ with exactly k elements. Then $D = (\mathcal{P}, \mathcal{B})$ is a k-$(v, k, 1)$ design.

Designs of this type are not very interesting and some theorems even do not hold for the cases $k = 1$ or $k = v$. Thus, they sometimes need to be exlcuded. This motivates the following definition:

Definition. A t-(v, k, λ) design is called *trivial* if every k-element subset of $\mathcal{P}$ is a block.

Stepping away from trivial designs, we now give a very well-known example for a design: the *Fano plane*. It is not only important in design theory, but it is also an important object in projective geometry and many other mathematical areas.

1.2 Example. The *Fano plane* is a 2-$(7, 3, 1)$ design. In other words it consists of 7 points and sets of 3 points as blocks such that any 2 distinct points are contained in exactly one block. An easy way to construct it is to use $\mathbb{F}_7$ as the set of points and the set $\{1, 2, 4\}$ (i.e. the squares modulo 7) and its translates as blocks. Written down explicitly, we have $\mathcal{P} = \{0, 1, 2, 3, 4, 5, 6\}$ and

$$\mathcal{B} = \{\{1, 2, 4\}, \{2, 3, 5\}, \{3, 4, 6\}, \{4, 5, 0\}, \{5, 6, 1\}, \{6, 0, 2\}, \{0, 1, 3\}\}.$$

It is easily checked that this is indeed a 2-$(7, 3, 1)$ design. This construction comes from a general construction using squares and difference sets, again showing that the Fano plane has connections to many different topics. A nice visualisation is given in figure 1.1.

We now investigate the parameter t of a design. It turns out that a t-design can also be viewed as an s-design for any integer $1 \leq s \leq t$. This allows us for example to use theorems on 2-designs for t-designs with $t > 2$. The theorem also gives rise to some divisibility constraints on the parameters of a design. However, they do not help us with the types of designs that we want to deal with, so we do not explicitly state them here.

1.3 Theorem. *Let D be a t-(v, k, λ) design and S be a set of s points with $0 \leq s \leq t$. Then the number λ_s of blocks containing S is independent of the choice of the s points and is given by the formula*

$$\lambda_s = \lambda \frac{(v - s)(v - s - 1) \cdots (v - t + 1)}{(k - s)(k - s - 1) \cdots (k - t + 1)}.$$

It follows that D is also an s-(v, k, λ_s) design for every integer s with $1 \leq s \leq t$.

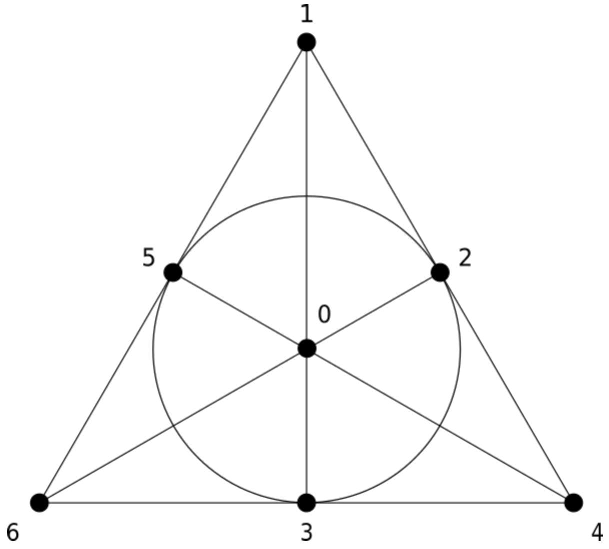


Figure 1.1: The Fano plane

Proof. We consider the set

$$X := \{(T, B) \mid S \subseteq T \subseteq B,\ |T| = t,\ B \in \mathcal{B}\}$$

and compute $|X|$ in two ways.
First, we count how many sets T contain S and have exactly t elements. We can view this as augmenting S to T, i.e. we have to choose $t - s$ points from the $v - s$ points not contained in S. Now given a set $T \subseteq \mathcal{P}$ with $|T| = t$ and $S \subseteq T$, we need to count the blocks containing T. As D is a t-(v, k, λ) design, there are λ such blocks. Thus, we get

$$|X| = \lambda\binom{v-s}{t-s}.$$

Now we compute $|X|$ another way. Let the number of blocks containing S be m. Given a block $B \in \mathcal{B}$ with $S \subseteq B$ we have to count the number of sets T with $S \subseteq T \subseteq B$ and $|T| = t$. This can be viewed as choosing $t - s$ points of the $k - s$ points of B not contained in S. Thus, we get

$$|X| = m\binom{k-s}{t-s}.$$

Comparing the two results we get

$$\lambda\binom{v-s}{t-s} = m\binom{k-s}{t-s}.$$

We see that the number m of blocks containing S does not depend on the choice of points but only on the size of S. Thus, the number λ_s is well-defined and rearranging the above equation yields the desired formula. □

Theorem 1.3 gives a formula to calculate the number of blocks of a design ($s = 0$) and the number of blocks containing a given point ($s = 1$). Since those formulas are very important and helpful, we record them in a corollary:

1.4 Corollary. *Let D be a t-(v, k, λ) design. Then we have:*

(a) D has exactly

$$b := \lambda_0 = \lambda \frac{v(v-1)\cdots(v-t+1)}{k(k-1)\cdots(k-t+1)}$$

blocks.

(b) Every point of D is contained in exactly

$$r := \lambda_1 = \lambda \frac{(v-1)(v-2)\cdots(v-t+1)}{(k-1)(k-2)\cdots(k-t+1)}$$

blocks. The number r is called replication number *of D.*

We define another important parameter based on theorem 1.3:

Definition. Let D be a t-design with $t \geq 2$. We call the number $n := r - \lambda_2$ the *order* of D.

This definition seems arbitrary at first, but it turns out that the order is of crucial importance when building linear codes from designs in coding theory. It is also a vital piece of the prime power conjecture.
Some simple relations between the parameters are collected in the following lemma:

1.5 Lemma. *Let D be a t-(v, k, λ) design. Then we have:*

(1) $vr = bk$

(2) $r(k-1) = \lambda_2(v-1)$

(3) $n = 0 \iff k = v$

Proof. (1) Double-count the set of flags $S := \{(p, B) \in \mathcal{P} \times \mathcal{B} \,|\, p \in B\}$. There are v points and every points lies on r blocks, so we have $|S| = vr$. On the other hand D has b blocks and every block contains k points. Thus, we have $|S| = bk$, giving the desired formula.
(2) Compare the formulas for $s = 1$ and $s = 2$ from theorem 1.4. We have

$$r = \lambda_1 = \lambda \frac{(v-1)(v-2)\cdots(v-t+1)}{(k-1)(k-2)\cdots(k-t+1)}$$

and

$$\lambda_2 = \lambda \frac{(v-2)(v-3)\cdots(v-t+1)}{(k-2)(k-3)\cdots(k-t+1)}.$$

Those two expressions only differ by a factor of $(v-1)/(k-1)$. Rearranging gives the desired result.
(3) The order $n = r - \lambda_2$ is zero if and only if $r = \lambda_2$. By (2) this is exactly the case when $k - 1 = v - 1$. □

Thus, if we have a design with $k < v$, then its order n is positive.
We now describe two standard ways to obtain a new structure from an existing one. They will be especially helpful for symmetric designs that we will work with later.

Definition. Let $D = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ be an incidence structure. Then the structure $D^* = (\mathcal{B}, \mathcal{P}, \mathcal{I}^*)$ with

$$(p, B) \in \mathcal{I} \Longleftarrow (B, p) \in \mathcal{I}^* \text{ for all } p \in \mathcal{P}, B \in \mathcal{B}$$

is called the *dual* of D.

For a design $D = (\mathcal{P}, \mathcal{B})$ the dual can be obtained by considering $\mathcal{B}$ as the set of points and $\mathcal{P}$ as the set of blocks. The latter is done by identifying a point p with the set of all blocks that it is contained in. This identification obviously only works for simple designs. Note that if D is a design, then D^* is a 1-design but not always a 2-design. This is because if D^* is a 2-design, it has the parameters 2-$(b, r, \widetilde{\lambda})$ for some integer $\widetilde{\lambda}$. Thus, any two blocks of D need to intersect in a constant number of points. This is usually not the case for arbitrary designs. We will see that the designs D such that D^* is a 2-design are precisely the symmetric designs we will deal with later.
Another important related structure is the complement:

Definition. Let $D = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ be an incidence structure. Then the structure $\overline{D} = (\mathcal{P}, \mathcal{B}, \overline{\mathcal{I}})$ with

$$\overline{\mathcal{I}} := (\mathcal{P} \times \mathcal{B}) \setminus \mathcal{I}$$

is called the *complement* of D.

For a design D the complement $\overline{D}$ is obtained by exchanging every block B for its complement B^C (note that we consider the blocks as subsets of the point set $\mathcal{P}$).

1.6 Lemma. *Let D be a t-(v, k, λ) design with $v - k \geq t$. Then $\overline{D}$ is a t-$(v, v-k, b-2r+\lambda)$ design.*

Proof. Since we have $v - k \geq t$, the parameter t is feasible for $\overline{D}$. The set of points does not change, so $\overline{D}$ has v points, and the blocks of $\overline{D}$ have $v - k$ points because the blocks of D have k points.
Now let $p, q \in \mathcal{P}$ be two distinct points. We need to count the number of blocks of $\overline{D}$ that contain p and q, i.e. the blocks of D containing neither p nor q. There are r blocks containing p, r blocks containing q, and λ blocks containing both points. Thus, there are $2r - \lambda$ blocks containing at least one of the two points. This means that there are $b - 2r + \lambda$ blocks containing neither p nor q. □

The question of which designs are “essentially the same“ comes up naturally. Relabeling points should yield the same design, albeit written down in a different manner. Thus, we need a notion of equivalence for designs, so that we can identify two designs having essentially the same structure with each other.

Definition. Let $D = (\mathcal{P}, \mathcal{B})$ and $D' = (\mathcal{P}', \mathcal{B}')$ be t-designs. A bijection $\varphi : \mathcal{P} \cup \mathcal{B} \to \mathcal{P}' \cup \mathcal{B}'$ is called *isomorphism* between D and D' if the following conditions are satisfied:

(1) $\varphi(\mathcal{P}) = \mathcal{P}'$ and $\varphi(\mathcal{B}) = \mathcal{B}'$

(2) For any $p \in \mathcal{P}$ and $B \in \mathcal{B}$: $p \in B \Longleftrightarrow \varphi(p) \in \varphi(B)$

If there exists an isomorphism between D and D', they are called isomorphic, denoted as $D \cong D'$. An isomorphism of D onto itself is called *automorphism.*
Furthermore if $D \cong D^*$, then D is called *self dual.*

Note that we do not have to map the blocks of D explicitly. As we only deal with simple designs, the image of a block $B \in \mathcal{B}$ must be exactly the set of images of the points contained in it. Thus, we could simplify the definition to require only a bijection between $\mathcal{P}$ and $\mathcal{P}'$ with the map between $\mathcal{B}$ and $\mathcal{B}'$ defined implicitly. However, this approach fails for designs with repeated blocks, and because the above definition is the standard one, we leave it as is.
Now we will define the incidence matrix of a design. It is an important tool for examining designs because it lets us use theorems on matrices from linear algebra.

Definition. Let $D = (\mathcal{P}, \mathcal{B})$ be a t-design. Write $\mathcal{P} = \{p_1, \dots, p_v\}$ and $\mathcal{B} = \{B_1, \dots, B_b\}$ for arbitrary orders of the elements of $\mathcal{P}$ and $\mathcal{B}$. Then the *incidence matrix* $A = (a_{ij})$ of D is a $(v \times b)$-matrix with entries in $\{0, 1\}$ defined by

$$a_{ij} = \begin{cases} 1, & \text{if } p_i \in B_j \\ 0, & \text{if } p_i \notin B_j \end{cases} .$$

Its rows and columns are called *incidence vectors* (of a point or block).

Of course the incidence matrix depends on the chosen orders for $\mathcal{P}$ and $\mathcal{B}$. If we choose another order on $\mathcal{P}$, the incidence matrices are related by a multiplication with a $(v \times v)$-permutation matrix from the left, and similarly a different order on $\mathcal{B}$ corresponds to multiplication with a $(b \times b)$-permutation matrix from the right. Since we are only interested in designs up to isomorphism, the orders of the points and blocks does not matter.
An important property of incidence matrices that will be used very often in this thesis is stated in the following lemma.

1.7 Lemma. *The incidence matrix A of a 2-(v, k, λ) satisfies the following equations:*

(a) $$AA^T = (r - \lambda)I_v + \lambda J_v = \begin{pmatrix} r & \lambda & \lambda & \cdots & \lambda \\ \lambda & r & \lambda & \cdots & \lambda \\ \lambda & \lambda & r & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \lambda \\ \lambda & \lambda & \cdots & \lambda & r \end{pmatrix}$$

(b) $$det(AA^T) = \Big(r + \lambda(v - 1)\Big)(r - \lambda)^{v-1} = rkn^{v-1}$$

Proof. (a) The entries of AA^T are scalar products of the incidence vectors of points. Thus, the diagonal entries are equal to the number of blocks that contain a given point (which is r), and the off-diagonal entries are equal to the number of blocks that contain two given distinct points (which is λ).
(b) One way to calculate the determinant is to use row and column operations to obtain the triangular matrix

$$\begin{pmatrix} r+(v-1)\lambda & * & \cdots & * \\ 0 & r-\lambda & \ddots & \vdots \\ \vdots & \ddots & \ddots & * \\ 0 & \dots & 0 & r-\lambda \end{pmatrix}.$$

Another way is to note that the matrix AA^T has $r+(v-1)\lambda$ as an eigenvalue with multiplicity 1 (with eigenvector $(1,\dots,1)^T$) and $(r-\lambda)$ as an eigenvalue with multiplicity $v-1$ (with eigenvectors $(1,-1,0,\dots,0)^T,(0,1,-1,0,\dots,0)^T,\dots,(0,\dots,0,1,-1)^T$). Either way, we obtain

$$det(AA^T)=(r-\lambda(v-1))(r-\lambda)^{v-1}.$$

By definition we have $n=r-\lambda$ and by lemma 1.5 we have $r+\lambda(v-1)=r+r(k-1)=rk$, giving the desired formula. □

Now we are ready to prove Fisher's inequality. It relates the number of points v to the number of blocks b and motivates the study of symmetric designs.

1.8 Theorem (Fisher's inequality). *Let D be a t-(v,k,λ) design with $t \geq 2$ and $k < v$. Then $v \leq b$.*

Proof. Since $k<v$, we have $n>0$. If D is a t-design with $t \geq 2$, it is also a 2-design by theorem 1.3, so we can apply the above lemma to obtain

$$det(AA^T)=rkn^{v-1}>0.$$

Thus, AA^T is an invertible $(v \times v)$-matrix. But then we have

$$rank(A) \geq rank(AA^T)=v,$$

where the rank is taken over the field of rational numbers $\mathbb{Q}$, so A needs to have at least v columns, i.e. $b \geq v$. □

Definition. A t-(v,k,λ) design is called *symmetric* if it has the same number of points and blocks, i.e. $v=b$.

1.2 Symmetric designs

By Fisher's inequality symmetric designs have the smallest possible number of blocks among all non-trivial designs. In a practical setting this could mean minimal costs, for example if every block represents a test for a disease, an object to be built or similar things. Sometimes it is also surprisingly simple to write down all blocks of a symmetric design. For bigger designs with less internal structure writing down every block can be a big problem.
Note that the incidence matrix of a symmetric design is quadratic but not necessarily symmetric. In this context the term “symmetric“ is somewhat misleading, but it is the standard name for those designs.
This section is based on chapter 4 from “Designs and their Codes“ by Assmus and Key [2].

1.9 Remark. There are many different equivalent definitions for a symmetric design. Here we collect a few:

(a) $v = b$

(b) $r = k$

(c) Any two distinct blocks have exactly λ points in common.

Although symmetric designs have nice properties, there are only interesting (i.e. non-trivial) symmetric designs for $t = 2$. This might be a little disappointing at first, but there is still a lot to discover about symmetric designs.

1.10 Theorem. *Every symmetric t-(v, k, λ) design D with $t \geq 3$ is trivial, i.e. every subset of $\mathcal{P}$ with k elements is a block.*

Proof. Without loss of generality we assume $t = 3$. If we have a design with $t > 3$, we view it as a 3-(v, k, λ_3) design according to theorem 1.3. Furthermore, we assume $k < v$, otherwise D is obviously trivial.
Choose any point $p \in \mathcal{P}$ and consider the structure $D_p := (\mathcal{P}_p, B_p)$ defined by

$$\mathcal{P}_p = \mathcal{P} \setminus \{p\}, \quad B_p = \{B \setminus \{p\} \mid B \in \mathcal{B} \text{ with } p \in B\}.$$

It consists of all points except p together with all blocks that contain p. It is easy to check that D_p is a 2-design (in general if D is a t-design, then D_p is a $(t-1)$-design). Since D has v points and p is contained in exactly r blocks, D_p has $v - 1$ points and $r = k$ blocks (D is symmetric), each containing $k - 1$ points. As we have $k < v$, we have $k - 1 < v - 1$, so we can invoke Fisher's inequality for D_p to obtain

$$v - 1 \leq r = k.$$

Since $k < v$, k can only equal $v - 1$. This means that D is a trivial t-$(v, v-1, \lambda)$ design. □

In view of this theorem we will only deal with symmetric 2-designs. From now on if we write “symmetric“ design, we mean a symmetric 2-design. We will also assume $\lambda < k < v-1$ because designs with $k = \lambda$, $k = v-1$ or $k = v$ are trivial.
One symmetric design actually gives rise to three more symmetric designs, that may or may not be isomorphic to the first one.

1.11 Lemma. *Let D be a symmetric 2-(v,k,λ) design. Then its dual D^* is a symmetric 2-(v,k,λ) design, its complement $\overline{D}$ is a symmetric 2-$(v, v-k, v-2k+\lambda)$ design and the complement of the dual $\overline{D^*}$ is a symmetric 2-$(v, v-k, v-2k+\lambda)$ design.*

Proof. By definition D^* is a 1-(b,r,k) design. Since D is symmetric, we have $v = b, r = k$ and any two blocks intersect in precisely λ points by remark 1.9. Thus, D^* is a 2-(v,k,λ) design.
By our assumptions we have $k \leq v-2$, so we can apply lemma 1.6. We obtain that $\overline{D}$ and $\overline{D^*}$ are designs with parameters 2-$(v, v-k, v-2k+\lambda)$ and they are symmetric because taking the complement of a design does not change the number of blocks. □

It is easy to see that $\overline{D^*} = \overline{D}^*$, so the order of operations does not matter and does not give rise to two different designs.
Some examples of symmetric designs are the following.

1.12 Example. (a) The Fano plane from example 1.2 is symmetric and its complement is a symmetric 2-$(7,4,2)$ design. Both designs are self dual.
(b) The 2-$(4n-1, 2n-1, n-1)$-Hadamard designs ($n \in \mathbb{N}$):
An incidence matrix of a Hadamard design can be derived from a Hadamard matrix, i.e. an $(n \times n)$-matrix H with $HH^T = nI_n$ and entries only $+1$ and -1. The Hadamard designs can be constructed by taking a normed Hadamard matrix of size $4n$ (i.e. all entries in the first row and column are equal to 1), deleting the first row and column and exchanging all -1 for 0. Their complements are 2-$(4n-1, 2n, n)$ designs and are sometimes also called Hadamard designs.

Hadamard designs are important because they realise an extreme case for symmetric designs. They have as few points as possible given the order n. We have the following theorem:

1.13 Theorem. *Let D be a symmetric 2-(v,k,λ) design with order n. Then we have*

$$4n-1 \leq v \leq n^2+n+1.$$

Proof. By lemma 1.5b and because D is symmetric, we have

$$k(k-1) = \lambda(v-1).$$

It follows that λ divides $k(k-1)$, so it also divides $(k-\lambda)(k-\lambda-1) = n(n-1)$. Write $n(n-1) = \lambda\mu$ for some integer $\mu \geq 0$. Then we have

$$v = \frac{k(k-1)}{\lambda} + 1 = \frac{(n+\lambda)(n+\lambda-1)}{\lambda} + 1$$

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

We start with the case $n = 1$ so that we can assume $n \geq 2$ and thus $\mu > 0$ later. If $n = 1$, then we have $\mu = 0$, $k = n + \lambda = \lambda + 1$ and $v = 2n + \lambda + \mu = \lambda + 2$. Thus, D is a 2-$(\lambda + 2, \lambda + 1, \lambda)$ design. But then we have $k = v - 1$, violating our assumption $k < v - 1$, so the case $n = 1$ is not possible.
Now assume $n \geq 2$. For the upper bound note that we have $\lambda, \mu \geq 1$. It follows that $(\lambda - 1)(\mu - 1) \geq 0$, or equivalently $\lambda + \mu \leq \lambda\mu + 1$. We obtain

$$v = 2n + \lambda + \mu \leq 2n + \lambda\mu + 1 = 2n + n(n-1) + 1 = n^2 + n + 1.$$

For the lower bound note that

$$\begin{aligned}(\lambda - \mu)^2 &= (\lambda - (v - 2n - \lambda))^2 = (2(n + \lambda) - v)^2 = (2k - v)^2 = v^2 - 4kv + 4k^2 \\ &= v^2 - 4k(v-1) - 4k + 4k^2 = v^2 - 4k(v-1) + 4k(k-1) \\ &= v^2 - 4k(v-1) + 4\lambda(v-1) = v^2 - (4k - 4\lambda)(v-1) = v^2 - 4n(v-1).\end{aligned}$$

Since $\lambda\mu = n(n-1)$, we have $\lambda \neq \mu$ because $n(n-1)$ can never be a perfect square (remember that $n > 1$). Thus, we have

$$0 < (\lambda - \mu)^2 = v^2 - 4n(v-1)$$

and we obtain

$$v^2 - 4n(v-1) - 1 \geq 0.$$

Rearranging gives

$$(v-1)(v - 4n + 1) \geq 0,$$

and as we have $v > 1$, we finally obtain $v \geq 4n - 1$. □

For many $n \in \mathbb{N}$ there are symmetric designs with $4n - 1$ and $n^2 + n + 1$ points, respectively. However, in general it is an open question for which values of n such designs exist. The case $v = 4n - 1$ is realised by the Hadamard designs from example 1.12b, and the case $v = n^2 + n + 1$ is realised by the finite projective planes that we will deal with in the next chapter.
We close this chapter with a theorem characterizing symmetric designs with order n and $n^2 + n + 1$ points.

1.14 Theorem. *Let D be a symmetric design with order $n \in \mathbb{N}$ and $v = n^2 + n + 1$ points. Then D is either a 2-$(n^2 + n + 1, n + 1, 1)$ design or its complement, i.e. a 2-$(n^2 + n + 1, n^2, n(n-1))$ design.*

Proof. In the proof of the upper bound of theorem 1.13, the case $v = n^2 + n + 1$ occurs exactly when $(\lambda - 1)(\mu - 1) = 0$, i.e. $\lambda = 1$ or $\mu = 1$. Since we have $\lambda\mu = n(n-1)$, we can directly write down the parameters of the resulting designs. The case $\lambda = 1$ gives rise to a 2-$(n^2 + n + 1, n + 1, 1)$ design, while the case $\mu = 1$ gives rise to a 2-$(n^2 + n + 1, n^2, n(n-1))$ design. By lemma 1.11 this is the complement of a 2-$(n^2 + n + 1, n + 1, 1)$ design. □

1.15 Remark. An analogous theorem holds for Hadamard designs:
A symmetric design with order $n \geq 2$ and $v = 4n - 1$ points is a Hadamard design, i.e. a 2-$(4n - 1, 2n - 1, n - 1)$ design, or its complement, i.e. a 2-$(4n - 1, 2n, n)$ design.

2 Projective Planes

The goal of this thesis is to gain insight into the possible orders of finite projective planes. This section gives an overview of the definitions and theorems needed. Most results in this chapter are taken from the book “Projective Planes“ by Hughes and Piper [28] and the reader is referred there for a broader overview of the theory. The remaining design theoretic results can be found in chapter 3 of the book “Designs and their Codes“ by Assmus and Key [2].

2.1 Basic results

There are many equivalent definitions of a projective plane. Here we give one that fits our purpose and emphasises the connection to design theory.

Definition. Let $n \geq 2$ be an integer. A 2-$(n^2+n+1, n+1, 1)$ design is called a *finite projective plane.* The number n is called the *order* of the plane.

As we view projective planes as designs, we do not need to define terms like *isomorphism, automorphism* and *dual structure* for projective planes because we have already defined them for designs. This is not a synthetic geometric definition, but it fits our purposes perfectly. For comparison and historic context we give a more standard definition of a projective plane and then shortly discuss both definitions.

Definition. A *projective plane* Π is an incidence structure $\Pi = (\mathcal{P}, \mathcal{L}, \mathcal{I})$ of a non-empty set $\mathcal{P}$ of *points* and a non-empty set $\mathcal{L}$ of *lines* with $\mathcal{P} \cap \mathcal{L} = \emptyset$ such that the following hold:

(1) For any two points $p \neq q \in \mathcal{P}$ there exists a unique line $L \in \mathcal{L}$ such that $p, q \,\mathcal{I}\, L$. This line is denoted with $L = pq$ and we say that L *joins* p and q.

(2) For any two lines $L \neq M \in \mathcal{G}$ there exists a unique point $p \in \mathcal{P}$ such that $p \,\mathcal{I}\, L, M$. This point is (in abuse of notation) denoted with $p = L \cap M$.

(3) There exists a quadrangle, i.e. four distinct points such that no three of those points are collinear.

The plane Π is called *finite* if $|\mathcal{P}| < \infty$. Points will be denoted with lower case letters and lines with upper case letters.

This definition easily handles infinite projective planes, which our design theoretic definition cannot handle. However, this is not a problem for us since the prime power conjecture only deals with finite projective planes.
It is easy to show that the two definitions are equivalent. Thus, the class of symmetric designs with order $n \geq 2$ and parameters 2-$(n^2+n+1, n+1, 1)$ is precisely the class of finite projective planes in the sense of the geometric definition. This also means that without loss of generality we can view the lines as sets of points and the incidence relation $\mathcal{I}$ as the membership relation $\in$. So for our purposes, a projective plane is just a pair $\Pi = (\mathcal{P}, \mathcal{L})$ without explicitly mentioning the incidence relation. Problems with this approach only arise in cases where the third axiom does not hold, i.e. incidence structures without a quadrangle.
If we accept the 2-$(3,2,1)$ design as a projective plane, then the two definitions do not agree anymore because the 2-$(3,2,1)$ design is not the only incidence structure without a quadrangle satisfying the first two axioms for a projective plane. One way to obtain such a *degenerate plane* is to take $n+1$ points with a line containing n of them. Then for every point on this line add a line containing this point and the point not on the line. Figure 2.1 illustrates the construction.

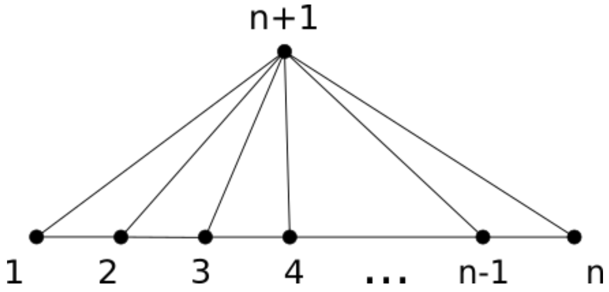


Figure 2.1: A degenerate projective plane

This incidence structure satisfies the first two axioms for a projective plane. Any two distinct points are joined by a unique line and any two distinct lines intersect in a unique point. However, we see that not all lines have the same number of points, so this is not a design and the two definitions do not agree anymore. This is because this incidence structure does not contain a quadrangle, and this is why we only deal with designs of order $n \geq 2$.
Examples of finite (and also infinite) projective planes are the projective planes $PG(2, F)$ for a field F, called *pappian planes*. The term “pappian“ is due to the fact that the projective planes $PG(2, F)$ are exactly the projective planes where a geometric result called “Pappus’ Theorem“ is universally valid. However, we do not need the theorem in this thesis.

2.1 Example. Let F be a field. The projective plane $PG(2, F)$ is given by:

- The set of points $\mathcal{P} = \{U \subset F^3 \,|\, U \text{ is a 1-dimensional subspace of } F^3\}$
- The set of lines $\mathcal{L} = \{L \subset F^3 \,|\, L \text{ is a 2-dimensional subspace of } F^3\}$

Any two distinct points $U, U' \in \mathcal{P}$ lie on exactly one line, namely $U + U'$, and any two distinct lines $L, L' \in \mathcal{L}$ intersect in exactly one point because of the dimension formula:

$$dim(L \cap L') = \dim(L) + dim(L') - dim(L + L') = 2 + 2 - 3 = 1$$

The subspaces generated by the points $(1, 0, 0), (0, 1, 0), (0, 0, 1)$ and $(1, 1, 1)$ form a quadrangle.
This type of projective plane is finite if and only if F is a finite field. If $|F| = q$, i.e. $F = \mathbb{F}_q$ for some prime power q, then the projective plane $PG(2, F)$ is a 2-$(q^2 + q + 1, q + 1, 1)$ design and is usually denoted as $PG(2, q)$. We see that its order is q.

If F is a skewfield, then we can also construct the projective planes $PG(2, F)$. These are called the *desarguesian planes.* Since every finite skewfield is a field, there is no difference between desarguesian and pappian planes for finite projective planes. As with pappian planes, the term desarguesian planes comes from a geometric result called "Desargues' Theorem" that is universally valid in $PG(2, F)$ if F is a skewfield. However, we do not need this theorem in this thesis. Nonetheless, as the term "desarguesian" appears in the theory of projective planes quite frequently, we still define it. For our purposes it is enough to know that the desarguesian planes are the projective planes $PG(2, F)$ for a skewfield F.
From the construction above we immediately obtain:

2.2 Theorem. *If $q = p^n$ is a prime power, then there exists a finite projective plane of order q.*

Proof. If $q = p^n$ is a prime power, then the projective plane $PG(2, q)$ has order q. □

This is a first indication towards the plausibility of the prime power conjecture. For every prime power there is a finite field and the size of every finite field is a prime power, so the order of desarguesian planes is always a prime power. However, not all projective planes are of this type. In fact, today there are many different projective planes known and the vast majority are not desarguesian planes.
An important concept in projective geometry is *duality.* We have already seen in chapter 1 that every design has a dual and that the dual of a symmetric design is again a symmetric design with the same parameters. Since finite projective planes are symmetric designs, the dual of a finite projective plane is again a finite projective plane. An important consequence of this fact is that we get "two theorems for the price of one": If we know that a statement about projective planes is true for every projective plane, then the dual of that statement is also true for every projective plane. We formalise this concept:

Definition. If we have a statement A about projective planes, then the *dual statement* A^* is obtained by interchanging the words "point" and "line" and switching the concepts "lies on" and "goes through".

For example, the dual of the statement "Any point lies on at least 3 lines" is "Any line goes through at least 3 points". The projective planes $PG(2, q)$ that we defined above are

self dual. An isomorphism between $PG(2,q)$ and $PG(2,q)^*$ is given by taking orthogonal complements. This converts 1-dimensional subspaces (i.e. points) into 2-dimensional subspaces (i.e. lines) and vice versa and preserves incidence. So if a theorem is true for $PG(2,q)$ (that does not have to be true for *all* projective planes), then its dual is also true for $PG(2,q)$.
Another important concept is switching between projective and affine planes. As with projective planes, we define affine planes from the view of design theory.

Definition. Let $n \geq 2$ be an integer. A 2-$(n^2, n, 1)$ design $\mathcal{A} = (\mathcal{P}, \mathcal{L})$ is called a *finite affine plane.* The number n is called the *order* of the plane.

The term “order“ has a slightly different definition for affine planes compared to projective planes. The *order* of an affine plane is the number of points on any line, so an affine plane that is a 2-$(n^2, n, 1)$ design is an affine plane of order n while its order as a design is $n-1$ (a projective plane of order n has $n+1$ points on any line and order n as a design).

2.3 Example. Let F be a field. The affine plane $AG(2,F)$ is given by:

- The set of points $\mathcal{P} = F^2$
- The set of lines $\mathcal{L} = \{x + L \subset F^2 \,|\, x \in F^2,\ L \text{ is a 1-dimensional subspace of } F^2\}$

The lines of $AG(2,F)$ are simply all lines of F^2 and its translates, i.e. all 1-dimensional affine subspaces of F^2. If F is a finite field with q elements, then $AG(2,F)$ has q^2 points and every line has q points. Two distinct points $a, b \in F^2$ lie on a unique affine subspace, namely $a + F(b-a)$. Thus, $AG(2,F)$ is an affine plane and is also denoted as $AG(2,q)$. Its order is q.

Affine planes do not exhibit the same duality as projective planes do, but they are important to us because of the following two theorems.

2.4 Theorem. *Let $\Pi = (\mathcal{P}, \mathcal{L})$ be a projective plane of order n and L any line of Π. Then the incidence structure $\Pi^L := (\mathcal{P} \setminus L, \mathcal{L} \setminus \{L\}, \in)$ obtained by removing all points of L from Π is an affine plane of order n. We will call this the* affine residual *of Π.*

Proof. We know that Π is a 2-$(n^2+n+1, n+1, 1)$ design and we have to show that Π^L is a 2-$(n^2, n, 1)$ design. Removing the line L removes $n+1$ points, so Π^L has n^2 points. Since Π is symmetric, any two lines intersect in a unique point. Thus, any line other than L contains exactly one point of L, i.e. any line in Π^L has n points. Finally, any two distinct points lie on a unique line as this was already true for Π. Thus, Π is a 2-$(n^2, n, 1)$ design, i.e. an affine plane of order n. □

We see that a projective plane of order n gives rise to an affine plane of order n. The converse is also true:

2.5 Theorem. *Let $\mathcal{A} = (\mathcal{P}, \mathcal{L})$ be an affine plane of order n. Then there exists a projective plane Π such that $\mathcal{A} = \Pi^L$ for some line L of Π.*

Proof. We use the same construction as in theorem 2.4 but backwards, i.e. we add $n+1$ points to $\mathcal{A}$, add a line containing those $n+1$ points to $\mathcal{L}$ and add one point to every line in an appropriate way.
We know that $\mathcal{A}$ is a 2-$(n^2, n, 1)$ design. Thus, through a given point p there are

$$r = \lambda \frac{v-1}{k-1} = \frac{n^2-1}{n-1} = n+1$$

lines. Since every line has n points and any two points of $\mathcal{A}$ lie on a unique line, it follows that for every line L and every point $p \notin L$ there is a unique line M through p that does not intersect L. This allows us to decompose the set of lines $\mathcal{L}$ into parallel classes, i.e. sets of pairwise disjoint lines. Every parallel class is a partition of the point set (given a block, there is a parallel through every point and two distinct parallels cannot intersect because the parallel through every point is unique). Since there are $n+1$ lines through any point, there are $n+1$ parallel classes.
We now add $n+1$ points to $\mathcal{A}$ and associate every point with a parallel class. Every new point is added to all lines of its associated parallel class. Finally, we add one line to $\mathcal{A}$ that contains all $n+1$ new points. We claim that this structure Π is a 2-$(n^2+n+1, n+1, 1)$ design.
It is immediate that Π has n^2+n+1 points and every line has $n+1$ points. Now consider two points $p \neq q$ of Π. If both are points of $\mathcal{A}$, then there is a unique line through p and q in $\mathcal{A}$ and thus by construction a unique line through p and q in Π. If exactly one of them is one of the new points that were added to $\mathcal{A}$, say q, then there is a unique line containing both p and q, namely the line of the parallel class associated with q that goes through p. Finally, if both p and q are new points, then they are on the unique new line that was added to $\mathcal{A}$. Thus, Π is a 2-$(n^2+n+1, n+1, 1)$ design, i.e. a projective plane of order n. By construction we have $\mathcal{A} = \Pi^L$ for the new line L. □

This means that there exists a projective plane of order n if and only if there exists an affine plane of order n. It can be shown that the projective plane in theorem 2.5 is unique up to isomorphism. This justifies calling it *the projective completion* of $\mathcal{A}$.
Applying the last two theorems to the projective planes $PG(2,q)$, it is easily seen that every affine residual of $PG(2,q)$ is isomorphic to $AG(2,q)$. Conversely, the projective completion of $AG(2,q)$ is $PG(2,q)$.
The last two theorems show that affine and projective planes are closely related and that we can switch back and forth between them without much effort. We will often consider them together and work in the structure that is better suited for the context we are dealing with. If we have an affine plane $\mathcal{A}$ and a projective plane Π with $\mathcal{A} = \Pi^L$, we will call L the *line at infinity* of $\mathcal{A}$ and we will say that the lines of $\mathcal{A}$ intersect the line at infinity L, even when we consider them as lines in $\mathcal{A}$ where the line at infinity does not exist. Conversely, we will call the points of Π that are not on the line L the *affine* points of Π, even if we did not construct Π from an affine plane. As long as we specify the line L by which the two planes are related, this will not cause any confusion. It should be noted that removing any line from a projective plane yields an affine plane but the affine planes obtained by removing different lines need not be isomorphic. This

is the reason why it is important to clarify which line is to be taken as the line at infinity. If we start with an affine plane $\mathcal{A}$ and then speak of the affine points of its projective completion Π, they are always to be taken with respect to the line at infinity that was added to construct Π from $\mathcal{A}$.

2.2 History of the prime power conjecture

In this section we give a short historic overview of the key results on projective planes regarding the prime power conjecture. History of projective geometry is taken from the book “Geometry in History“ [12] (especially chapter 6 by Sunada and chapter 8 by Pambuccian and Schacht) and the reader is also referred there for further reading. More about the history of finite geometries can be found in the well-known book “Finite Geometries“ by Dembowski [13].

One of the major influences of projective geometry was the art of drawing in perspective. This goes back to the 15th century with Filippo Brunelleschi (1377 - 1446) named as the creator of this technique, allowing artists to paint objects and places like one might actually see them. Projective geometry as a mathematical discipline goes mainly back to Girard Desargues (1591 - 1661). The well-known “Desargues’ Theorem“ appeared in one of his books in 1639. At this point in time projective geometry was not concerned with finite models and was not built upon an axiomatic system like it is today.
In the 19th century some mathematicians, for example Karl von Staudt (1798 - 1867), started considering *finite* projective geometries. Von Staudt developed a theory in which he viewed finitely many points in the real plane [52]. But although projective geometry had already been studied extensively, it was not until the end of the 19th century that the *axiomatic* definition of a projective plane came about. It is attributed to Gino Fano, one of the founders of finite geometry. In his article from 1892 [19], he considers a set of points and a set of subsets of that set, called lines, and gives some postulates that those sets should satisfy. His axioms, stated in a slightly more modern language, were:

1) Any two points lie on exactly one line.

2) Each line is completely determined from any two of its points.

3) Any two lines meet in exactly one point.

4) Each line contains at least three points.

This is very close to our modern definition we gave before. Fano then derives some properties from these axioms like the number of points of a projective plane, defines further concepts like the projective harmonic conjugate and also constructs the projective planes $PG(2, p)$ for a prime number p (in fact, he constructed the projective spaces $PG(k, p)$ of dimension k for a positive integer k and a prime p). This means that he proved that there exists a finite projective plane of order p for any prime number p.

In 1906, Oswald Veblen and William Henry Bussey [55] constructed the projective planes $PG(2, q)$ for all prime powers $q = p^n$. Since $PG(2, q)$ has order q, this showed that any prime power can be the order of a finite projective plane. They also gave a system of axioms for projective geometry and constructed projective spaces of higher dimension. Using their axiom system they showed that every projective space of dimension $k \geq 3$ is isomorphic to $PG(k, q)$, showing that only the case of dimension 2 gives rise to a wide variety of different projective geometries. In the case of dimension 2 the plane $PG(2, q)$ is not the only projective plane of order q. For example, the projective plane of order 2 is unique (up to isomorphism), but there are four non-isomorphic projective planes of order 9 (see chapter 7). After projective planes with order q for any prime power q became known, but no one could construct a projective plane with order not a prime power, it was conjectured that no such planes exist. It seems that this conjecture cannot be ascribed to a single person, but rather that it arose in the mathematical community over time.

At the beginning of the 20th century, the smallest open case was whether or not there exists a projective plane of order 6 because the number 1 cannot be the order of a (non-degenerate) projective plane by definition and the numbers 2, 3, 4 and 5 are all prime powers. Nowadays we know that there is no projective plane of order 6. In principle this was proved by Gaston Tarry in 1901 [53]. He proved that Euler's "Thirty-Six officers problem" had no solution. Euler's problem is essentially asking whether there is a pair of orthogonal Latin squares of order 6. We briefly define this term.

Definition. A Latin square of order n is an array of size $n \times n$ filled with n different symbols such that every symbol occurs exactly once in every row and exactly once in every column. Two Latin squares A and B are called orthogonal if the n^2 pairs obtained by superimposing A on B are all different.

Thus, put another way, Tarry proved that there exist no mutually orthogonal Latin squares of order 6. His proof essentially consisted of checking every case, i.e. a proof by exhaustion. However, the connection between mutually orthogonal Latin squares and finite projective planes was not known until 1938, when Raj Chandra Bose published an article on the topic [7]. Bose proved that the existence of a set of $n - 1$ mutually orthogonal Latin squares is equivalent to the existence of an affine plane of order n (and thus equivalent to the existence of a projective plane of order n). It can be shown that for any integer $n \geq 2$ there can be no more than $n - 1$ mutually orthogonal Latin squares, so a set of $n - 1$ such squares is called *complete*. As Tarry proved that there are no two mutually orthogonal Latin squares of order 6, there surely cannot be a complete set of mutually orthogonal Latin squares of order 6. Bose's theorem together with Tarry's result proves that there is no projective plane of order 6 and the case $n = 6$ was thus settled in 1938.

The next big step regarding projective planes and the prime power conjecture was the Bruck-Ryser theorem published by Richard Bruck and Herbert Ryser in 1949 [8]. It was arguably the biggest step towards the prime power conjecture so far and probably still is today because it settles the non-existence for infinitely many cases. It states that if the order n of a projective plane is congruent to 1 or 2 modulo 4, then n is a sum of two squares. Using this theorem we can immediately rule out values like 14 or 22. We also get another proof that there exists no finite projective plane of order 6 (which can be considered “better“ than Tarry’s proof because enumeration by hand is prone to errors and some cases can easily be overlooked). However, since 10 is the sum of two squares, the theorem does not help us with the case $n = 10$. The Bruck-Ryser theorem was generalised to the Bruck-Ryser-Chowla theorem, which is applicable to arbitrary symmetric designs, in 1950 [9]. However, this generalisation does not give new constraints on the order of a projective plane. We will deal with the Bruck-Ryser-Chowla theorem and its consequences in detail in chapter 5.

After the Bruck-Ryser theorem settled infinitely many cases, there was only one more case for which the non-existence was proven. It was the next smallest open case, i.e. the case $n = 10$. This was done by Clement Lam et al. in 1989. The work of many different people went into this and we cannot name everybody here. We will only give a very rough description of the proof. For a more detailed illustration of the proof, the story behind it and references for the results that went into the proof, the reader is referred to Lam’s article [31].

The proof that there is no projective plane of order 10 relies on an exhaustive search on a computer made possible by methods to reduce the size of the search space. The key idea of the proof was to consider the binary code of a (hypothetical) projective plane Π of order 10, i.e. the vector space over $\mathbb{F}_2$ spanned by the columns of any incidence matrix of Π (or equivalently the row span since the dual of Π is also a projective plane of order 10). One important quantity of a codeword (i.e. an element of the code) is its weight, which is the number of non-zero coordinates it has. Assmus and Mattson showed that the number of codewords of weight k in the code of a projective plane of order 10 is uniquely determined by the number of codewords of weight 12, 15 and 16. MacWilliams et al. showed that there are no codewords of weight 15. The other numbers were later shown to be equal to zero as well. Thus, it could now be calculated that there would have to be exactly 24675 codewords of weight 19. The final part was then letting a computer check all possible configurations showing that there are no codewords of weight 19. This contradiction shows that there is no projective plane of order 10. A very big amount of computing time went into the proof. The final program ran for over two years and there were even some computer errors along the way. After these were dealt with, the project was eventually finished in 1989.

After that there were no major breakthroughs regarding the prime power conjecture. The smallest open case today is $n = 12$. No one has found a projective plane of order 12 or proven that it does not exist. There are some coding theoretic results analogous to the case $n = 10$. For example, Hall and Wilkinson considered ternary (i.e. over $\mathbb{F}_3$) and binary codes for a projective plane of order 12 [23]. They showed that the number of codewords of any weight k in the ternary code can be calculated in terms of twelve parameters, which is a lot more than in the case $n = 10$ where three parameters were sufficient. Furthermore, the binary code of a projective plane of order 12 is harder to deal with than the binary code in the case $n = 10$, so using the same approach as in the case $n = 10$ seems very challenging. In theory it is possible to adapt Lam's method to the search for a projective plane of order 12. However, the search space is much bigger and even with faster computers that we have today - 30 years later - it seems infeasible. It looks like we are still quite far away from proving or disproving the existence of a projective plane of order 12.

Apart from work on the next smallest case, there are some proofs of special cases of the prime power conjecture. For example, Blokhuis, Jungnickel and Schmidt showed that the prime power conjecture holds for finite projective planes of order n that have an abelian collineation group (which is another word for an automorphism group in the context of geometry) of order n^2 [6]. A similar result was proven by Jungnickel and de Resmini [30]. They proved the same result but for an abelian collineation group of order $n(n-1)$. Other results include the determination of planes that admit a certain group as a collineation group or the non-existence of planes with a certain collineation group or with a certain substructure.

In the next chapter we turn to an older special class of projective planes essentially developed by André in 1954 [1], building on the works of Moufang and Hall. He dealt with structures called *translation planes*. Like the newer results mentioned above, it is a class of projective planes with certain restrictions on the existence of collineation groups. It turns out that their order is always a prime power.

3 Translation planes

In this chapter we will investigate translation planes. We are only interested in finite translation planes but many results in this chapter hold for infinite planes as well. Our goal is to prove the following theorem about translation planes, which will be defined afterwards.

3.1 Theorem. *Let* Π *be a translation plane of order* n*. Then* n *is a prime power.*

There are many different ways to prove this theorem. We will take one that does not require much foreknowledge and needs only few preliminary results. As our approach to projective planes is rooted in design theory, we will prove this theorem from a combinatorial point of view, avoiding the introduction of coordinates in a suitable algebraic structure.

3.1 Collineations and collineation groups

The defining property of translation planes is the existence of certain *collineations*. Before we can define translation planes, we need to define and study these collineations. The results in this section are taken from chapter 4 of the book "Projective Planes" by Hughes and Piper [28].

Definition. Let Π be a projective plane. An autormorphism of Π is called a *collineation*. The group of all collineations of Π is called the *full collineation group* of Π, denoted $\mathrm{Aut}(\Pi)$. A subgroup of $\mathrm{Aut}(\Pi)$ is called *a collineation group*.

It is straightforward to check that $\mathrm{Aut}(\Pi)$ is a group with respect to composition of functions. In slight abuse of notation we will denote the identity collineation with 1. Our first goal is to prove the following theorem that gives a very important insight into the structure of collineations.

3.2 Theorem. *Let* Π *be a finite projective plane and* $\alpha \neq 1$ *be a collineation. If* α *fixes a line* L *pointwise, then there exists a point* p *fixed linewise by* α *(i.e.* $\alpha(M) = M$ *for all lines* M *through* p*). Furthermore,* α *fixes no other point or line.*

An easy proof can be given by using *closed Baer subsets*.

Definition. Let $\Pi = (\mathcal{P}, \mathcal{L})$ be a projective plane and $\widetilde{\Pi} = (\widetilde{\mathcal{P}}, \widetilde{\mathcal{L}})$ be a substructure of Π (i.e. $\widetilde{\mathcal{P}} \subseteq \mathcal{P}$ and $\widetilde{\mathcal{L}} \subseteq \mathcal{L}$).

(a) $\widetilde{\Pi}$ is called *closed* if it satisfies the first two axioms of the geometric definition of a projective plane, i.e. any two points are joined by a unique line and any two lines intersect in a unique point.

(b) $\widetilde{\Pi}$ is called a *Baer subset* (also called a *dense* subset) if every point of Π is incident with a line of $\widetilde{\Pi}$ and every line of Π is incident with a point of $\widetilde{\Pi}$.

The importance of closed Baer subsets to us is due to the following lemma.

3.3 Lemma. *Let Π be a projective plane. A closed Baer subset $\mathcal{B}$ of Π is either a subplane of Π or it consists of a line L and all the points on it together with a point p and all the lines through it.*

Proof. If $\mathcal{B}$ contains a quadrangle, then $\mathcal{B}$ is a projective plane and thus a subplane of Π. So we can now assume that $\mathcal{B}$ does not contain a quadrangle. We consider two cases.
Case 1: $\mathcal{B}$ contains a triangle.
Call the points of the triangle a, b, c. Then all points of $\mathcal{B}$ must lie on one of the three sides ab, ac and bc of the triangle because we assumed that $\mathcal{B}$ does not contain a quadrangle. In fact, only one of the sides of the triangle can contain more than two points because if we had two distinct lines with at least three points on them, then there would exist four points that form a quadrangle. Without loss of generality let this be the side bc.
Now let q be any point on bc not equal to b or c (exists because any line of a projective plane contains at least three points) and let L be any line through q not equal to bc or aq (exists because any point of a projective plane lies on at least three lines). Since $\mathcal{B}$ is a Baer subset, $\mathcal{B}$ must contain a point of L. But since L does not contain the point a by construction, this point must lie on bc as it is the only line that can contain points other than a, b, c. The intersection of L and bc is the point q that was chosen in the beginning. Thus, $\mathcal{B}$ contains the point q. Since q was an arbitrary point on the line bc, $\mathcal{B}$ contains every point of bc, and since $\mathcal{B}$ is closed, it also contains the lines joining a to the points of bc as well as the line bc itself. As any line through a intersects bc, $\mathcal{B}$ contains all lines through a.
Finally, $\mathcal{B}$ cannot contain any other point of Π because every point of $\mathcal{B}$ other than a must lie on the line bc. Similarly, $\mathcal{B}$ cannot contain any other line of Π because any line other than bc and the lines through a would intersect at least one of the sides ab and ac in a point other than a, b, c. But since $\mathcal{B}$ is closed, this point would have to belong to $\mathcal{B}$ too, which cannot be the case. An example visualisation is given in figure 3.1. It has the same structure as the degenerate projective plane that we constructed as an example in chapter 2.
Case 2: $\mathcal{B}$ does not contain a triangle.
Then all points of $\mathcal{B}$ must lie on one line of Π, call this line L. Consider a point p on L and a line $M \neq L$ through p. Since $\mathcal{B}$ is a Baer subset, $\mathcal{B}$ must contain a point of M. As all points of $\mathcal{B}$ lie on L, this must be the point $L \cap M = p$. As p was an arbitrary point on L, all points of L must belong to $\mathcal{B}$. Since $\mathcal{B}$ is closed, the line L also belongs to $\mathcal{B}$.
Now consider a point p not on L. Then $\mathcal{B}$ must contain a line M through p. Let the intersection $L \cap M$ be the point q. Now $\mathcal{B}$ cannot contain a line through any point other

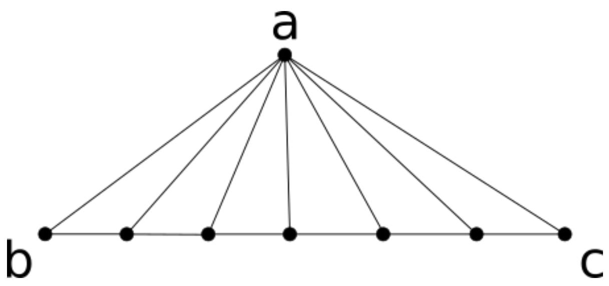


Figure 3.1: A closed Baer subset with a triangle

than q because otherwise the intersection of that line with M would have to belong to $\mathcal{B}$ (since $\mathcal{B}$ is closed), but it would not lie on L. Thus, all lines of $\mathcal{B}$ go through q. Finally, as $\mathcal{B}$ is a Baer subset, its lines must cover all points of Π. Thus, all lines through q belong to L. An example visualisation is given in figure 3.2. □

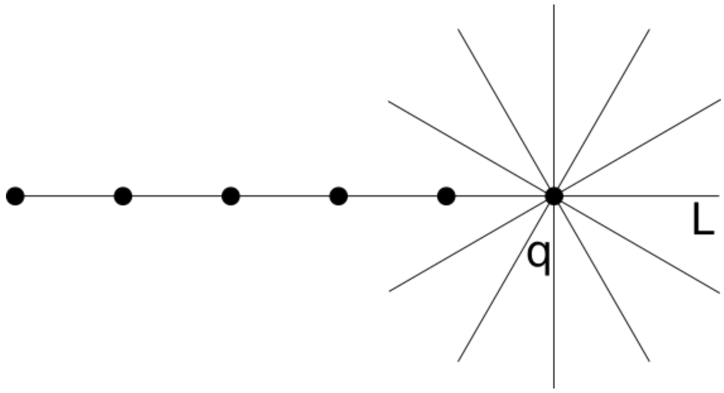


Figure 3.2: A closed Baer subset without a triangle

We are now ready to prove theorem 3.2.

Proof of theorem (3.2). Let $\mathrm{Fix}(\alpha)$ denote the incidence structure whose points and lines are the points and lines of Π that are fixed by α, respectively. The idea is to prove that $\mathrm{Fix}(\alpha)$ is a closed Baer subset and then invoke lemma 3.3. First note that since every line of Π intersects L, every line of Π contains a point of $\mathrm{Fix}(\alpha)$.
Let p be any point that does not lie on L.
Case 1: $\alpha(p) = p$
Then for all points q on L we have $\alpha(pq) = \alpha(p)\alpha(q) = pq$, as α fixes p by assumption and q because it lies on L. Thus, α fixes the line pq and p is incident with a line of $\mathrm{Fix}(\alpha)$.
Case 2: $\alpha(p) \neq p$
Consider the point $q = p\alpha(p) \cap L$. Then we have

$$\alpha(pq) = \alpha(p)\alpha(q) \overset{q \in L}{=} \alpha(p)q = pq.$$

The last equality is due to the fact that q lies on the line joining p and $\alpha(p)$. Thus, p is again incident with a line of $\mathrm{Fix}(\alpha)$. We have thus shown that $\mathrm{Fix}(\alpha)$ is a Baer subset of Π. It remains to show that $\mathrm{Fix}(\alpha)$ is closed.
In case 1 we have already seen that if α fixes p and q, then it fixes the line pq, and thus pq belongs to $\mathrm{Fix}(\alpha)$. Arguing dually, if α fixes the lines M and N, then it fixes the point $M \cap N$, and thus $M \cap N$ also belongs to $\mathrm{Fix}(\alpha)$. This means that $\mathrm{Fix}(\alpha)$ is closed.
Now by lemma 3.3 $\mathrm{Fix}(\alpha)$ is either a subplane of Π or a line with all of its points together with a point and all lines through it. The latter is exactly what we want so the last part is to prove that $\mathrm{Fix}(\alpha)$ cannot be a subplane of Π.
Assume that $\mathrm{Fix}(\alpha)$ is a subplane of Π. Then $\mathrm{Fix}(\alpha)$ has the same order as Π because the line L together with all of its points belongs to $\mathrm{Fix}(\alpha)$. But since the number of points of a projective plane is determined by its order, $\mathrm{Fix}(\alpha)$ has exactly as many points as Π, and because $\mathrm{Fix}(\alpha)$ is a subplane of Π we must have $\mathrm{Fix}(\alpha) = \Pi$. This means that α is the identity. Since $\alpha \neq 1$ is one of the prerequisites of theorem 3.2, $\mathrm{Fix}(\alpha)$ cannot be a subplane and the theorem is proved. □

Theorem 3.2 motivates the following definition.

Definition. Let α be a collineation fixing a point p linewise and a line L pointwise. Then α is called a (p, L)-*perspectivity*. The point p is called the *centre* of α and the line L is called the *axis* of α.
If p is on L, then α is called an *elation*, and if p is not on L, then α is called a *homology*.

It is immediate that the set of all (p, L)-perspectivities forms a group. The identity collineation is considered to be both an elation and a homology. We are interested in the cases where many (p, L)-perspectivities exist.

Definition. A projective plane Π is called (p, L)-*transitive* if the group of all (p, L)-perspectivities acts transitively on the non-fixed points of the lines through p (that is for any line M through p and a, b on M, $a, b \neq p$ and $a, b \notin L$, there exists a (p, L)-perspectivity sending a to b).
Furthermore, Π is called (L, L)-transitive for a line L if it is (p, L)-transitive for all p on L. In this case L is called a *translation line* of Π.

We are now ready to define translation planes.

Definition. A projective plane is called a *translation plane* if it has a translation line.
An affine plane is called a translation plane if it can be obtained by removing a translation line from a projective translation plane.

The term “translation plane“ comes from the effect that (p, L)-perspectivities have on the affine plane $\mathcal{A}$ obtained by removing the translation line L. Every point p of L stands for one parallel class of $\mathcal{A}$. A (p, L)-perspectivity leaves the lines of the parallel class corresponding to p invariant (as a set). Such collineations are translations in the usual geometric sense when viewed in the usual field planes. If $\mathcal{A}$ is a translation plane, then for every two points a and b there is a (p, L)-perspectivity mapping a to b (where p is the point of L that stands for the parallel class of the line ab). In other words the translations of $\mathcal{A}$ act transitively on its points.

3.4 Remark. Many authors mean an *affine* translation plane when using the word “translation plane“. We could also have gone this way by defining affine translation planes and then define projective translation planes based on that. Translations (apart from the identity) in affine planes are collineations that fix no point. They correspond to elations whose axis is the line at infinity. An affine plane is called a translation plane if it has a group of translations that acts transitively on its points. A projective translation plane can then be defined as the projective completion of an affine translation plane. Since we are mainly interested in projective planes, we did not choose this approach. Another reason is that the proof of theorem 3.7 that we give in this chapter uses projective planes and elations, not the underlying affine translation plane. However, the affine definition motivates the name “translation plane“ better and it is convenient to have both definitions. Sometimes one definition is better suited to a certain construction than the other.

Note that there is a slight asymmetry between the definitions for a projective and for an affine translation plane. While the projective completion of an affine translation plane is a projective translation plane, the residual affine plane of a projective translation plane is only a translation plane if a translation line is removed. Removing other lines generally does not yield a translation plane.
As a simple example, we show that the well-known affine planes $AG(2,F)$ for a skewfield F are translation planes.

3.5 Example. The planes $AG(2,F)$ are defined on the vector space F^2. For every element $v \in F^2$, the mapping

$$\tau_v : F^2 \to F^2,\ x \mapsto x + v$$

is a collineation and a translation by the definition of remark 3.4. This is what we would call a translation in the usual euclidean sense. For any two points $p, q \in F^2$, there exists a translation τ with $\tau(p) = q$, namely $\tau = \tau_{q-p}$. All these translation exist, so the group

$$T(V) = \{\tau_v \mid v \in F^2\}$$

is a group of translations that acts transitively on F^2. So $AG(2,F)$ is an affine translation plane. The desarguesian planes $PG(2,F)$ are thus projective translation planes as they are the projective completions of the affine translation planes $AG(2,F)$.

The main tools that we will use to prove theorem 3.1 are collineation groups and their actions. Thus, we will now take a closer look at sets of (p,L)-perspectivities.

Definition. Let Π be a projective plane and let $\Gamma \leq \mathrm{Aut}(\Pi)$ be a collineation group. For a point p and a line L of Π we define

$$\begin{aligned}\Gamma_{(p,L)} &\coloneqq \text{ The set of all } (p,L)\text{-perspectivities in } \Gamma,\\ \Gamma_{(L,L)} &\coloneqq \bigcup_{p\in L} \Gamma_{(p,L)}.\end{aligned}$$

3.6 Lemma. *Let* Π *be a projective plane and let* $\Gamma \leq Aut(\Pi)$ *be a collineation group. Then* $\Gamma_{(p,L)}$ *and* $\Gamma_{(L,L)}$ *are subgroups of* Γ *for every choice of a point* p *and a line* L *of* Π.

Proof. If $\alpha, \beta \in \Gamma$ are collineations fixing L pointwise and p linewise, then so do $\alpha\beta$ and α^{-1}. Thus, $\Gamma_{(p,L)}$ is a subgroup of Γ.
For $\Gamma_{(L,L)}$ we have to show that for $\alpha \in \Gamma_{(a,L)}$ and $\beta \in \Gamma_{(b,L)}$ with $a, b \in L$, $\alpha \neq \beta$, the collineation $\alpha^{-1}\beta$ is in $\Gamma_{(L,L)}$. Since α and β fix L, so does $\alpha^{-1}\beta$. Thus, by theorem 3.2 $\alpha^{-1}\beta$ has a unique centre and we need to show that this centre lies on L. Since we already know that $\Gamma_{(p,L)}$ is a group for any p and L, we can assume that $a \neq b$. In order to show that the centre of $\alpha^{-1}\beta$ lies on L, we can show that $\alpha^{-1}(\beta(x)) \neq x$ for all points $x \notin L$ (note that we have $\alpha^{-1}\beta \neq 1$ by assumption).
Let x be a point not on L and assume $\alpha^{-1}(\beta(x)) = x$. Then $\alpha(x) = \beta(x)$. Since a is the centre of α, the points a, x and $\alpha(x)$ are collinear. Similarly b, x and $\beta(x)$ are collinear. But since $\alpha(x) = \beta(x)$, this means that a and b both lie on the line $x\alpha(x)$. However, this cannot be the case as this would mean that the line $x\alpha(x)$ intersects L in two distinct points a and b. Since $x\alpha(x) \neq L$, this is impossible. Thus, we have $\alpha^{-1}\beta \in \Gamma_{(L,L)}$. The proof is visualised in figure 3.3. □

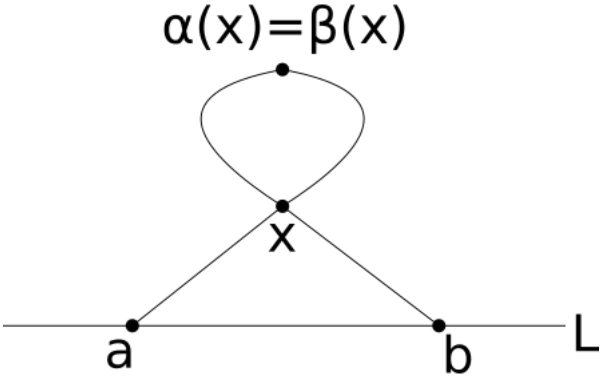


Figure 3.3: Proof of lemma 3.6

We can now state and prove the key result that we will use to prove the prime power conjecture for translation planes.

3.7 Theorem. *Let* Π *be a projective plane and* $\Gamma \leq Aut(\Pi)$ *be a collineation group. If* $\Gamma_{(a,L)}$ *is non-trivial for two distinct choices of points* a *on* L, *then* $\Gamma_{(L,L)}$ *is abelian and all its non-identity elements have the same order (either infinite or a prime).*

Proof. We first show that $\Gamma_{(L,L)}$ is abelian and start by showing that any two elations with axis L and distinct centres commute. Throughout the proof, we will pick non-trivial elations for two different points on L. This is possible by the prerequisites of the theorem and we will not state this every time we consider such collineations.
Let $\alpha \in \Gamma_{(a,L)}$ and $\beta \in \Gamma_{(b,L)}$ for $a, b \in L$, $a \neq b$, and $\alpha, \beta \neq 1$. Consider the collineation $\beta\alpha\beta^{-1}$. By lemma 3.6 it is an element of $\Gamma_{(L,L)}$, i.e. it is a (p, L)-perspectivity for some point $p \in L$. Since α fixes all lines throught a, $\beta\alpha\beta^{-1}$ fixes all lines through $\beta(a)$.

Thus, $\beta\alpha\beta^{-1}$ is a $(\beta(a), L)$-elation. But as a is on L, we have $\beta(a) = a$, so $\beta\alpha\beta^{-1}$ is an (a, L)-elation.
With similar reasoning, $\alpha^{-1}\beta^{-1}\alpha$ is a (b, L)-elation (note that β^{-1} is a (b, L)-elation since β is a (b, L)-elation).
Now consider the collineation $\alpha^{-1}\beta^{-1}\alpha\beta$. Writing

$$\alpha^{-1}\beta^{-1}\alpha\beta = \underbrace{\alpha^{-1}}_{\in\Gamma_{(a,L)}} \underbrace{(\beta^{-1}\alpha\beta)}_{\in\Gamma_{(a,L)}}$$

we see that $\alpha^{-1}\beta^{-1}\alpha\beta \in \Gamma_{(a,L)}$. Similarly, writing

$$\alpha^{-1}\beta^{-1}\alpha\beta = \underbrace{(\alpha^{-1}\beta^{-1}\alpha)}_{\in\Gamma_{(b,L)}} \underbrace{\beta}_{\in\Gamma_{(b,L)}}$$

wee see that $\alpha^{-1}\beta^{-1}\alpha\beta \in \Gamma_{(b,L)}$. Thus, we have $\alpha^{-1}\beta^{-1}\alpha\beta \in \Gamma_{(a,L)} \cap \Gamma_{(b,L)}$. But since we have $a \neq b$ and every elation has a unique centre (apart from the identity), we have $\Gamma_{(a,L)} \cap \Gamma_{(b,L)} = \{1\}$. Hence $\alpha^{-1}\beta^{-1}\alpha\beta = 1$, i.e. $\alpha\beta = \beta\alpha$.
Now we have to show that two elations with the same centre commute. Let $\alpha_1, \alpha_2 \in \Gamma_{(a,L)}$ for some $a \in L$ and $\beta \in \Gamma_{(b,L)}$ for some $b \in L$, $a \neq b$ and $\alpha_1, \alpha_2, \beta \neq 1$. Then by the argument above α_1 and α_2 commute with β. We claim that the centre of $\alpha_2\beta$ is different from the centre of α_1. If we show this, it follows that

$$\alpha_1\alpha_2\beta = \alpha_1(\alpha_2\beta) = (\alpha_2\beta)\alpha_1 = \alpha_2(\beta\alpha_1) = \alpha_2(\alpha_1\beta) = \alpha_2\alpha_1\beta$$

since we already know that elations with different centres commute. We obtain $\alpha_1\alpha_2\beta = \alpha_2\alpha_1\beta$ and cancelling β gives $\alpha_1\alpha_2 = \alpha_2\alpha_1$. Hence $\Gamma_{(L,L)}$ is abelian.
To complete the proof, we need to show that the centre of the elation $\alpha\beta$, where $\alpha \in \Gamma_{(a,L)}$, $\beta \in \Gamma_{(b,L)}$, $a \neq b$ and $\alpha, \beta \neq 1$, is different from a and b. First, consider a line M through b with $M \neq L$. Then β fixes M, so we have

$$\alpha(\beta(M)) = \alpha(M) \neq M$$

as α fixes exactly the lines through a and M does not go through a. So the centre of $\alpha\beta$ is not b.
Similarly, consider a line M through a with $M \neq L$. If we had $\alpha(\beta(M)) = M$, then we would have

$$\beta(M) = \alpha^{-1}(M) = M$$

since α fixes M. However, this cannot be the case as β fixes exactly the lines through b and M does not go through b. Thus, a cannot be the centre of $\alpha\beta$. This completes the proof that $\Gamma_{(L,L)}$ is abelian.
Now we prove the second part of the theorem that all non-identity elements of $\Gamma_{(L,L)}$ have the same order. We show that if $\Gamma_{(L,L)}$ has an element of finite order, then all non-identity elements must have this order. If $\Gamma_{(L,L)}$ has an element α of finite order, then it also has an element of prime order (which can be obtained by taking a suitable power of α). Let $\gamma \in \Gamma_{(c,L)}$ for some $c \in L$ be such an element of order p, p a prime.

Now consider any non-identity elation $\delta \in \Gamma_{(d,L)}$ with $c \neq d$. Then, as $\Gamma_{(L,L)}$ is abelian, we have

$$(\gamma\delta)^p = \gamma^p\delta^p \overset{\gamma^p=1}{=} \delta^p.$$

As we have seen before, the centre of the product $\gamma\delta$ is different from the centre of γ and δ since $c \neq d$. Call this centre e. Then we have $\gamma\delta \in \Gamma_{(e,L)}$ and thus $(\gamma\delta)^p \in \Gamma_{(e,L)}$, but we also have $\delta^p \in \Gamma_{(d,L)}$. Now since $d \neq e$, it follows that $\delta^p \in \Gamma_{(d,L)} \cap \Gamma_{(e,L)} = \{1\}$, i.e. $\delta^p = 1$. Since p is a prime and δ was not the identity, the order of δ is p.
We have now shown that any non-identity elation with centre $d \neq c$ has order p. The same argument with another point on L in place of c now shows that *every* non-identity element of $\Gamma_{(L,L)}$ has order p, which completes the proof. □

As we do not need the above theorem in its full generality, we record the result we need in a corollary.

3.8 Corollary. *Let Π be a translation plane with translation line L. Then the group $Aut(\Pi)_{(L,L)}$ of all elations with axis L is an abelian p-group.*

Proof. Since L is a translation line, there are certainly two points a and b on L such that non-trivial (a, L)- and (b, L)-elations exist (all points of L have this property). Using theorem 3.7 for $\Gamma = \mathrm{Aut}(\Pi)$, we obtain that all non-identity elements of $\mathrm{Aut}(\Pi)_{(L,L)}$ have order p. Thus, the order of $\mathrm{Aut}(\Pi)_{(L,L)}$ must be a prime power p^k (if there existed another prime q dividing the order, then by Cauchy's theorem there would also exist an element of order q in $\mathrm{Aut}(\Pi)_{(L,L)}$). □

Using this corollary, we can now give a short proof of theorem 3.1.

3.2 Proof of the main theorem and further results

We can now prove the main theorem of this chapter. We repeat the statement here.

3.1 Theorem. *Let Π be a translation plane of order n. Then n is a prime power.*

Proof. Let L be a translation line of Π. Consider any point $a \in L$ and the group $\Gamma :=$ $\mathrm{Aut}(\Pi)_{(a,L)}$ of all (a, L)-elations. By corollary 3.6 Γ is a subgroup of the group $\mathrm{Aut}(\Pi)_{(L,L)}$ which is a p-group by corollary 3.8. Thus, Γ is a p-group as well, i.e. its order is a prime power p^k.
Now consider any line $M \neq L$ through a. Then by definition of a translation plane, the group Γ acts transitively on the non-fixed points of M, i.e. all points of M except a. In fact, Γ acts sharply transitive on $M \setminus \{a\}$. In order to see that consider two points $b, c \in M$, $b, c \neq a$. Then there exists an elation $\gamma \in \Gamma$ such that $\gamma(b) = c$. Now let $\delta \in \Gamma$ be another elation with $\delta(b) = c$. Then $\gamma^{-1}\delta$ is an element of Γ that satisfies

$$\gamma^{-1}(\delta(b)) = \gamma^{-1}(c) = b,$$

i.e. $\gamma^{-1}\delta$ fixes b. But by lemma 3.2 an (a, L)-elation that is not the identity does not have any fixed points apart from the points of L. Thus, we have $\gamma^{-1}\delta = 1$, or in other

words $\gamma = \delta$. This shows that Γ acts sharply transitive on $M \setminus \{a\}$.
It is well-known that if a group G acts sharply transitive on a non-empty set X, then $|G| = |X|$ (choose any point $x \in X$, then the mapping $g \mapsto g(x)$ is a bijection from G to X). Applied to our setting, this means that $M \setminus \{a\}$ has exactly as many elements as Γ. Since the order of Γ is p^k, M has exactly $p^k + 1$ elements. By definition of the order of a projective plane, the order of Π is a prime power. □

In the proof of theorem 3.1, we only considered a single point on L and the lines through it. One could ask why we need a translation line at all and whether (a, L)-transitivity for a single point a on L is sufficient to obtain the result. But for theorem 3.7, which allowed us to conclude that $\mathrm{Aut}(\Pi)_{(L,L)}$ is a p-group, we needed that $\mathrm{Aut}(\Pi)_{(a,L)}$ is non-trivial for two distinct points a on L. Only (a, L)-transitivity for a single point a is not sufficient. If we have that $\mathrm{Aut}(\Pi)_{(a,L)}$ and $\mathrm{Aut}(\Pi)_{(b,L)}$ are non-trivial for two distinct points a, b on L, then we can conclude that $\mathrm{Aut}(\Pi)_{(L,L)}$ is a p-group (and thus $\mathrm{Aut}(\Pi)_{(a,L)}$ is a p-group as well). But if we do not have transitivity, then we cannot conclude that the order of a line of Π is the same as the order of $\mathrm{Aut}(\Pi)_{(a,L)}$. Trying to require "less" transitivity in a projective plane leads to *semi-translation planes* which we will define in the next chapter.

Many more things can be said about the structure of translation planes, far too much to be included in this thesis. We give some further results without proof. For proofs and related results, the reader is referred to the book "Projective Planes" by Hughes and Piper [28] and the "Handbook of Finite Translation Planes" by Johnson, Jha and Biliotti [29].

3.9 Remark. Let Π be a finite projective plane.

- If Π is (p, L)- and (q, L)-transitive for $p, q \in L$, $p \neq q$, then L is a translation line (Theorem 4.19 in [28]).
- If Π has two distinct translation lines, then every line of Π is a translation line (Theorem 6.18 in [28]). Such planes are called *Moufang planes.* Finite Moufang planes are pappian (and thus also desarguesian), so Moufang planes that are not desarguesian are infinite (see the corollary to theorem 6.20 in [28]).
- There are many different characterisations of translation planes. Some examples include:
    - Every translation plane gives rise to a *congruence partition* and every congruence partition gives rise to an affine translation plane (and thus a projective translation plane). There is a one-to-one correspondence between congruence partitions and translation planes. Similar to congruence partitions, there is a one-to-one correspondence between translation planes and *spreads*, which are essentially congruence partitions in a vector space. See chapter 7 in [28] and chapter 2 in [29] for more information about the relation between these structures.

  - Translation planes are exactly the class of projective planes that can be coordinatised by a *quasifield*. More information about coordinatisation can be found in chapter 5 of [28]. The relation between quasifields, spreads and translation planes is highlighted in chapter 5 of [29].

- All translation planes of order ≤ 49 are known, mostly by computer programs (section 96.1 in [29]).

- A translation plane of prime order is desarguesian (see excercise 7.14 in [28]).

- At the end of section 2.2, we stated that the order n of a projective plane with an abelian collineation group of order n^2 is a prime power. A translation plane Π with translation line L has $n+1$ points and for every point there are $n-1$ non-identity elations. Thus, since distinct centres yield distinct elations, $\text{Aut}(\Pi)_{(L,L)}$ has $(n+1)(n-1)+1 = n^2$ elements and is abelian by corollary 3.8. We see that every translation plane of order n has an abelian collineation group of order n^2, so this theorem can be viewed as a generalisation of theorem 3.1.

- If an affine plane $\mathcal{A}$ has a collineation group that acts transitively on the lines of $\mathcal{A}$, then $\mathcal{A}$ is a translation plane (Wagner 1965 [56]). Chapter 14 in [28] deals with Wagner's theorem and related results.

- If Π has a collineation group that acts *doubly* transitively on the points of Π, then Π is desarguesian (see theorem 14.13 in [28]). This result is known as the *Ostrom-Wagner theorem.*

We see that there are a lot of things to investigate regarding translation planes. However, for our purpose, which is the prime power conjecture, they can be considered "solved". Thus, we now turn to projective planes for which the prime power conjecture is still open, i.e. non-translation planes.

4 Non-translation planes

As we have shown that the prime power conjecture holds for translation planes, it can be argued that the difficulty of the prime power conjecture comes from non-translation planes. There are only a few non-translation planes known. This chapter aims to give an overview of the known non-translation planes. We will elaborate on theorem 105.7 from the book “Handbook of Finite Translation Planes“ from Johnson, Jha and Biliotti [29]. As this chapter is not meant to give an in-depth view into every of these classes of projective planes, there will be less proofs and more references to other works.

4.1 Theorem (Theorem 105.7 in [29])**.** *The known finite projective or affine planes that are not translation planes are included in the following list:*

- *Dual translation planes*
- *Semi-translation planes and their duals*
  (Derived dual translation planes and their duals)
- *Planar function planes of Coulter-Matthews*
- *Hughes planes and irregular Hughes planes*
- *Ostrom-Rosati planes and their duals*
  (Derived Hughes planes and their duals)
- *Figueroa planes*
- *The Mathon plane of order 16 and its dual*
- *The two Moorhouse planes of order 25 (derivates of each other)*

As the book was published in 2007, one should specify that these are the translation planes known at that time. Furthermore, it should be noted that the wording “included in the following list“ is important as not all dual translation planes are non-translation planes (take the self dual translation planes $PG(2, q)$ as an example). The same is true for semi-translation planes.

When working with projective planes, it can be helpful to think of translation planes with the *Lenz-Barlotti classification* in mind. This classification divides projective planes into certain classes depending on how many points p and lines L there are such that a given plane is (p, L)-transitive. It was first proposed by Lenz in 1954 [34] and later refined by Barlotti in 1957 [4]. A detailed explanation can be found in section 3.1 in the book by Dembowski [13] where the reader can also find references and explanations for all non-existence results known as of 1968 that are mentioned below without a citation. For a projective plane Lenz defined what we now call the *Lenz figure.* If Π is a projective plane, then its Lenz figure $L(\Pi)$ is defined as

$$L(\Pi) = \{(p, L) \in \mathcal{P} \times \mathcal{L} \mid p \in L \text{ and } \Pi \text{ is } (p, L)\text{-transitive}\}.$$

Lenz then gave seven classes with two of them divided into two subclasses. These were:

$$\begin{aligned}
\mathrm{I} &: L(\Pi) = \emptyset \\
\mathrm{II} &: L(\Pi) = \{(p, L)\} \text{ for a line } L \text{ and a point } p \\
\mathrm{III} &: L(\Pi) = \{(q, pq) \in \mathcal{P} \times \mathcal{L} \,|\, q \in L\} \text{ for a line } L \text{ and a point } p \notin L \\
\mathrm{IVa} &: L(\Pi) = L \times \{L\} \text{ for a line } L \\
\mathrm{IVb} &: L(\Pi) = \{p\} \times \{L \in \mathcal{L} \,|\, p \in L\} \text{ for a point } p \\
\mathrm{V} &: L(\Pi) = (L \times \{L\}) \cup (\{p\} \times \{M \in \mathcal{L} \,|\, p \in M\}) \text{ for a line } L \text{ and a point } p \in L \\
\mathrm{VIa} &: L(\Pi) = \{(p, M) \in \mathcal{P} \times \mathcal{L} \,|\, p \in L,\, M \in \mathcal{L}\} \text{ for a line } L \\
\mathrm{VIb} &: L(\Pi) = \{(q, L) \in \mathcal{P} \times \mathcal{L} \,|\, q \in \mathcal{P},\, p \in L\} \text{ for a point } p \\
\mathrm{VII} &: L(\Pi) = \{(p, L) \in \mathcal{P} \times \mathcal{L} \,|\, p \in L\}
\end{aligned}$$

Every projective plane belongs to exactly one Lenz class. The Lenz classes II to VIb are visualised in figure 4.1. We recreated the image that appears in Lenz's article [34]. Dots represent centres and lines represent axes. The dashed line is a line of the projective plane that is not an axis.

It has been shown that there are no projective planes (neither finite nor infinite) of classes VIa and VIb. The translation planes that we dealt with in the last chapter are exactly the projective planes of Lenz class IVa, V or VII. Class VII is the class of Moufang planes (see remark 3.9). Class IVa is the class of projective planes with a unique translation line and no other point-line transitivities. The class IVb is dual to class IVa, i.e. if a projective plane Π is in class IVa, then its dual is in class IVb and vice versa. Thus, class IVb is the class of the dual translation planes that were mentioned in theorem 4.1. If Π is a projective plane in class IVa, then its dual is a non-translation plane. This is one way of constructing non-translation planes. For some examples of projective planes of Lenz class IVa, the reader is referred to section 5.2 in Dembowski's book [13] which deals with projective planes of this type. A list of some translation planes such that their duals are non-translation planes appears in a different context in the article by Coulter and Matthews [10] which we will take a closer look at later.
The non-translation planes that we are interested in are the projective planes of Lenz class I, II and III and IVb. It turns out that it makes a huge difference whether a plane is finite or not. Hering and Kantor [25] showed that there are no finite projective planes of Lenz class III (but infinite projective planes of Lenz class III are known). As we are interested in finite projective planes this means that we “only“ have to deal with projective planes of Lenz class I, II and IVb (or equivalently IVa). However, the non-existence of (p, L)-perspectivities leads to a less symmetric structure which is harder to deal with. It should be noted that every Lenz class corresponds to an algebraic

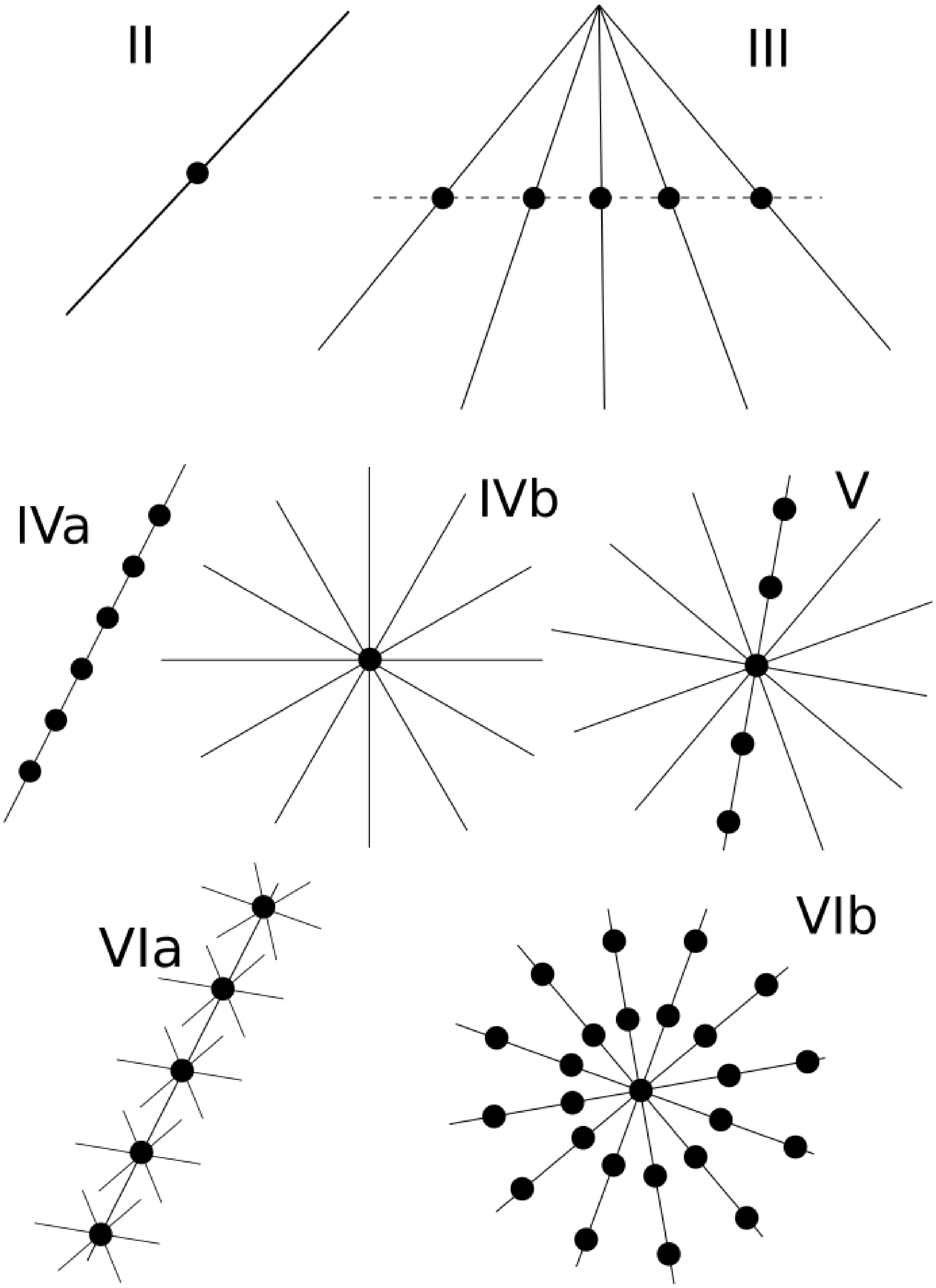


Figure 4.1: The Lenz classes

structure, i.e. the projective planes in a Lenz class are exactly the projective planes that can be coordinatised by a certain algebraic structure. However, since we do not concern ourselves with coordination in this thesis, we will not go into more detail here. See theorem 3.1.22 in [13] for more information.
Barlotti refined the Lenz classification by not only considering elations but also homologies. The Lenz-Barlotti figure is defined as

$$B(\Pi) = \{(p, L) \in \mathcal{P} \times \mathcal{L} \mid \Pi \text{ is } (p, L)\text{-transitive}\}.$$

This leads to more possibilities, and thus there are more Lenz-Barlotti classes than Lenz classes. Every Lenz class is divided into subclasses (apart from class V which does not split up further by switching from the Lenz figure to the Lenz-Barlotti figure). For example, a projective plane which is only (p, L)-transitive for a single point p and a single line L with $p \notin L$ is of the same Lenz class as a projective plane that is not (p, L)-transitive for any choice of p and L but not of the same Lenz-Barlotti class. Thus, the Lenz-Barlotti class gives more information about a projective plane than the Lenz class.
In his article from 1957 [4], Barlotti divided Lenz class I into eight subclasses (written as I.1, ..., I.8). Three of them (I.5, I.7, I.8) have been shown to be empty. Hering and Kantor showed that there are no finite projective planes of Lenz-Barlotti class I.6. However, it is not known whether there are infinite projective planes of class I.6. Barlotti divided Lenz class II into three subclasses, class II.3 was shown to be empty. A proof can also be found in the article by Hering and Kantor but the result was already known before (see the article by Spencer [51]). Class III is of no interest to us as there are no finite projective planes in this class, and class IVa (and thus class IVb) was divided into three subclasses. All of them contain finite projective planes. Thus, the Lenz-Barlotti classes that we need to deal with are I.1, I.2, I.3, I.4, II.1, II.2, IVb.1, IVb.2 and IVb.3. We now give the definitions for these classes. The points p, q, r are arbitrary but non-collinear.

$$\begin{aligned}
\text{I.1} &: B(\Pi) = \emptyset \\
\text{I.2} &: B(\Pi) = \{(p, qr)\} \\
\text{I.3} &: B(\Pi) = \{(p, qr), (q, rp)\} \\
\text{I.4} &: B(\Pi) = \{(p, qr), (q, rp), (r, pq)\} \\
\text{II.1} &: B(\Pi) = \{(p, pq)\} \\
\text{II.2} &: B(\Pi) = \{(p, pq), (q, pr)\} \\
\text{IVb.1} &: B(\Pi) = \{(x, pq) \mid x \in pq\} \\
\text{IVb.2} &: B(\Pi) = \{(x, pq) \mid x \in pq\} \cup \{(p, L) \mid q \in L\} \cup \{(q, M) \mid p \in M\} \\
\text{IVb.3} &: B(\Pi) = \{(x, L) \mid x \in pq, \alpha(x) \in L\} \\
&\qquad\qquad \text{for an involutory and fixed-point free collineation } \alpha : pq \to pq
\end{aligned}$$

We keep this classification in mind when describing the known non-translation planes.

Before we describe the mentioned classes of projective planes in theorem 4.1, we have to explain what a “derived“ plane is. Simply put, it is a method of constructing new planes from a given one. This is best motivated with a theorem about Baer subplanes. Recall that a Baer subset $\mathcal{B}$ is a substructure of a projective plane Π that touches every element of Π, i.e. every point of Π lies on a line of $\mathcal{B}$ and every line of Π goes through a point of $\mathcal{B}$. If $\mathcal{B}$ is a subplane, then it is called a Baer subplane. We need the following theorem:

4.2 Theorem (Theorem 3.8 in [28]). *Let Π be a finite projective plane of order n with a proper subplane Π_0 of order m. Then Π_0 is a Baer subplane if and only if $n = m^2$.*

The key idea of derivation is to take an affine plane $\mathcal{A}$ of order n^2 and consider its projective completion Π such that $\mathcal{A} = \Pi^L$ for some line L. The lines of $\mathcal{A}$ have n^2 elements. A Baer subplane $\mathcal{B}$ of Π has order n and thus n^2+n+1 points. If it contains exactly $n+1$ points of L, then n^2 points of $\mathcal{B}$ are points of $\mathcal{A}$. By taking some lines of $\mathcal{A}$ and some Baer subplanes of Π, we can construct a new affine plane of order n^2. This process is called derivation. However, before we formalise this process, we have to prove theorem 4.2. It follows easily from a theorem by Bruck that also has a connection to the prime power conjecture.

4.3 Theorem (Bruck, Theorem 3.7 in [28]). *Let Π be a finite projective plane of order n with a proper subplane Π_0 of order m. Then $n = m^2$ or $n \geq m^2 + m$.*

Proof. Consider a line L of Π_0. Since Π_0 has order m, the line L contains $m+1$ points of Π_0 and thus $n+1-(m+1) = n-m$ points of $\Pi \setminus \Pi_0$. Now those $n-m$ points are different for every line of Π_0 since any two lines of Π_0 intersect in a point of Π_0 . As Π_0 has exactly m^2+m+1 lines, this means that there are exactly $(m^2+m+1)(n-m)$ points in $\Pi \setminus \Pi_0$ that are incident with a line of Π_0. Together with the m^2+m+1 points of Π_0, this gives a lower bound on the points of Π. We obtain

$$\begin{array}{rrcl} & n^2+n+1 & \geq & (m^2+m+1)(n-m)+m^2+m+1 \qquad (*) \\ \iff & n^2+n+1 & \geq & m^2(n-m)+mn-m^2+n-m+m^2+m+1 \\ \iff & 0 & \geq & m^2(n-m)+mn-n^2 \\ \iff & 0 & \geq & (m^2-n)(n-m). \end{array}$$

Since Π_0 is a proper subplane, we have $n > m$, so it follows that $n \geq m^2$.
Note that if we have $n = m^2$, then equality holds in $(*)$. This means that the points of $\Pi \setminus \Pi_0$ that are incident with a line of Π_0 together with the points of Π_0 make up all points of Π. Every point of Π lies on a line of Π_0. The same proof for the dual planes Π^* and Π_0^* yields that this is also true for them, i.e. every point of Π^* lies on a line of Π_0^*. Thus, by duality every line of Π goes through a point of Π_0.
Now assume that $n \neq m^2$. Then there must exist a point p of Π not incident with any line of Π_0. It follows that no line through p can contain more than one point of Π_0 because otherwise the line would belong to Π_0. Furthermore, every point of Π_0 is on a line through p (otherwise there would exist two points in Π not joined by a line). Finally, no two lines through p can go through the same point of Π_0 since the lines joining two distinct points are unique. This means that there are at least as many lines through p as there are points in Π_0. This gives $n+1 \geq m^2+m+1$ or equivalently $n \geq m^2+m$. □

Since we saw in the proof above that we have $n = m^2$ if and only if Π_0 touches every element of Π, theorem 4.2 is now a direct corollary of this theorem. Furthermore, there are no projective planes known where the second case (i.e. $n \geq m^2 + m$) holds with equality. This suggests that the bound is not optimal. If there was a projective plane satisfying $n = m^2 + m$, then this plane would be a counterexample to the prime power conjecture as $m^2 + m = m(m + 1)$ is never a prime power (because we have $m > 1$).

Now we are ready to formalise the construction of a derived plane. Definitions and theorems about derivation that are not ascribed explicitly to an author are taken from chapter 10 of "Projective Planes" by Hughes and Piper [28].

Definition. Let $\mathcal{A}$ be an affine plane of order n^2 and let L be the line of its projective completion Π such that $\mathcal{A} = \Pi^L$. A set $\mathcal{S}$ of $n+1$ points of L is called a *derivation set* if for any two distinct points p, q of $\mathcal{A}$ such that the line pq meets L in $\mathcal{S}$ there exists a Baer subplane of Π containing p, q and $\mathcal{S}$.
If $\mathcal{A} = \Pi^L$ is an affine plane of order n^2 with derivation set $\mathcal{S}$, then we define the following incidence structure $\mathcal{D}_{\mathcal{S}}(\mathcal{A})$:
The points of $\mathcal{D}_{\mathcal{S}}(\mathcal{A})$ are the points of $\mathcal{A}$
The lines of $\mathcal{D}_{\mathcal{S}}(\mathcal{A})$ are all sets of the following two types:
1) The lines of $\mathcal{A}$ meeting L *not* in $\mathcal{S}$
2) The sets $\mathcal{B} \setminus L$ for every Baer subplane $\mathcal{B}$ of Π that contains $\mathcal{S}$

4.4 Theorem. *The incidence structure $\mathcal{D}_{\mathcal{S}}(\mathcal{A})$ is an affine plane of order n^2.*

Proof. Since $\mathcal{A}$ has order n^2, it has n^4 points. Every line of $\mathcal{D}_{\mathcal{S}}(\mathcal{A})$ has n^2 points because it is either a line of $\mathcal{A}$ (which has n^2 points) or the set of affine points of a Baer subplane $\mathcal{B}$ of Π that contains $\mathcal{S}$. As $\mathcal{B}$ is a projective plane of order n by theorem 4.2, it has $n^2 + n + 1$ points and every line has $n + 1$ points. Thus, if $\mathcal{B}$ contains the $n + 1$ points of $\mathcal{S}$, then these are exactly the points from L that are contained in $\mathcal{B}$. So $\mathcal{B} \setminus L$ has exactly n^2 points, and thus every line of $\mathcal{D}_{\mathcal{S}}(\mathcal{A})$ has exactly n^2 points.
It remains to show that any two distinct points p, q of $\mathcal{D}_{\mathcal{S}}(\mathcal{A})$ lie on a unique line. If the line pq does not intersect L in $\mathcal{S}$, then there is exactly one line in $\mathcal{D}_{\mathcal{S}}(\mathcal{A})$ containing p and q, namely the unique line of $\mathcal{A}$ joining p and q. A Baer subplane $\mathcal{B}$ containing $\mathcal{S}$ cannot contain both p and q as then the intersection of pq with L would have to belong to $\mathcal{B}$ too, which cannot be the case as it does not lie on L. Thus, there is a unique line of $\mathcal{D}_{\mathcal{S}}(\mathcal{A})$ joining p and q.
If the line pq intersects L in $\mathcal{S}$, then by definition of a derivation set there exists a Baer subplane in Π containing p, q and $\mathcal{S}$. We have to show that this Baer subplane is unique. Let $\mathcal{B}_1$ and $\mathcal{B}_2$ be Baer subplanes of Π containing p, q and $\mathcal{S}$. Let $\mathcal{C} = \mathcal{B}_1 \cap \mathcal{B}_2$ be the intersection of these two Baer subplanes. Then $\mathcal{C}$ contains p, q and the $n + 1$ points of $\mathcal{S}$. Since $n + 1 \geq 3$, there exist at least two points r and s that are not on the line pq. Then the points p, q, r, s form a quadrangle. Now $\mathcal{C}$ contains a quadrangle and is the intersection of two subplanes, so $\mathcal{C}$ is a subplane as well. As $\mathcal{C}$ contains the $n+1$ collinear points of $\mathcal{S}$ the order of $\mathcal{C}$ is n. But $\mathcal{B}_1$ and $\mathcal{B}_2$ are subplanes of order n as well and we have $\mathcal{C} \subseteq \mathcal{B}_1, \mathcal{B}_2$. It follows that $\mathcal{C} = \mathcal{B}_1 = \mathcal{B}_2$, i.e. the Baer subplane containing p, q and $\mathcal{S}$ is unique. Thus, $\mathcal{D}_{\mathcal{S}}(\mathcal{A})$ is a 2-$(n^4, n^2, 1)$ design, i.e. an affine plane of order n^2. □

One important fact about derivation is that multiple derivations with respect to the same derivation set $\mathcal{S}$ do not lead to new planes. However, derivation with respect to different derivation sets can lead to new planes which can make multiple derivation useful. We will see some examples later.

4.5 Theorem. *Let $\mathcal{A}$ be an affine plane with derivation set $\mathcal{S}$. Then $\mathcal{D}_{\mathcal{S}}(\mathcal{D}_{\mathcal{S}}(\mathcal{A}))$ is naturally isomorphic to $\mathcal{A}$.*

Proof. See theorem 10.4 in [28]. □

It should be noted that the order of the derived plane is the same as the order of the plane we started with. In other words, this construction cannot produce a counterexample to the prime power conjecture (in case such a counterexample exists). We have the following theorem regarding the derivation of translation planes.

4.6 Theorem. *Let $\mathcal{A}$ be a translation plane with a derivation set $\mathcal{S}$. Then $\mathcal{D}_{\mathcal{S}}(\mathcal{A})$ is a translation plane.*

Proof. See theorem 10.7 in [28]. □

Since we know by theorem 4.5 that $\mathcal{D}_{\mathcal{S}}(\mathcal{D}_{\mathcal{S}}(\mathcal{A}))$ is isomorphic to $\mathcal{A}$, theorem 4.6 implies that the derivation of a non-translation plane is also a non-translation plane.
In order to obtain a non-translation plane using derivation, we have to derive a non-translation plane. One option is to take the dual translation planes that we identified as non-translation planes before (i.e. Lenz class IVb). A list of admissible dual translation planes appears in the article by Coulter and Matthews [10] that we also mentioned earlier. However, derivation can be applied to many other projective planes. It can be shown that some of the known planes are derivates of each other, uncovering a connection between different classes of projective planes. Deriving dual planes was mentioned in theorem 4.1 in conjunction with *semi-translation planes* which we will take a look at now.

Semi-translation planes are - as the name suggests - projective planes that have a property similar to translation planes. As was stated in remark 3.9, we know that a line L of a projective plane Π is a translation line if Π is (p, L)-transitive for two different points $p \in L$. Thus, restricting ourselves to fewer points $p \in L$ where Π is (p, L)-transitive does not really work unless we restrict ourselves to a single point-line transitivity which is not what we want. Another possibility of loosening the requirements for a translation plane is to not require the group of all (p, L)-perspectivities to act transitively on the lines through p, but to require that there exist at least some non-trivial elations. This is the key idea behind semi-translation planes. They are a way of generalising translation planes. We already mentioned semi-translation planes in the discussion after the proof of theorem 3.1 where we examined its requirements.
As always, such a class of planes can be defined from the view of affine or projective geometry. We give the definition from the projective point of view due to Ostrom [46].

Definition. Let Π be a projective plane of order n^2 with $n > 2$ and L a line of Π. The plane Π is called a *semi-translation plane* with respect to the line L if there exists a set $\mathcal{M}$ of $n+1$ points on L such that if $p \in \mathcal{M}$, then Π has a group Γ of elations with centre p and axis L with $|\Gamma| = n$. If the group of all elations with axis L is of order n^2, then Π is called a *strict* semi-translation plane.

Note that in the case of a strict semi-translation plane the elations with centre in $\mathcal{M}$ are actually all elations of Π with axis L because every non-identity elation has a unique centre and there are $n-1$ non-identity elations in Γ per point. Thus, in total there are $(n+1)(n-1)+1 = n^2$ elation with axis L and centre in $\mathcal{M}$. So strict semi-translation planes are non-translation planes while semi-translation planes can be translation planes (since Γ could be a proper subgroup of the group of all (p, L)-perspectivities). We call a semi-translation plane *proper* if it is not a translation plane.

Although semi-translation planes are in general not translation planes, they lead to smaller translation planes in a natural way.

4.7 Theorem (Ostrom 1964)**.** *Let Π be a semi-translation plane with respect to the line L and points $\mathcal{M}$ on L. Suppose Γ is a group of elations with axis L such that $|\Gamma| = n^2$ and for each point $p \in \mathcal{M}$ the subgroup of Γ of elations with centre p has order n. Let $\mathcal{T}$ be an orbit under the action of Γ on points not on L. Then $\mathcal{T} \cup \mathcal{M}$ is a projective subplane of Π of order n.*

Proof. See lemma 1 in [46]. □

This theorem gives us a way of interpreting of semi-translation planes. In a translation plane Π of order n^2 with translation line L, the action of the group of all (p, L)-elations on the points not on L has only one orbit which is the set of all affine points of Π while in semi-translation planes the orbits are affine subplanes of order n, i.e. affine Baer subplanes. So although there are multiple orbits, they are as large as they can be since Baer subplanes are maximal proper subplanes of Π (see theorem 4.6 in [28]). This means semi-translation planes are non-translation planes that are as close to being translation planes as possible. Some authors define semi-translation planes as projective planes such that the orbits of the group of all (p, L)-elation are affine Baer subplanes.

A very important result about the construction of semi-translation planes is the following:

4.8 Theorem (Ostrom 1964)**.** *Let $\mathcal{A}$ be a derivable affine plane with derivation set $\mathcal{S}$ and L be a line of $\mathcal{A}$ that is not a line of $\mathcal{D}_{\mathcal{S}}(\mathcal{A})$ (i.e. L intersects the line at infinity in $\mathcal{S}$). If $\mathcal{A}$ has a group of translations that acts transitively on the points of L, then the projective completion of $\mathcal{D}_{\mathcal{S}}(\mathcal{A})$ is a semi-translation plane with respect to the line at infinity. Conversely, if $\mathcal{D}_{\mathcal{S}}(\mathcal{A})$ is a semi-translation plane, there exists such a line in $\mathcal{A}$.*

Proof. See section 3 in [46]. □

This theorem implies that we can use a derivable affine plane to construct semi-translation planes if its projective completion is (p, L)-transitive for the line at infinity L and a suitable point p on it (and these are exactly the planes such that their derivation is a semi-translation plane by the latter part of the theorem). Of course this is satisfied for a derivable translation plane, but then the semi-translation plane obtained is a translation plane as well and at the moment we are not interested in that. One way to obtain a non-translation plane is to start with a proper translation plane Π with translation line L (i.e. Lenz class IVa), consider the dual plane Π^* and then construct a residual affine plane $\mathcal{A} = (\Pi^*)^M$ from Π^* such that the removed line M contains, as a point L^*, the centre of the elations of Π^* (L is the common axis of the elations in Π so L^* is the common centre of the elations in Π^*). If L^* is in the derivation set $\mathcal{S}$, then we are in a situation where we can apply theorem 4.6 to obtain a non-translation plane. And of course we can dualise the obtained plane and - if it is not self dual - possibly obtain another non-translation plane.

Now we give some examples of derivable planes which we can use for the construction above. We have already mentioned the list of some admissible planes appearing in the article by Coulter and Matthews [10] multiple times. It can be also shown that the finite affine planes $AG(2,q^2)$ are derivable (see theorem 10.8 in [28]). In this way we can obtain the *André planes* and the *Hall planes* (see theorem 10.12 and the following corollary in [28]). These are two classes of projective planes that were found by André (see [1]) and Hall (see [22]), respectively, using coordinate methods. We see that some classes of projective planes can be viewed as derivations of other well-known planes (here $AG(2,q^2)$) showing how ubiquitous derivation is. Furthermore, it gives us a different way to approach them.
Finally, we mention that there also exists “general derivation“. It is essentially a similar construction using coordinatisation of affine planes of order q^2. If the coordinatizing structure has certain properties, then the affine plane is derivable, giving a rich class of affine planes to apply derivation to. For some cases it is also easy to say when the derived plane is a translation plane and when not. See section 4 in chapter 10 of [28] for more information.

We have now explained the two “general“ constructions of non-translation planes of theorem 4.1 and now turn to the classes of non-translation planes named after their discoverers. The first on the list are the planes obtained from planar functions by Coulter and Matthews.

The Coulter-Matthews planes from planar functions were introduced by Coulter and Matthews in 1997 [10], building on results about planar functions which were defined by Dembowski and Ostrom in 1968 [15]. Dembowski and Ostrom considered projective planes Π of order n with a collineation group Γ of order n^2 such that the action of the permutation group induced by Γ on any point or line orbit is regular, or equivalently: if Γ fixes an element x (either a point or a line), then Γ fixes the whole orbit of x. This is for example the case if Γ is abelian. Dembowski showed earlier [14] that in this case there exists a flag (p, L) that is fixed by every collineation in Γ such that Π is (p, L)-transitive and Γ contains the group of all (p, L)-elations (which has order n). There are now two possible cases:

(1) Γ consists entirely of elations (with either common axis L or common centre p by

the above). Then Π is a translation plane or a dual translation plane.

(2) The elations in Γ are precisely those of Π. Then the action of Γ on the points (as well as on the lines) has three orbits.

While the structure of the projective planes in case (1) is known, it is not clear whether the projective planes in case (2) are transitive for other flags than the flag (p, L) or not. Dembowski and Ostrom essentially introduced planar functions to deal with the second case. At the time of publication of their article, all known examples in case (2) were translation planes.
We now define planar functions and their associated planes.

Definition (Dembowski & Ostrom [15])**.** Let G and H be finite groups of order n, written additively and not necessarily commutative. A function $f : G \to H$ is called *planar* if the functions λ_u and μ_u for $u \in G$, $u \neq 0$, defined by

$$\begin{aligned}\lambda_u(x) &= f(u + x) - f(x)\\ \mu_u(x) &= -f(x) + f(x + u)\end{aligned}$$

are bijections for every $u \neq 0$.
Given two groups G, H and a function $f : G \to H$, define an incidence strucure $I(G, H; f)$ as follows.

- The set of points is the set $G \times H$
- The set of lines is the set of all symbols $L(g, h)$ for $g \in G, h \in H$ and all symbols $L(g)$ for $g \in G$
- The incidence relation is defined by

$$\begin{aligned}(x, y)\ I\ L(g, h) &\iff y = f(x - g) + h\\ (x, y)\ I\ L(g) &\iff x = g\end{aligned}$$

Dembowski and Ostrom then proved the following result:

4.9 Theorem (Dembowski & Ostrom [15], Lemma 12)**.** *A function $f : G \to H$ is a planar function if and only if $I(G, H; f)$ is an affine plane.*

A simple example is the function $f : \mathbb{F}_q \to \mathbb{F}_q$ for odd q with $f(x) = x^2$. This function is planar and the affine plane $I(\mathbb{F}_q, \mathbb{F}_q; f)$ is isomorphic to the affine plane $AG(2, q)$.
Dembowski and Ostrom then showed that all projective planes in case (2) with some further restrictions are exactly the projective planes such that the residual affine plane Π^L (recall that L is an axis such that Π is (p, L)-transitive) is of the form $I(G, H; f)$, i.e. it comes from a planar function between some groups G and H (see theorem 5 in [15]). Furthermore, they found a necessary and sufficient criterion for f such that $I(G, H; f)$ is a translation plane (see corollary 4 in [15]). They also noted that all planar functions known at the time come from a certain class of polynomials and asked the question

whether every planar function is representable that way.
Coulter and Matthews denied that. They defined a class of planar functions (now called Coulter-Matthews functions) that are not Dembowski-Ostrom polynomials (i.e. planar functions of the form discussed in the article by Dembowski and Ostrom). It can be shown that every function $f : \mathbb{F}_q \to \mathbb{F}_q$ must be the evaluation map of some polynomial over $\mathbb{F}_q$. The planar functions of Coulter and Matthews are thus given in the form of polynomials.

4.10 Theorem (Coulter & Matthews [10], Theorem 4.1)**.** *Let $e \in \mathbb{N}$, $q = 3^e$ and $\alpha \in \mathbb{N}$. Then the polynomial $x^{(3^\alpha+1)/2}$ is planar over $\mathbb{F}_q$ if and only if $gcd(\alpha, e) = 1$ and α is odd.*

The polynomials of the form $x^{p^\alpha+1}$ were already known to be planar in certain cases by Dembowski and Ostrom (albeit their theorem on exactly when these polynomials are planar was not entirely correct). But the polynomials in theorem 4.10 were not studied by them. We can now state the result that we are interested in.

4.11 Theorem (Coulter & Matthews [10], Theorem 6.2)**.** *Let $f(x) = x^{(3^\alpha+1)/2}$ be a planar polynomial over $\mathbb{F}_q$ with $q = 3^e$ and suppose that $\alpha \neq \pm 1 \ mod\ 2e$. Then the affine plane $I(\mathbb{F}_q, \mathbb{F}_q; f)$ is not a translation plane.*

Coulter and Matthews also showed that the projective completion Π of the affine plane constructed above is not a dual translation plane. Thus, Π is not in Lenz class IVa or IVb. Since there are no finite projective planes of Lenz class III and since we know that planes constructed from planar functions are (p, L)-transitive for at least a single choice of a point p on a line L, it follows that Π is of Lenz class II. The projective planes constructed by Coulter and Matthews have order 3^e and the planes with odd e were the first known projective planes of Lenz-Barlotti class II whose order is not a square. This also implies that these planes cannot be constructed from other planes using derivation because we can only derive planes whose order is a square. It is interesting to note that the planes by Coulter and Matthews have a collineation group that acts transitively on the points of the plane but not all Coulter-Matthews planes are translation planes. More information about Coulter-Matthews planes like when they are isomorphic and how they can be coordinatised can be found in the article by Coulter and Matthews [10].

We now turn to the next class of non-translation planes on our list, the *Hughes planes*. The Hughes planes were defined by Hughes in 1957 [27]. Their construction relies on nearfields which we will define now. The following description of Hughes planes is based on section 6 from chapter 9 of the book by Hughes and Piper [28].

Definition. A *(left-)nearfield* is a set N together with two binary operations $+$ and $\cdot$ satisfying the following axioms:

1) $(N, +)$ is an abelian group.

2) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in N$.

3) There is an element $1 \in N$ such that $1 \cdot a = a \cdot 1 = a$ for all $a \in N$.

4) For every $a \in N$, $a \neq 0$, there exists an element $a^{-1} \in N$ such that $aa^{-1} = a^{-1}a = 1$.

5) $a \cdot (b + c) = a \cdot c + b \cdot c$ for all $a, b, c \in N$.

The *centre* of N is the set $\{z \in N \mid zn = nz \text{ for all } n \in N\}$.

It should be noted that if we replace axioms 2), 3) and 4) by the axiom "$(N \setminus \{0\}, \cdot)$ is a group", then there exists an exceptional nearfield in which the multiplication is defined by $x \cdot y = x$ for all $x, y \in N$. The difference is that axiom 3) requires the element 1 to be neutral for all elements of N while the axiom "$(N \setminus \{0\}, \cdot)$ is a group" only requires the element 1 to be neutral for all non-zero elements of N. As we do not want to deal with this exceptional structure, we use the axioms 2), 3) and 4).
To construct the Hughes planes $\mathcal{H}$, we need nearfields with p^{2n} elements for an odd prime p and a positive integer n whose centre is a field with p^n elements (i.e. isomorphic to $\mathbb{F}_{p^n}$). Such nearfields exist for any choice of p and n (see lemma 9.6 in [28]). Now let N be such a nearfield and set $V = N^3$ and $q = p^n$. The case $q = 9$ is somewhat exceptional because the nearfield of order 9 has some additional properties and sometimes needs to be treated separately. However, the same construction applies.
We essentially want to view V as a 3-dimensional vector space over N, but this is in general not possible as we do not have distributivity from the right. However, it helps to think of V that way. Define addition in V by $(x_1, x_2, x_3)+(y_1, y_2, y_3) = (x_1+y_1, x_2+y_2, x_3+y_3)$ and scalar multiplication from the left with elements of N by $k \cdot (x_1, x_2, x_3) = (kx_1, kx_2, kx_3)$. The point set of $\mathcal{H}$ is essentially the set $V \setminus \{(0, 0, 0)\}$, but we make the identification $(x_1, x_2, x_3) = (kx_1, kx_2, kx_3)$ for all non-zero elements $k \in N$. If (x_1, x_2, x_3) is a non-zero element of V, we denote the corresponding point of $\mathcal{H}$ as $\langle x \rangle$.
Although V is not a vector space over N, we can define the action of linear maps in the usual way if we restrict ourselves to (3×3)-matrices whose elements all come from the centre F of N. Let $A = (a_{ij}) \in GL(3, q)$ be an invertible (3×3)-matrix with entries from F, then we define the function $\alpha : V \to V$ by

$$\alpha(x_1, x_2, x_3) = (a_{11}x_1 + a_{12}x_2 + a_{13}x_3, a_{21}x_1 + a_{22}x_2 + a_{23}x_3, a_{31}x_1 + a_{32}x_2 + a_{33}x_3).$$

This is just the usual definition of the matrix-vector product and we will denote this suggestively as $\alpha(x) = Ax$. Note that since the entries of A belong to the centre F of N, we have

$$\alpha(k \cdot x) = A(k \cdot x) = k \cdot Ax,$$

i.e. every bijective linear map $A \in GL(3, q)$ induces a well-defined permutation on the points $\langle x \rangle$ of $\mathcal{H}$. The lines of $\mathcal{H}$ are defined by starting with some sets of points and then taking all of their images under a suitable linear map A and all of its powers A^m for non-zero integers m. First, note that for any element $t \in N$ and $x \in V$ we have

$$x_1 + x_2t + x_3 = 0 \iff kx_1 + (kx_2)t + kx_3 = 0$$

for all non-zero k in N. Thus, the set of all $x \in V$ such that $x_1 + x_2t + x_3 = 0$ consists of the point $(0, 0, 0)$ and a set of points $\langle x \rangle$ of $\mathcal{H}$. This set of points of $\mathcal{H}$ is denoted as $L(t)$.

The sets $L(t)$ for $t = 1$ and $t \in N \setminus F$ are our “base“ lines.
Now we need to find a suitable linear map $A \in GL(3, q)$. In order to construct a projective plane, we need exactly as many lines as there are points. We already know the set of points, it is the set $V \setminus \{(0, 0, 0)\}$ in which we identify some elements with each other. There are q^2 elements in N, so there are $q^6 - 1$ non-zero elements in V. Every point of $\mathcal{H}$ is a set of $q^2 - 1$ points and any such sets are disjoint. Thus, we know that $\mathcal{H}$ has exactly

$$\frac{q^6 - 1}{q^2 - 1} = q^4 + q^2 + 1$$

points. Furthermore, we have defined $q^2 - q + 1$ “base“ lines $L(t)$. So if we want a linear map A such that we can take the images of these lines under all of its powers, then $\mathcal{A}$ needs to have order

$$\frac{q^4 + q^2 + 1}{q^2 - q + 1} = q^2 + q + 1.$$

In fact, since the points of $\mathcal{H}$ are not simply elements of V but we associate all scalar multiples of a non-zero element x with each other, it suffices that A^{q^2+q+1} is a scalar multiple of the identity matrix (but not necessarily the identity matrix itself) and no smaller power (greater than 0) of A has this property. So $q^2 + q + 1$ is not necessarily the order of A, but $\mathcal{A}$ has order $q^2 + q + 1$ when viewed as a permutation of the points of $\mathcal{H}$.
It is known that such a matrix A exists in $GL(3, q)$. This is due to Singer [50]. Singer proved that the projective plane $PG(2, q)$ always has a collineation α of order $q^2 + q + 1$, i.e. if we start with an arbitrary point x and consider the points $x, \alpha(x), \alpha(\alpha(x)), \ldots$ then we will hit each point exactly once before coming back to the point x that we started with. Since the points of $PG(2, q)$ are 1-dimensional subspaces of $\mathbb{F}_q^3$ (see example 2.3) this collineation α corresponds to a matrix $A \in GL(3, q)$ such that A^{q^2+q+1} is a multiple of the identity matrix while no smaller power has this property, i.e. exactly what we need. Now using this matrix A, we are ready to define the lines of $\mathcal{H}$.
The set of lines of $\mathcal{H}$ consists of all sets

$$L(t)A^m = \{\langle A^m x\rangle \mid \langle x\rangle \in L(t)\}$$

for $0 \leq m \leq q^2 + q$ and either $t = 1$ or $t \in N \setminus F$.

4.12 Theorem. *If $\mathcal{H}$ is the set of points and lines as defined above with incidence given by set theoretic inclusion, then $\mathcal{H}$ is a finite projective plane of order q^2.*

Proof. See theorem 9.14 in [28]. □

4.13 Theorem. *A Hughes plane is not (p, L)-transitive for any choice of point p and line L and is thus neither a translation nor a dual translation plane.*

Proof. See corollary 2 to theorem 9.18 in [28]. □

This means that Hughes planes are of Lenz-Barlotti class I.1. Hughes planes are self dual and the full collineation group has exactly two point orbits and exactly two line

orbits (see theorem 5.4.1 in [13]).
The list in Theorem 4.1 also mentions “irregular“ Hughes planes. These come from the fact that there are exceptional nearfields. All finite nearfields have been classified by Zassenhaus, see Satz 17 in his article [59] for a complete list. Although the exceptional nearfields of orders 5^2 and 7^2 cannot be used directly for the construction of a Hughes plane, they have a property which enables a different construction due to Ostrom. He constructed an associated affine versions of the Hughes planes which can be used to obtain Hughes planes from the exceptional nearfields of order 5^2 and 7^2. Johnson, Jha and Biliotti call these the *irregular* Hughes planes in their “Handbook of Finite Translation Planes“ (see section 100.1 in [29]). They are also called *exceptional* Hughes planes. Note that these Hughes planes should not be confused with the regular Hughes planes from the usual nearfields of order 5^2 and 7^2. Finally, we mention that there also exist “generalised Hughes planes“. Sometimes the terms “Hughes planes“ and “generalised Hughes planes“ are also used interchangeably. The generalised Hughes planes come essentially from the exceptional nearfields that Hughes did not deal with. See the article by Lüneburg [36] for their construction and more information.

We have seen that Hughes planes have order q^2 for a prime power q. Thus, judging solely from the order, they are a candidate for derivation. And indeed it was shown that Hughes planes are derivable. Ostrom used his affine version of the Hughes planes and applied derivation to construct a new class of projective planes [45]. These planes were discovered indepently by Rosati [48] who also determined the full collineation group of the generalised Hughes planes earlier. Thus, they are now called the *Ostrom-Rosati-planes*. The Ostrom-Rosati planes were the first known finite projective planes of Lenz-Barlotti class II.1. See theorems 5.4.4 and 5.4.5 in [13] for more information.

Next on our list are the *Figueroa planes*. These planes were constructed by Figueroa [20] by studying the action of the group $PSL(3, q)$ on the projective plane $PG(2, q^3)$ and replacing some of the orbits. Figueroa's original construction only worked for prime powers q with $q \not\equiv 1 \; mod \; 3$ and $q > 2$. Later Hering and Schaeffer [24] and Grundhöfer [21] noticed that the restriction on q can be dropped and every projective plane $PG(2, q^3)$ can be used to construct a Figueroa plane. Here, we give the synthetic construction from the article by Grundhöfer.
Let $\Pi = (\mathcal{P}, \mathcal{L})$ be a finite projective plane and let $\alpha \in \mathrm{Aut}(\Pi)$ be a collineation of order 3. If p is a point of Π, there are three possibilities:

1) p is fixed by α.

2) p is not fixed by α and the points p, $\alpha(p)$ and $\alpha^2(p)$ are collinear.

3) p is not fixed by α and the points p, $\alpha(p)$ and $\alpha^2(p)$ are not collinear.

Similarly, there are three possibilities for a line L of Π, which are dual to the three cases above:

1) L is fixed by α.

2) L is not fixed by α and the lines L, $\alpha(L)$ and $\alpha^2(L)$ are concurrent.

3) L is not fixed by α and the lines L, $\alpha(L)$ and $\alpha^2(L)$ are not concurrent.

Thus, the point set $\mathcal{P}$ can be decomposed into three subsets $\mathcal{P}_1$, $\mathcal{P}_2$ and $\mathcal{P}_3$ corresponding to the above three cases. Similarly, we obtain a partition of the line set $\mathcal{L}$ into three subsets $\mathcal{L}_1$, $\mathcal{L}_2$ and $\mathcal{L}_3$. Now we can define an involution μ that interchanges the sets $\mathcal{P}_3$ and $\mathcal{L}_3$ by

$$\mu(p) = \alpha(p)\alpha^2(p) \;\text{ and }\; \mu(L) = \alpha(L) \cap \alpha^2(L)$$

for $p \in \mathcal{P}_3$ and $L \in \mathcal{L}_3$. The functions μ maps points to lines and vice versa. Since the images of $\mu(p)$ under α and α^2 are the lines $\alpha^2(p)p$ and $p\alpha(p)$, respectively, it follows immediately that $\mu(p) \in \mathcal{L}_3$ for $p \in \mathcal{P}_3$. Similarly, we have $\mu(L) \in \mathcal{P}_3$ for $L \in \mathcal{L}_3$. To show that μ is an involution, let $p \in \mathcal{P}_3$ and consider

$$\mu(\mu(p)) = \mu\left(\alpha(p)\alpha^2(p)\right) = \alpha\left(\alpha(p)\alpha^2(p)\right) \cap \alpha^2\left(\alpha(p)\alpha^2(p)\right) = \left(\alpha^2(p)p\right) \cap (p\alpha(p)) = p.$$

Similarly, it follows that $\mu(\mu(L)) = L$ for every $L \in \mathcal{L}_3$. So μ is bijective and swaps the roles of the points and lines of $\mathcal{P}_3$ and $\mathcal{L}_3$. The effect of μ is visualised in figure 4.2. We can now give the definition of a Figueroa plane.

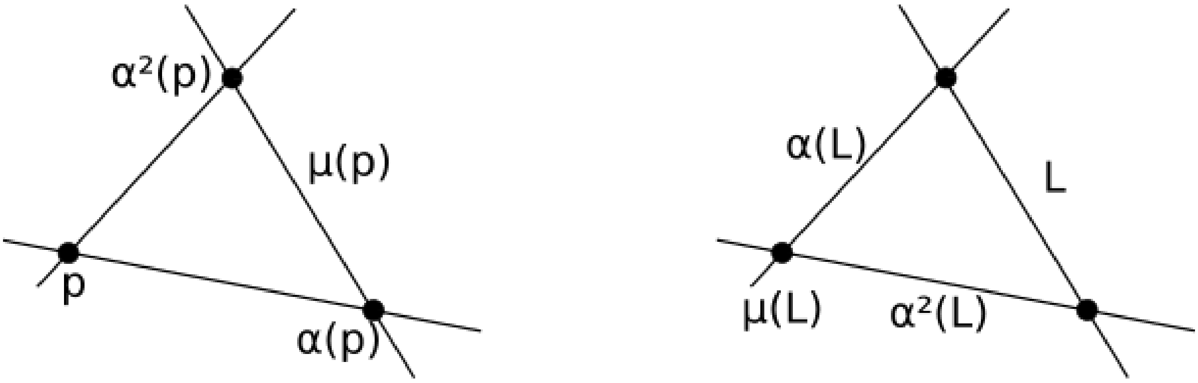


Figure 4.2: The involution μ

Definition. Let $\Pi = (\mathcal{P}, \mathcal{L}, \mathcal{I})$ be a projective plane (with $\mathcal{I} = \in$ in our usual setting) and α be a collineation of Π of order 3. Define the sets $\mathcal{P}_i$ and $\mathcal{L}_i$ for $i = 1, 2, 3$ as above and denote with $\mathcal{I}_{33}$ the incidence relation $\mathcal{I}_{33} = \mathcal{I} \cap (\mathcal{P}_3 \times \mathcal{L}_3)$ that defines the incidence between the points of $\mathcal{P}_3$ and the lines of $\mathcal{L}_3$. We define a new incidence structure $\Pi_\alpha := (\mathcal{P}, \mathcal{L}, \mathcal{I}^*)$ with

$$\mathcal{I}^* := (\mathcal{I} \setminus I_{33}) \cup \delta\left(\mu(\mathcal{I}_{33})\right)$$

where $\delta(L, p) = (p, L)$ for all $p \in \mathcal{P}$ and $L \in \mathcal{L}$. In other words: The incidence structure Π_α has the same incidence relation as Π, only the incidence between points of $\mathcal{P}_3$ and lines of $\mathcal{L}_3$ is redefined by

$$p \, \mathcal{I}^* L \iff \mu(L) \, \mathcal{I} \, \mu(p)$$

for all $p \in \mathcal{P}_3$ and $L \in \mathcal{L}_3$.

The incidence structure Π_α is not always a projective plane. This depends on the structure of the projective plane Π that we started with and on the collineation α. As a first step we have:

4.14 Theorem. *Let Π be a pappian projective plane that admits a collineation of order 3. Then Π_α is a projective plane.*

Proof. See theorem 1 in [21]. □

But even if we restrict ourselves to the projective planes $\Pi = PG(2, q)$, the structure Π_α is not always a Figueroa plane. What is missing is a property of the collineation α that we will define now.

Definition. Let Π be a projective plane and $\alpha \in Aut(\Pi)$ be a collineation. Then α is called *planar* if the structure $\mathrm{Fix}(\alpha)$ of fixed points and fixed lines is a subplane of Π.

The reason for introducing this term is the following theorem.

4.15 Theorem. *Let Π be a pappian projective plane with a collineation α of order 3. If α is not planar, then Π_α is isomorphic to Π.*

Proof. See Theorem 3 in [21]. □

Thus, we need planar collineations to construct new projective planes. We have to exclude one last special case: The projective plane $PG(2, 8)$ admits a planar collineation of order 3, but the resulting plane $PG(2, 8)_\alpha$ is isomorphic to $PG(2, 8)$. Thus, we have to exclude it. Now we can state the main result.

4.16 Theorem. *Let Π be a pappian projective plane of order greater than 8 with a planar collineation α of order 3. Then Π_α is not desarguesian.*

Proof. See theorem 2 in [21]. □

The projective planes constructed in this way are called the Figueroa planes. We can construct infinite Figueroa planes by starting with an infinite pappian plane but for our purposes we will focus on the finite Figueroa planes.
A finite Figueroa plane can be constructed from every projective plane $PG(2, q^3)$. The points of $PG(2, q^3)$ are 1-dimensional subspaces of $\mathbb{F}_{q^3}$. Consider the map $\alpha : \mathbb{F}_{q^3} \to \mathbb{F}_{q^3}$ defined by

$$\alpha(x, y, z) = (x^q, y^q, z^q).$$

Since $q = p^k$ (for some prime p and positive integer k) is a power of the characteristic of $\mathbb{F}_{q^3}$, this is a linear map and thus a collineation. Furthermore, we have

$$\alpha^3(x, y, z) = (x^{q^3}, y^{q^3}, z^{q^3}) = (x, y, z),$$

so α has order 3. It can be shown that α is planar, so this collineation gives rise to a Figueroa plane. The fact that the Figueroa planes are not translation planes can be seen from the structure of their collineation group. The full collineation group is known both in the finite and in the infinite case. See section 4 in [21] for more information.

The second to last entry in our list of non-translation planes is the Mathon plane (and its dual). It was constructed by Rudolf Mathon and presented at the conference “Finite Geometries and Combinatorics“ in Deinze in 1992 [37]. There is surprisingly little information available on the Mathon plane. The article by Mathon that some authors refer to seems to never actually have appeared and in the book by Beutelspacher about the conference of 1992 which features chapters about 35 of the 52 talks there is no chapter about the talk by Mathon. Furthermore, Gordon Royle’s website about projective planes of order 16, that is also often cited, is not available any more. However, a list of all lines and generators of the full collineation group of the Mathon plane and its dual can be found on the website by Moorhouse about projective planes of order 16 [41]. We have checked using SageMath that this list of lines indeed forms a projective plane. Furthermore, in the article by Moorhouse about projective planes of order less than 32 [40], which we will take a closer look at in chapter 7, Moorhouse states that the Mathon plane was constructed using “net replacement“, so we give a little introduction into this technique. The following results are taken from an article by Ostrom [47].

Definition. A *net* is an incidence structure $N = (\mathcal{P}, \mathcal{L})$ where the lines occur in classes called “parallel classes“ such that the following holds:

(1) Each point belongs to exactly one line of each parallel class.

(2) If $L_1, L_2 \in \mathcal{L}$ are lines from different parallel classes, then L_1 and L_2 intersect in a unique point.

(3) There are at least three parallel classes and every line contains at least two points.

Nets with only one or two parallel classes are called *trivial.*
For every net N there exists a positive integer n such that

(1) Each line contains exactly n points.

(2) Each parallel class consists of exactly n lines.

(3) There are exactly n^2 points in total.

The integer n is called the *order* of the net.

We immediately see that affine planes are nets of order $n+1$ and a net can for example be obtained by deleting some parallel classes from an affine plane. There are further terms and properties of nets that one could analyse, but we only need the following definition.

Definition. A net N is called *replacable* if there exists a net N' defined on the same points such that every two points lie on a common line in N if and only if they lie on a common line in N'. The net N' is called a *replacement* of N.

Now we can define the procedure of *net replacement.* It is contained in the following theorem.

4.17 Theorem. *Let $\Pi = N_1 \cup \ldots N_k \cup M$ be an affine plane such that $N_1, \ldots, N_k$ are replaceable nets while M may or may not be replaceable. Let N_i' be a replacement for N_i for every $i = 1, \ldots, k$. Then $\Pi' = N_1' \cup \ldots N_k' \cup M$ is an affine plane*

Proof. See theorem 3.4 in [47]. □

Net replacement is similar to derivation that we defined earlier and in fact it is easily seen that derivation is a special case of net replacement. If $\mathcal{A}$ is an affine plane with line at infinity L, then all lines of a parallel class intersect L in the same point. The union of all parallel classes whose point at infinity is in the derivation set is a net. This net is then replaced with the affine residuals of all Baer subplanes that contain the derivation set. As we have seen in theorem 4.4, any two such affine residuals intersect in either zero points or in one point. Thus, the maximal sets of pairwise disjoint affine Baer subplanes form a parallel class and their union is a net. So net replacement is a generalisation of derivation. For more information on net replacement the reader is referred to the article by Ostrom [47].

Finally, we come to the last finite non-translation planes of theorem 4.1. These are the two Moorhouse planes. Called “Wyoming planes“ by Moorhouse, they were constructed by a method called “lifting quotients“ which we will explain now.
If we have a projective plane Π and a collineation α of Π of order two, then we can build a new incidence structure $\Sigma = \Pi/\alpha$ where the points and lines are the orbits of length two under α, i.e. sets $\{p, \alpha(p)\}$ and $\{L, \alpha(L)\}$, respectively. It can be shown that the plane Π can be recovered from the orbits of length two only, so we can disregard the fixed points and lines. Incidence in Σ is defined naturally: the point $\{p, \alpha(p)\}$ lies on $\{L, \alpha(L)\}$ if and only if $p \in L$ or $p \in \alpha(L)$. Now since Π is a projective plane, the incidence structure Σ has some certain special properties, and we call a structure with these properties a *semibiplane.* See the article by Moorhouse about semibiplanes [43] for more information.
The method of lifting quotients now tries to reverse the construction above: given a semibiplane Σ, can we find a projective plane Π with a collineation α of order two such that Π/α is isomorphic to Σ?
Moorhouse gives a list of known projective planes that can be obtained by lifting quotients. The two Moorhouse planes are the first planes obtained by this method that were not known before. They are of Lenz-Barlotti class II.1 and I.1 and thus not translation planes. For the algorithm, the computer programs used and further information see section 3 in the article by Moorhouse [40].

We have now described all known classes of finite non-translation planes. The order of all of these planes is a prime power. However, this is mainly due to the fact that most of these planes are constructed from other known ones without changing the order. Since the order of all known finite projective planes is a prime power, the order of the constructed planes is a prime power as well. In fact, from the list of theorem 4.1, only the planar function planes and the Hughes planes are not constructed as the modification of an existing plane. All other projective planes mentioned in theorem 4.1 are constructed by starting with a known projective plane and altering the incidence relation (derivation, net replacement) or by trying to make a known structure bigger (lifting).

After all these results about the existence of certain projective planes, we now turn to a well-known non-existence result - the Bruck-Ryser-Chowla theorem.

5 The Bruck-Ryser-Chowla theorem

In this chapter we will state and prove the Bruck-Ryser-Chowla theorem. It gives necessary conditions for the existence of a symmetric 2-(v, k, λ) design. The Bruck-Ryser-Chowla theorem is a generalisation of the Bruck-Ryser theorem, which we will obtain as a corollary. We can use it to exclude possible orders of finite projective planes.

5.1 Theorem (Chowla & Ryser [9])**.** *Suppose a symmetric* 2-(v, k, λ) *design exists. Then the following holds:*

(1) If v is even, then $k - \lambda$ is a square in $\mathbb{N}$.

(2) If v is odd, then the equation

$$x^2 = ny^2 + (-1)^{\frac{v-1}{2}} \lambda z^2$$

has an integer solution $(x, y, z) \neq (0, 0, 0)$.

This theorem is called the Bruck-Ryser-Chowla theorem. To prove it, we need the following well-known results. They are taken from the book “Topics in Number Theory Volume 1“ by LeVeque [35].

5.2 Lemma (Lagrange's 4-square theorem)**.** *Every positive integer is the sum of at most four integer squares.*

Proof. See theorem 7-9 in [35]. □

The following result is sometimes called “Euler's 4-square theorem“ and can easily be verified by straightforward algebraic manipulations.

5.3 Lemma. *Let $a, b, c, d, x_1, x_2, x_3, x_4$ be integers. Then we have*

$$\begin{aligned} & (a^2 + b^2 + c^2 + d^2)(x_1^2 + x_2^2 + x_3^2 + x_4^2) \\ = \; & (ax_1 + bx_2 + cx_3 + dx_4)^2 + (-bx_1 + ax_2 - dx_3 + cx_4)^2 \\ + \; & (-cx_1 + dx_2 + ax_3 - bx_4)^2 + (-dx_1 - cx_2 + bx_3 + ax_4)^2. \end{aligned}$$

A product of two sums of four squares is thus again a sum of four squares. Furthermore, if we call the sums in the brackets on the right hand side y_1, y_2, y_3, y_4, then they are given bilinearly in terms of a, b, c, d and x_1, x_2, x_3, x_4 by

$$\begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix} = \begin{pmatrix} a & b & c & d \\ -b & a & -d & c \\ -c & d & a & -b \\ -d & -c & b & a \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}.$$

Now we are ready to prove the Bruck-Ryser-Chowla theorem.

Proof of Theorem 5.1. We essentially give the proof that Ryser and Chowla gave in their original article [9].
(1): By lemma 1.7b, any incidence matrix A of D satisfies

$$(det(A))^2 = det(AA^T) = rkn^{v-1} = k^2(k-\lambda)^{v-1}.$$

Since the left side is an integer square and v is even, $n = k - \lambda$ is an integer square.
(2): Let $x \in \mathbb{Q}^n$ and A be an incidence matrix of D. The idea of this proof is to interpret A as a quadratic form and then make the resulting sum of squares smaller to obtain the desired equation.
By lemma 1.7a we have the identity

$$xAA^Tx^T = x(nI + \lambda J)x^T = nxx^T + \lambda xJx^T.$$

Let $z = xA$ to obtain

$$zz^T = nxx^T + \lambda xJx^T.$$

This gives us the identity

$$z_1^2 + \ldots + z_v^2 = n(x_1^2 + \ldots + x_v^2) + \lambda s^2 \tag{$*$}$$

for some number $s = x_1 + \ldots + x_k \in \mathbb{Q}$.
First, we want to eliminate the factor n as much as possible. By lemma 5.2 n is a sum of four integer squares. Write

$$n = a^2 + b^2 + c^2 + d^2,$$

then $n(x_1^2 + x_2^2 + x_3^2 + x_4^2) = (a^2 + b^2 + c^2 + d^2)(x_1^2 + x_2^2 + x_3^2 + x_4^2)$ is again a sum of four squares by lemma 5.3. This lemma also gives us the matrix

$$S = \begin{pmatrix} a & b & c & d \\ -b & a & -d & c \\ -c & d & a & -b \\ -d & -c & b & a \end{pmatrix},$$

which satisfies

$$SS^T = (a^2 + b^2 + c^2 + d^2)I_4 = nI_4.$$

Thus, we have

$$xSS^Tx^T = n(x_1^2 + x_2^2 + x_3^2 + x_4^2).$$

Case 1: $v \equiv 1 \; mod \; 4$
Group the sum $nx_1^2 + \ldots + nx_v^2$ in equation $(*)$ into sums of four squares with x_v^2 left over and use the above result for each group. More explicitly, set

$$T = \begin{pmatrix} S & 0 & \ldots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & S & 0 \\ 0 & \ldots & 0 & 1 \end{pmatrix}$$

and set $y = xT$ to obtain

$$y_1^2 + \ldots + y_v^2 = yy^T = xTT^Tx^T = nx_1^2 + \ldots + nx_{v-1}^2 + x_v^2.$$

Plugging this into equation $(*)$ leaves us with (note that $x_v = y_v$)

$$z_1^2 + \ldots + z_v^2 = y_1^2 + \ldots + y_{v-1}^2 + ny_v^2 + \lambda s^2 \tag{$**$}$$

for some (possibly different) number s, and z given in terms of y because we have $z = xA = y(T^{-1}A)$.

We now want to reduce the sum. This is done by picking a value for y_1 such that $y_1^2 = z_1^2$, then picking a value for y_2 such that $y_2^2 = z_2^2$ and so on. We will later refer to this step as *Bruck-Ryser-Chowla elimination*.

We have $z = yC$ for some rational matrix $C = T^{-1}A$, or more explicitly for the first coordinate

$$z_1 = c_{11}y_1 + \ldots + c_{v1}y_v.$$

We want $y_1^2 = z_1^2$, so we need $y_1 = \pm z_1$. If $c_{11} \neq 1$, we can achieve $y_1 = z_1$ by considering

$$y_1 = z_1 = c_{11}y_1 + \ldots + c_{v1}y_v \iff y_1 = \frac{1}{1 - c_{11}}(c_{21}y_2 + \ldots + c_{v1}y_v).$$

If $c_{11} = 1$, we can achieve $y_1 = -z_1$ by considering

$$-y_1 = z_1 = c_{11}y_1 + \ldots + c_{v1}y_v \iff y_1 = \frac{1}{-1 - c_{11}}(c_{21}y_2 + \ldots + c_{v1}y_v).$$

Thus, we can always pick a value for y_1 depending on $y_2, \ldots, y_v$ such that $y_1 = \pm z_1$. Substituting a suitable value for y_1 in equation $(**)$ leaves us with the equation

$$z_2^2 + \ldots + z_v^2 = y_2^2 + \ldots + y_{v-1}^2 + ny_v^2 + \lambda s^2,$$

where y_1 does not show up anymore. The number s now depends on $y_2, \ldots, y_v$. But the exact value does not matter to us, so we will keep denoting it with s.

Since y_1 was chosen linearly depending on $y_2, \ldots, y_v$, the values $z_2, \ldots, z_v$ are now given as rational linear combinations of $y_2, \ldots, y_v$. This means that we can now iterate the process, i.e. we can choose a value for y_2 depending linearly on $y_3, \ldots, y_v$ such that $y_2^2 = z_2^2$, and thus obtain an equation where neither y_1 nor y_2 shows up. We can do this elimination as long as there exist at least two values y_k not chosen yet. Thus, the last step is picking y_{v-1} as a rational multiple of y_v such that $y_{v-1}^2 = z_{v-1}^2$. After the last elimination we are left with the equation

$$z_v^2 = ny_v^2 + \lambda s^2.$$

Now let y_v be any non-zero rational number. Then the value of y_{v-1} is fixed as it was chosen as a multiple of y_v. Now the value of y_{v-2} is fixed as it was chosen as a rational combination of y_{v-1} and y_v. Continuing this way we obtain values for every y_k and based on that values for the z_k and for s such that equation $(**)$ holds. This means that there also exists a rational solution to the equation

$$z_v^2 = ny_v^2 + \lambda s^2$$

with $y_v \neq 0$. By renaming the variables and multiplying with a suitable integer, we obtain that the equation

$$x^2 = ny^2 + \lambda z^2$$

has an integer solution with $(x, y, z) \neq (0, 0, 0)$. Since we assumed $v \equiv 1$ *mod* 4, this is exactly the desired equation.

Case 2: $v \equiv 3$ *mod* 4

Let x_{v+1} denote a new variable and add nx_{v+1}^2 to both sides of equation $(*)$ to obtain

$$z_1^2 + \ldots + z_v^2 + nx_{v+1}^2 = n(x_1^2 + \ldots + x_{v+1}^2) + \lambda s^2. \qquad (***)$$

Now we can proceed like we did in case 1. Group the sum $nx_1^2 + \ldots + nx_{v+1}^2$ into sums of four squares. This time there is no variable left over. Consider the matrix

$$T = \begin{pmatrix} S & 0 & \ldots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \ldots & 0 & S \end{pmatrix}$$

and set $y = xT$ to obtain

$$y_1^2 + \ldots + y_{v+1}^2 = nx_1^2 + \ldots + nx_{v+1}^2.$$

Plugging this into equation $(***)$ leaves us with

$$z_1^2 + \ldots + z_v^2 + nx_{v+1}^2 = y_1^2 + \ldots + y_{v+1}^2 + \lambda s^2.$$

Now we can use Bruck-Ryser-Chowla elimination again. Note that the appearance of the new variable x_{v+1} in this equation does not the change the fact that all variables on the left side of the equation are linear combinations of the y_k. The elimination leaves us with the equation

$$nx_{v+1}^2 = y_{v+1}^2 + \lambda s^2.$$

This time, by renaming the variables and multiplying with a suitable integer, we obtain that the equation

$$x^2 = ny^2 - \lambda z^2$$

has an integer solution with $(x, y, z) \neq (0, 0, 0)$. Since this is the desired equation in the case $v \equiv 3$ *mod* 4, this completes the proof. □

We can now obtain the Bruck-Ryser theorem as a corollary of the Bruck-Ryser-Chowla theorem. Before that we give two lemmas that will be needed in the proof, again taken from the book by LeVeque [35].

5.4 Lemma. *Let p be a prime number. Then -1 is a square modulo p if and only if $p = 2$ or $p \equiv 1 \; mod \; 4$.*

Proof. See theorem 5-3 in [35]. □

5.5 Lemma. *Let $n \in \mathbb{N}$ be an integer. Then n is a sum of two squares if and only if the square-free part of n has no prime divisors $p \equiv 3 \; mod \; 4$.*

Proof. See theorem 7-3 in [35]. □

5.6 Theorem (Bruck & Ryser [8])**.** *If there exists a projective plane of order n and $n \equiv 1 \; mod \; 4$ or $n \equiv 2 \; mod \; 4$, then n is a sum of two squares in $\mathbb{N}$.*

Proof. We essentially give the proof that Ryser and Chowla gave in their article in which they proved the Bruck-Ryser-Chowla theorem [9].
A finite projective plane is a 2-$(n^2+n+1, n+1, 1)$ design. If $n \equiv 1 \; mod \; 4$ or $n \equiv 2 \; mod \; 4$, then $v \equiv 3 \; mod \; 4$. We obtain from the Bruck-Ryser-Chowla theorem that there exist $x, y, z \in \mathbb{Z}$ not all zero with

$$x^2 = ny^2 - z^2.$$

Let p be a prime dividing the square-free part of n (if no such p exists, then n is a square and so it is also a sum of two squares). Then the above equation can be rewritten as

$$x^2 = pty^2 - z^2 \tag{$*$}$$

with $t \in \mathbb{N}$ not divisible by p (and possibly different y). Note that z cannot be zero (otherwise n is a square or $x = y = z = 0$). Without loss of generality we can assume that neither x nor z are divisible by p. If one of them is divisible by p, the other has to be too, because we have $x^2 \equiv z^2 \; mod \; p$. But then pty^2 has to be divisible by p^2, and because t is not divisible by p, y must be divisible by p. Thus, we can divide x, y and z by p until we get a solution with p not dividing x and z. Reducing equation $(*)$ modulo p gives

$$x^2 \equiv -z^2 \iff (xz^{-1})^2 \equiv -1,$$

so -1 is a square modulo p. By lemma 5.4, we have $p = 2$ or $p \equiv 1 \; mod \; 4$. In other words, the square-free part of n cannot have a prime divisor equal to $3 \; mod \; 4$. By lemma 5.5 n is the sum of two integer squares. □

The smallest numbers ruled out by the Bruck-Ryser theorem are 6, 14, 21, 22 and 30. For a list of ruled out values see entry A046712 in the On-Line Encyclopedia of Integer Sequences [44].
The smallest values for which this theorem applies but cannot rule out the existence of a projective plane are 10 and 12. As it was shown that there exists no finite projective plane of order 10, the Bruck-Ryser-Chowla theorem gives necessary but not sufficient conditions for the existence of a finite projective plane.
The Bruck-Ryser-Chowla theorem can be applied to symmetric designs with $\lambda > 1$ for which the Bruck-Ryser theorem does not help us. As an example we take a look at the Hadamard designs.

5.7 Example. The Hadamard designs are symmetric 2-$(4n-1, 2n-1, n-1)$ designs of order n. Using the Bruck-Ryser-Chowla theorem we obtain that the equation

$$x^2 = ny^2 - (n-1)z^2$$

has a non-trivial integer solution. Since $x = y = z = 1$ is a solution for any n, the Bruck-Ryser-Chowla theorem does not help us with the existence of Hadamard designs.

We also give an example where the Bruck-Ryser-Chowla theorem yields strong results. It is taken from the book “Einführung in die endliche Geometrie I“ by Beutelspacher [5].

5.8 Example. There are no projective planes of order $n \equiv 6 \ mod \ 8$.
This is because $n \equiv 6 \ mod \ 8$ implies $n \equiv 2 \ mod \ 4$, and thus by the Bruck-Ryser theorem n would have to be the sum of two squares. However, the squares modulo 8 are 0, 1 and 4 and the sum of two of those values is never 6. So there cannot be a projective plane of order $n \equiv 6 \ mod \ 8$.

We close this chapter by giving a different formulation of the Bruck-Ryser-Chowla theorem which is usually easier to apply in practice. The following is taken from chapter 2 of the book “Symmetric Designs“ by Lander [33].
The equations coming from the Bruck-Ryser-Chowla theorem are of the form

$$x^2 = ay^2 + bz^2,$$

and we want to know whether they are solvable for given integers a and b. We consider the slightly more general equation

$$ax^2 + by^2 + cz^2 = 0 \tag{$*$}$$

for given integers a, b, c and we are looking for a non-zero integer solution. Without loss of generality we can assume that a, b and c are square-free. If one of the coefficients, say a, can be written as $a = \widetilde{a}s^2$ for some integer $s \neq 0, \pm 1$, then we have

$$ax^2 + by^2 + cz^2 = \widetilde{a}(sx)^2 + by^2 + cz^2,$$

so we can also consider the equation

$$\widetilde{a}x^2 + by^2 + cz^2 = 0.$$

This equation has a non-zero solution if and only if equation $(*)$ has a non-zero solution because the solutions only differ by a factor of s in the first component.
We can also assume that a, b and c are pairwise relatively prime. If two coefficients, say a and b, had a common prime factor p, then the summand cz^2 must be divisible by p as well. If c is divisible by p, we can divide the whole equation by p. If z^2 is divisible by p, it is also divisible by p^2 and we can equivalently consider the equation

$$\frac{a}{p}x^2 + \frac{b}{p}y^2 + pcz^2 = 0.$$

We can iterate this process for every common factor until all coefficients are pairwise relatively prime.

Now we argue exactly like in the proof of the Bruck-Ryser theorem. If p is an odd prime dividing one of the coefficients, say a, then we can reduce the equation modulo p to obtain

$$by^2 + cz^2 = 0 \; mod \, p \quad \Longleftrightarrow \quad by^2 = -cz^2.$$

Since b and c are not divisible by p by assumption, it follows that $-bc$ is a square modulo p.

We can do the same for prime factors of b and c, so we also obtain that $-ac$ is a square modulo p for every odd prime p dividing b, and $-ab$ is a square modulo p for every odd prime p dividing c. Note that we do not have to consider the factor 2 because at most one of the coefficients is divisible by 2 (as the coefficients are relatively prime) and reducing the equation modulo 2 just gives either $x^2 + y^2 = 0$ or $x^2 + y^2 + z^2 = 0$, both of which are always solvable modulo 2. So reducing the equation modulo 2 gives us no restrictions on the coefficients. Finally, if all coefficients are positive or all coefficients are negative, there cannot exist a non-trivial integer solution. So the four conditions

(1) If an odd prime p divides a, then $-bc$ is a square modulo p.

(2) If an odd prime p divides b, then $-ac$ is a square modulo p.

(3) If an odd prime p divides c, then $-ab$ is a square modulo p.

(4) Not all coefficients have the same sign.

are necessary for the existence of a non-zero solution to the equation $(*)$. The important result now is a theorem by Legendre. These four conditions are not only *necessary* but also *sufficient* for the existence of a non-trivial integer solution. We will refer to this as *Legendre's theorem.* Using this insight we can give an alternative version of the Bruck-Ryser-Chowla theorem.

5.9 Theorem. *Suppose a symmetric 2-(v, k, λ) design exists. Let n^* and λ^* denote the square-free part of $n = k - \lambda$ and λ, respectively. Then the following hold for every odd prime p:*

(1) If $p \nmid n^*$ and $p \mid \lambda^*$, then n is a square modulo p.

(2) If $p \mid n^*$ and $p \nmid \lambda^*$, then $(-1)^{\frac{v-1}{2}}\lambda^*$ is a square modulo p.

(3) If $p \mid n^*$ and $p \mid \lambda^*$, then $(-1)^{\frac{v+1}{2}} \cdot (\lambda^*/p) \cdot (n^*/p)$ is a square modulo p.

Proof. The equation obtained from the Bruck-Ryser-Chowla theorem is

$$x^2 = ny^2 + (-1)^{\frac{v-1}{2}}\lambda z^2 \quad \Longleftrightarrow \quad -x^2 + ny^2 + (-1)^{\frac{v-1}{2}}\lambda z^2 = 0.$$

It is clear that not all coefficients have the same sign. (1) and (2) follow directly from Legendre's theorem (we have $a = -1$, $b = n^*$ and $c = (-1)^{\frac{v-1}{2}}\lambda^*$).
If $p \mid n^*$ and $p \mid \lambda^*$, then we rewrite the equation as shown before to

$$-px^2 + \frac{n^*}{p}y^2 + \frac{(-1)^{\frac{v-1}{2}}\lambda^*}{p}z^2 = 0.$$

Now we can apply Legendre's theorem to obtain that

$$-\frac{n^*}{p} \cdot \frac{(-1)^{\frac{v-1}{2}}\lambda^*}{p} = (-1)^{\frac{v+1}{2}} \cdot \frac{n^*}{p} \cdot \frac{\lambda^*}{p}$$

is a square modulo p. □

Using this theorem we can give a short proof of the Bruck-Ryser theorem: If Π is a projective plane of order n with $n \equiv 1 \ mod\ 4$ or $n \equiv 2 \ mod\ 4$, we have $v \equiv 3 \ mod\ 4$, $\lambda^* = 1$ and for every prime p dividing n^*, -1 is a square modulo p. From lemmas 5.4 and 5.5 it follows that n must be a sum of two squares.
We will make extensive use of this theorem in the next chapter to quickly determine which equations obtained from the Bruck-Ryser-Chowla theorem are solvable and which are not.

6 An approach using bordered matrices

In 2017 Mingchun Xu wrote an article [58] in which he proposed a generalisation of the Bruck-Ryser-Chowla theorem, but his proof was incorrect. In this chapter we describe his approach, give a counterexample to his theorem, explain where his proof fails and assess whether the approach can be altered to yield correct results. It appears that Xu is aware of his mistake as he wrote in a later article from 2019 [57] that the question whether there exists a finite projective plane of order 12 is still not solved, although he claimed to have solved this problem in his article from 2017.
Recall that by lemma 1.7 every incidence matrix A of a 2-(v, k, λ) design satisfies

$$AA^T = (r - \lambda)I_v + \lambda J_v.$$

6.1 Rectangular bordered matrices

The key idea of Xu's article from 2017 was the following: Assume a symmetric 2-(v, k, λ) design exists and take any incidence matrix A of it. Add some rows and columns to A to obtain a rectangular matrix $C \in \mathbb{Q}^{w \times w+d}$ for some integer $d \geq 1$ with

$$CC^T = aI_w + bJ_w$$

for positive integers a and b. Xu tried to show that there are certain restrictions on a and b depending on w and d. If they are not met, then the assumption that a 2-(v, k, λ) design exists must be false.

Definition. Let A be an incidence matrix of a symmetric design. If C is a $(w \times w + d)$-matrix ($d \geq 1$) obtained by adding rational rows and columns to A such that

$$CC^T = aI_w + bJ_w$$

for some positive integers a and b, then C is called a *(rectangular) bordered matrix* of A.

6.1 Remark. A matrix C in the situation above must necessarily be of rank w, i.e. full rank.

Xu dealt with the cases $d = 1$ and $d = 2$ and distinguished between $w \equiv 0, 1, 2, 3$ *mod* 4, giving 8 cases in total. As the attempted proofs for each case are all built (and thus fail) in the same way, we only state the claim for the case $d = 1$ and $w \equiv 0$ *mod* 4 and then give a counterexample.

6.2 Claim. *Let C be a rational $(w \times w+1)$-matrix with no constant column and*

$$CC^T = aI_w + bJ_w$$

for some positive integers a and b. If $w \equiv 0$ mod 4, then b is a square.

6.3 Counterxample. Consider a 2-$(3,2,1)$ design. A possible incidence matrix is given by

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

We now build the following (4×5) bordered matrix:

$$C = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 1/4 & 1/4 & 1/4 & 3/2 & 3/4 \end{pmatrix}$$

This matrix satisfies

$$CC^T = I_8 + 2J_8,$$

but 2 is not a square. Claim 6.2 does thus not hold.

Xu's proof attempt for claim 6.2 relies on the Bruck-Ryser-Chowla elimination (see theorem 5.1). However, Xu applied this in a situation where the needed conditions are not met. More explicitly, the equation obtained by using the Bruck-Ryser-Chowla approach for the matrix C from the above counterexample is

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 + y_5^2 = x_1^2 + x_2^2 + x_3^2 + x_4^2 + 2z^2 \tag{$*$}$$

with $(x_1, x_2, x_3, x_4) \in \mathbb{Q}^4$, $y = xC$ and $z = x_1 + x_2 + x_3 + x_4$. Using Bruck-Ryser-Chowla elimination this can be reduced to

$$y_4^2 + y_5^2 = x_4^2 + 2\tilde{z}^2.$$

In this situation the same elimination procedure cannot be applied because there is only one variable left. We cannot pick a value for x_4 in terms of the remaining variables as there are none. Picking $x_4 = 0$ yields only the trivial solution $x = (0,0,0,0)$, $y = (0,0,0,0,0)$ and $z = 0$.
Xu's solution to that problem was not to pick values for the x_i but to pick values for the y_i. As C is of full rank, the linear map $L : x \mapsto xC$ is an isomorphism onto its image. If we restrict the equation $(*)$ to values $y \in im(L)$, we could pick values for the y_i and do a similar elimination because the x_i are given as rational linear combinations of the y_i. But this does not solve the problem. We would arrive at the same equation as by using the usual elimination and would (in general) be unable to pick a value for the remaining variables. However, Xu reduced the equation one more time to obtain his desired result. This was the flaw in his proof.

In our example above we cannot choose y_4 in terms of y_5 such that we have $y_4^2 = x_4^2$ and $(y_1, y_2, y_3, y_4, y_5) \in im(C)$ because we are restricted in two ways: We need to pick y_4 in terms of y_5 such that $(y_1, y_2, y_3, y_4, y_5) \in im(C)$, but we also need to pick y_4 in terms of y_5 such that $y_4 = \pm x_4$. These two restrictions might be fulfillable simultaneously, but in general they are not. Note that any four columns of C are linearly independent, so any choice for four of the variables leads to exactly one value for the remaining variable such that $(y_1, y_2, y_3, y_4, y_5) \in im(L)$. If that was not the case, we would be even more restricted in our choice of the values. Furthermore, note that the equation obtained if we could achieve $y_4^2 = x_4^2$ has no non-trivial integer solution (as 2 is not a square), while the equation $(*)$ has a solution with $x_4 \neq 0$ (for example $x_4 = 1, \tilde{z} = 2, y_4 = 3, y_5 = 0$).

6.2 Square bordered matrices

The problem with the approach using rectangular bordered matrices was that the Bruck-Ryser-Chowla theorem only deals with square matrices and does not generalise to rectangular matrices. However, one could try to find a square bordered matrix and then use the Bruck-Ryser-Chowla theorem on it. Xu proposed this in his article from 2019 [57]. In this section we investigate this approach.

Definition. Let A be an incidence matrix of a symmetric design. If C is a rational $(w \times w)$-matrix obtained by adding rational rows and columns to A such that

$$CC^T = aI_w + bJ_w$$

for some positive integers a and b, then C is called a *(square) bordered matrix* of A.

When working with bordered matrices, one needs to be very careful because some theorems that hold for incidence matrices of symmetric designs do not hold any more for bordered matrices. In particular, the first part of the Bruck-Ryser-Chowla theorem, i.e. that n is a square if v is even, is in general false if v, k and λ are only defined by a rational $(v \times v)$-matrix A with $AA^T = (k - \lambda)I_v + \lambda J_v$, but A is not the incidence matrix of a design. This is because the crucial step in the proof of lemma 1.7 about the determinant of an incidence matrix, i.e.

$$det(AA^T) = \Big(r + \lambda(v-1)\Big)(r-\lambda)^{v-1} = rkn^{v-1},$$

relies upon the fact that we have $\lambda(v-1) = r(k-1)$ for 2-designs. Otherwise we cannot deduce that we have

$$det(A)^2 = k^2 n^{v-1}$$

for symmetric designs, which we need so that n must be a square for even v. Thus, we cannot use the first part of the Bruck-Ryser-Chowla theorem for bordered matrices. The following example illustrates the problem:

6.4 Example. Consider the symmetric 2-$(7, 3, 1)$ design. An incidence matrix can easily obtained by taking all cyclic permutations of the vector $(1, 0, 1, 1, 0, 0, 0)$ as the columns of a matrix. We add one column and one row to obtain the following bordered matrix:

$$C = \left(\begin{array}{ccccccc|c} 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 \end{array}\right)$$

We have $CC^T = 2I_8 + 2J_8$, which would mean (if this was the incidence matrix of a design) that $r = 4$, $\lambda = 2$ and $n = r - \lambda = 2$, so n is not a square. But since C is not a 0/1-matrix, C is not an incidence matrix of a symmetric design, so this is not a contradiction to the Bruck-Ryser-Chowla theorem.
We have $det(CC^T) = 2304$. The first formula of lemma 1.7, i.e.

$$det(AA^T) = (r + \lambda(v - 1))(r - \lambda)^{v-1},$$

is still correct for bordered matrices. This is because the proof only uses matrix operations on the matrix $(r - \lambda)I + \lambda J$ and does not use the structure of the underlying design. Plugging in $r = 4, \lambda = 2$ and $v = 8$ gives the correct result. However, the second formula for the determinant, i.e.

$$det(AA^T) = rk(r - \lambda)^{v-1},$$

does not hold for bordered matrices. This is no surprise because the number k is not well-defined for bordered matrices as the scalar product of a column with itself (i.e. the number of points contained in a block in the case of a design) is in general not the same for all columns of a bordered matrix. If we ignored this and tried to use the second formula for the symmetric case, i.e.

$$det(AA^T) = r^2(r - \lambda)^{v-1},$$

we would get $det(CC^T) = 2048$, which is wrong. We see that $r - \lambda$ does not need to be a square for bordered matrices if we determine r and λ from the matrix C with $CC^T = (r - \lambda)I + \lambda J$ by reading off the coefficients.

The second case of the Bruck-Ryser-Chowla theorem holds for arbitrary rational matrices and we could use it for a square bordered matrix. However, it is only applicable to matrices with an odd number of rows and columns. What can we say if the number of rows and columns is even?
We could try to imitate the proof of the Bruck-Ryser-Chowla theorem for a symmetric design with even v but we quickly run into a few problems doing so. The proof of theorem 5.1 mainly has three steps. First, we obtain an equation by viewing an incidence matrix

as a quadratic form, then we eliminate the factor n as much as possible, and finally we reduce the sum.
If we consider the case $v \equiv 0 \; mod \; 4$, then we start with the equation

$$z_1^2 + \ldots + z_v^2 = n(x_1^2 + \ldots + x_v^2) + \lambda s^2.$$

We can group the terms of the form nx_k^2 on the right into sums of four terms without any of them left over. Thus, by a change of basis the factor n disappears completely and we obtain the equation

$$z_1^2 + \ldots + z_v^2 = y_1^2 + \ldots + y_v^2 + \lambda s^2.$$

This means that we cannot draw any conclusions about the order n of the design from this equation as n has no influence on its solvability. Nevertheless, if we apply Bruck-Ryser-Chowla elimination we are left with the equation

$$z_v^2 = y_v^2 + \lambda s^2.$$

Now we would let y_v equal a non-zero rational number and conclude that this equation must have a non-trivial integer solution. But this statement is of no use to us as the equation

$$x^2 = y^2 + \lambda z^2$$

clearly has the non-trivial integer solution $x = y = 1$ and $z = 0$. So even though the parameter λ appears in the reduced equation, it has no influence on the existence of an integer solution. This means that even if we managed to construct a bordered matrix with $v \equiv 0 \; mod \; 4$ rows and columns of a hypothetical projective plane of order n, it would be of no use to us deciding whether such a plane exists (assuming that our only tool is the above analogue of the Bruck-Ryser-Chowla theorem).
If we have $v \equiv 2 \; mod \; 4$, the situation does not improve. We again consider the equation

$$z_1^2 + \ldots + z_v^2 = n(x_1^2 + \ldots + x_v^2) + \lambda s^2.$$

Since we can only eliminate the factor n in groups of four, we are left with the number n appearing two times in the equation after the usual change of basis. Adding new variables like we did in the case $v \equiv 3 \; mod \; 4$ also does not help because we would have to add two new variables to have a group of four terms of the form nx_k^2. But then the number n appears two times on the left side of the equation and we are stuck with the same situation. If we use Bruck-Ryser-Chowla elimination on an equation with two n's left, we end up with

$$z_{v-1}^2 + z_v^2 = ny_{v-1}^2 + ny_v^2 + \lambda s^2. \qquad (*)$$

We cannot do one more elimination step in this situation because we would have to achieve $z_{v-1}^2 = ny_{v-1}^2$ which is only possible if n is a square. However, if n is a square, then the whole procedure gives us no new information as we could just eliminate the factor n everywhere like we did in the case $v \equiv 0 \; mod \; 4$ and we would end up with an equation that is always solvable. Thus, in the case $v \equiv 2 \; mod \; 4$ if n is not a square, we cannot do better than the equation $(*)$. But this equation is always solvable due to a result called “Meyer’s theorem“. It states that a quadratic form over $\mathbb{Q}$ with at least five variables non-trivially represents 0 if and only if not all coefficients have the same sign (see [39] for a proof). Since n and λ are positive, this result ensures that there exists a non-zero rational solution to the equation

$$z_{v-1}^2 + z_v^2 - ny_{v-1}^2 - ny_v^2 - \lambda s^2 = 0.$$

By clearing denominators, we can also obtain a non-zero integer solution. So the existence of a non-zero solution to equation $(*)$ does not give us any information about the parameters n and λ because there *always* exists a non-zero solution.

We see that a bordered matrix with an even number of rows and columns does not help us deciding whether the incidence matrix it was built from exists or not because we do not have a statement like the Bruck-Ryser-Chowla theorem in this case.

Now we will consider the case that a bordered matrix C built from an incidence matrix A has an odd number of rows and columns. Then we can use the Bruck-Ryser-Chowla theorem for the matrix C. For this case we will take a closer look at the construction of bordered matrices.

We will assume that the number of rows and columns added to A is small. This is mainly due to computational reasons. An exhaustive search for possible borders is harder for bigger matrices because the number of possible columns and rows that can (theoretically) be added to construct C grows rapidly when the bordered matrix gets bigger. On the other hand, restrictions on the size of C allow us to obtain more detailed results about bordered matrices that may not hold for bigger matrices, which can give rise to better algorithms that compute bordered matrices faster.

In particular, we will mainly focus on adding exactly two columns and rows to A. The reason for this is that we are interested in projective planes and these have an odd number of points and lines. As we have seen that bordered matrices with an even number of rows and columns do not help us, we need to add an even number of rows and columns to A. Thus, the smallest possible case is adding two rows and columns. We will add these two rows and columns in two steps. First, we will augment A by two columns and then we will try to add two rows to this augmented matrix. This way we have control over the numbers $\widetilde{n}$ and $\widetilde{\lambda}$ such that $CC^T = \widetilde{n}I + \widetilde{\lambda}J$ because they are determined by the scalar product of a row with itself and the scalar product of two distinct rows, respectively.

An important fact about bordered matrices of small size is that the columns added to A have to be constant. To see this consider a row $(a_{i1}, \dots, a_{iv}, a, b)$ of A that was augmented with the rational numbers a and b. The scalar product of any two distinct rows of A is constant and we want that the same holds for every augmented row of A. Thus, it follows that the scalar product of (a, b) with any of the other pairs (x, y) that were added to another row of A is constant. So all of these pairs lie on a common line that is orthogonal to (a, b) when viewed as points in $\mathbb{R}^2$.

Now if there was a row that was not augmented with the pair (a, b) but with a pair $(c, d) \neq (a, b)$, then the same argument holds for this row. All other pairs (x, y) that were added to a row of A must lie on a common line orthogonal to (c, d) in $\mathbb{R}^2$. Now since not only the scalar product of two distinct augmented rows is constant but also the scalar product of an augmented row with itself, we have that $a^2 + b^2 = c^2 + d^2$. From this it follows that (a, b) and (c, d) are linearly independent because if (c, d) was a multiple of (a, b), it could only be the pair $(-a, -b)$ (otherwise $a^2 + b^2 \neq c^2 + d^2$ and we assumed $(c, d) \neq (a, b)$). However, this cannot happen as a vector (x, y) cannot have the same scalar product with both (a, b) and $(-a, -b)$ unless $a = b = 0$, and this case can be excluded because then we would obtain the same equation by applying the Bruck-Ryser-Chowla theorem to the bordered matrix. Thus, the line orthogonal to (a, b) intersects the line orthogonal to (c, d) in a unique point. Since by the argument above all pairs other than (a, b) and (c, d) must lie on both lines, they must all be the same. It is now easy to show that then every row must have been augmented with this pair. This proves that to construct a bordered matrix with two added rows and columns we need to augment every row with the same pair (a, b).

To complete the argument above, assume there exist two distinct rows of A that were both augmented with the same pair of numbers. Say these are the numbers a and b. Now consider a third row that was augmented using the pair (c, d). Since the scalar product of any two distinct rows of C has to be constant, we must have $a^2 + b^2 = ac + bd$ (consider the two rows augmented with (a, b) and a row augmented with (a, b) together with the row augmented with (c, d)). However, this can only be the case if $a = c$ and $b = d$. To see this, note that $a \neq c$ implies $(a - c)^2 > 0$ and thus $2ac < a^2 + c^2$. Similarly, we have $2bc < b^2 + d^2$. Recalling that $a^2 + b^2 = c^2 + d^2 = ac + bd$ it follows that

$$a^2 + b^2 + c^2 + d^2 = 2ac + 2bd < a^2 + c^2 + b^2 + d^2,$$

which is a contradiction. So the columns added to our matrix A have to be constant. To see why this does not have to be the case for bigger bordered matrices, take a projective plane Π that has a proper subplane Π_0. An incidence matrix of Π is essentially a bordered matrix of Π_0, but the rows and columns added are not constant. However, as long as the number of added rows and colums is significantly smaller than the number of rows and columns of A the added columns have to be constant. To see this, we can essentially use the same idea as above with some additional arguments.

Now assume that we have chosen the two rational numbers a and b to augment the rows of A. We will now take a look at the restrictions on the rows that we want to add to A. First, by a similar argument like above, we have that the first v elements of an added row have to be the same. So as a start, consider adding one row to the augmented matrix, i.e. consider the matrix

$$\begin{pmatrix} & & & a & b \\ & A & & \vdots & \vdots \\ & & & a & b \\ c & \cdots & c & d & e \end{pmatrix}$$

for rational numbers c, d and e. If A is an incidence matrix of a symmetric 2-(v, k, λ) design, then the scalar product of a row of A with itself is k and the scalar product of two distinct rows is λ. So the product of a row of the bordered matrix with itself is $k + a^2 + b^2$ and the product of two distinct rows is $\lambda + a^2 + b^2$. If we want to construct a bordered matrix, then these properties must also hold for the added rows. Thus, we must have

$$vc^2 + d^2 + e^2 = k + a^2 + b^2, \quad kc + ad + be = \lambda + a^2 + b^2,$$

since A has v columns and exactly k ones per row. We can just compute some rows satisfying these criterions independently and then check whether they are compatible, i.e. whether the product of two distinct added rows is also equal to $\lambda + a^2 + b^2$. If this is the case, we have found a bordered matrix. Note that if we wanted to compute a bigger bordered matrix, then we would need to find a set of pairwise compatible rows.
If we manage to construct a bordered matrix C of A, then it satisfies

$$CC^T = nI + (\lambda + a^2 + b^2)J$$

because the scalar product of two distinct rows of C and the scalar product of a row of C with itself both grow by $a^2 + b^2$ as compared to the scalar product of the rows of A. Thus, the change is reflected only by a change of the factor in front of the ones matrix J.

Before we use the ideas above for the computation of bordered matrices, we give an example of a bordered matrix and summarise our findings. The example is taken from Xu's article [57]. Xu has given an example of a square bordered matrix for the (hypothetical) projective plane of order 12.

6.5 Example (Xu [57])**.** Assume that a finite projective plane of order 12 exists. Let A be any of its incidence matrices, which are 157×157-matrices. Then we can build a square bordered matrix

$$C = \begin{pmatrix} A & B_1 \\ B_2 & B_3 \end{pmatrix}$$

of size 160×160 with

$$B_1 = \begin{pmatrix} 2 & 0 & 2 \\ \vdots & \vdots & \vdots \\ 2 & 0 & 2 \end{pmatrix}, \quad B_2 = \begin{pmatrix} -\frac{1}{7} & \cdots & -\frac{1}{7} \\ \frac{15}{91} & \cdots & \frac{15}{91} \\ -\frac{5}{259} & \cdots & -\frac{5}{259} \end{pmatrix}, \quad B_3 = \begin{pmatrix} \frac{24}{7} & \frac{10}{7} & 2 \\ \frac{368}{91} & \frac{4}{91} & -\frac{8}{13} \\ \frac{694}{259} & -\frac{818}{259} & \frac{72}{37} \end{pmatrix}.$$

We have checked that $CC^T = 12I_{160} + 9J_{160}$. Although, as pointed out before, this example does not help us determining whether a projective plane of order 12 exists, it does show that it is possible to construct a square bordered matrix for the projective plane of order 12.

We summarise our findings about small square bordered matrices in the following remark.

6.6 Remark. Assume that we are given a rational matrix A with $AA^T = nI_v + \lambda J_v$ and a square bordered matrix C of A.

- C satisfies
$$CC^T = nI_w + \widetilde{\lambda} J_w$$
for some numbers w and $\widetilde{\lambda}$, i.e. n does not change.
- We do not have an analogue of the Bruck-Ryser-Chowla theorem for even v, so a bordered matrix with an even number of rows and columns does not help us.
- The columns added to A are constant, i.e. the rows of A were all augmented with the same numbers, if C is not significantly bigger than A.
- We have a way of quickly determining whether or not an equation of the form
$$x^2 = ny^2 + (-1)^{\frac{v-1}{2}} \lambda z^2$$
is solvable (see theorem 5.9). If we want to disprove the existence of a certain symmetric design, we need to find a bordered matrix the gives rise to an unsolvable equation.

6.3 Computational results

In this section we describe our findings from some attempts to construct bordered matrices. To keep the runtime of our algorithm reasonably short, we will focus on small cases. First of all, we fix some notation. In this section A denotes an incidence matrix of projective plane of order n, i.e. we have

$$AA^T = nI + J,$$

A is a $(v \times v)$-matrix for $v = n^2 + n + 1$, every row of A has exactly $n+1$ ones and for any two rows there is exactly one column where they both have the entry 1. Furthermore, the letters a, b, c, d and e always stand for the numbers that we use to border the matrix A, i.e. we consider the matrix

$$\begin{pmatrix} & & & a & b \\ & A & & \vdots & \vdots \\ & & & a & b \\ c & \cdots & c & d & e \end{pmatrix}.$$

Without loss of generality we can assume that:

- a and b are non-negative (otherwise replace a and d with $-a$ and $-d$ or b and e with $-b$ and $-e$ as needed)
- $a \geq b$ (otherwise swap the two rightmost columns)
- $a \neq 0$ (otherwise we had $a = b = 0$ and we would obtain the same equation from the Bruck-Ryser-Chowla theorem)

Furthermore, if we can add one more row to the matrix above to obtain a bordered matrix C, then we have

$$CC^T = nI + (1 + a^2 + b^2)J.$$

First of all, we take a look at which values for $a^2 + b^2$ give us an unsolvable equation from the Bruck-Ryser-Chowla theorem. If the equation is solvable, constructing a bordered matrix is pointless. We do this for the solved cases $n = 6$ and $n = 10$ and for the smallest cases where the existence of a projective plane of order n is neither proven nor disproven. The fact that these values for $a^2 + b^2$ indeed lead to unsolvable equations is easily verified using theorem 5.9.

n	$a^2 + b^2$
6	2, 3, 6, 8, ...
10	1, 2, 4, 6, 7, ...
12	1, 2, 4, 6, 7, 9, ...
15	1, 2, 4, 5, 6, 7, ...
18	2, 4, 5, 9, ...
20	1, 2, 5, 6, 7, 9, ...

We have only listed all suitable values for $a^2 + b^2$ that are smaller than 10. Now for every value s we need a list of pairs of rational numbers (a, b) such that $a^2 + b^2 = s$. Since an integer is the sum of two rational squares if and only if it is the sum of two integer squares (see theorem 4.2.3 in Beutelspacher's book [5] for a proof), there are no such pairs for some values. For example, 3 is not the sum of two integer squares, so it is also not the sum of two rational squares. Thus, we cannot construct a bordered matrix in which $a^2 + b^2 = 3$. However, these values can be obtained by adding four or more columns so we did not leave them out in the list above. They can still be helpful when constructing bigger bordered matrices.

For our purposes now, we can disregard the values 3, 6 and 7 because they are not sums of two squares. Now we need non-trivial rational solutions of

$$a^2 + b^2 = s$$

for $s \in \{1, 2, 4, 5, 8, 9\}$. A list of the pairs we used in our computations can be found in section 9.2 in the appendix.

We now describe the program that the author wrote to compute bordered matrices using SageMath. The function "border2($n, a, b, depth$)" tries to find a bordered matrix of an incidence matrix of a projective plane of order n by adding two columns and two rows to it. It takes as input the order n of the hypothetical projective plane, the two numbers a and b that are added to the right of the incidence matrix, and a parameter *depth* that is an upper bound on the denominator of some rational numbers involved to make iteration over rational numbers possible.

We are looking for rows to add to the bottom of an incidence matrix A of a projective plane of order n that was already augmented with two columns on the right. Recall that the augmented matrix with one added row looks like this

$$\begin{pmatrix} & & & a & b \\ & A & & \vdots & \vdots \\ & & & a & b \\ c & \cdots & c & d & e \end{pmatrix}$$

and that the relevant equations for adding a row are

$$vc^2 + d^2 + e^2 = k + a^2 + b^2, \quad kc + ad + be = 1 + a^2 + b^2 \tag{$*$}$$

where $v = n^2 + n + 1$ and $k = n + 1$. We will frequently use the following terms.

Definition. A row that satisfies both equations $(*)$ is called a *possible row.* Two possible rows are called *compatible* if their scalar product is equal to $1 + a^2 + b^2$.

Our goal is to find two compatible rows because then we have found a square bordered matrix. We will also use these terms for matrices with more than two added columns (i.e. a possible row is a row such that the scalar product with itself and the scalar product with the other rows is consistent with the rest of the matrix).
First, note that $d^2, e^2 \geq 0$, so we have

$$vc^2 \leq k + a^2 + b^2 \iff |c| \leq \sqrt{\frac{k + a^2 + b^2}{v}}.$$

As v is much bigger than $k + a^2 + b^2$ for small values of $a^2 + b^2$, this gives us a strong bound on c. Thus, the first step of the program is to compute all rational numbers with a denominator less than or equal to *depth* that satisfy the inequality above.
Now we would like to have a criterion that can rule out many values of c so we do not have to test whether or not there exist suitable numbers d and e to complete the row. Our approach is the following:
Since we have $a > 0$, we can solve the second equation $(*)$ for d. Plugging the result into the equation $vc^2 + d^2 + e^2 = k + a^2 + b^2$ eliminates the variable d and only the variables c and e remain. We cannot eliminate more variables but what we can do is rearrange all terms where the variable e shows up to the right side of the equation, complete the square so that e only shows up inside of brackets and then rearrange the rest to the other side of the equation. Then c is the only variable appearing on the left side of the equation and the right side of the equation is a rational square, no matter which value e has. The resulting equation is quite big and messy so we do not give it here but the interested reader can find it in section 9.1 in the appendix.
The program now takes one of the possible precomputed values for c and checks whether the formula yields a rational square when plugging in the value for c. If it does not, we can immediately go to the next candidate for c. If it does return a square, the corresponding value for e can be computed from the rearranged equation (in fact, there are two possible values as we have to take square roots) and using this information, we can easily compute the remaining value for d. Now we have a triple (c, d, e) that satisfies

both equations $(*)$, and thus we have found a possible row. When a row is found the program checks whether it is compatible with any row already computed. If it finds a compatible row, it prints the compatible rows and terminates. Else it just stores the row and tries the next value for c. If no compatible rows are found, there is no bordered matrix for the given input where the denominator of c is less than or equal to *depth*.

It should be noted that the upper bound on the denominator only affects the number c. The numbers d and e can have bigger denominators than c. We have checked that our algorithm indeed produces possible rows for a bordered matrix (i.e. satisfying the equations $(*)$) and that every possible row where the denominator of c is less than or equal to *depth* is computed by comparison with a simple brute force algorithm that checks every combination.

Now we have a tool to compute bordered matrices for projective planes with exactly two added rows and columns effectively. We will now describe the results of our computations. For every combination of n and $a^2 + b^2$ we ran our program for every decomposition listed in the appendix in section 9.2. We picked a value of $depth = 1000$ for every run. One reason for this is the runtime because then most runs finish in less than 30 seconds. Another reason is that we have seen that in the bordered matrix that Xu constructed (see example 6.5) every denominator is less than 1000 which shows that it is possible to construct a bordered matrix using “small“ numbers. Furthermore, the denominators of the numbers that we add to the right of the matrix are small so it is reasonable to assume that if a bordered matrix with these numbers on the right exists, then the denominators in this matrix are not too big.

The following table contains our results. The first two columns contain our input. In the third column we wrote down whether we found any possible rows and how many we found per run on average (since we tested multiple different decompositions per value of $a^2 + b^2$). The last column then shows whether we found compatible rows or not.

n	a^2+b^2	found possible rows?	found compatible rows?
6	2	yes (634 per run)	no
	8	no	no
10	1	no	no
	2	no	no
	4	no	no
12	1	yes (204 per run)	no
	2	yes (130 per run)	no
	4	yes (142 per run)	no
	9	no	no
15	1	no	no
	2	no	no
	4	no	no
	5	yes (224 per run)	no
18	2	no	no
	4	yes (228 per run)	no
	5	no	no
	9	no	no
20	1	no	no
	2	no	no
	5	no	no
	9	no	no

If no possible rows were found, we reran the search with a paramter of *depth* $= 5000$. Still no possible rows were found.
It turns out that the numbers in the third column are not only the averages of the numbers of possible rows we found. Every run returned the same number of possible rows (although the rows themselves were of course different). In fact, we can prove the following:
The number of possible rows that start with the number c only depends on a^2+b^2, not on the actual values of a and b. Thus, we get the same number of possible rows for different decompositions of the integer a^2+b^2 as the sum of two squares.
The proof is a little lengthy and technical, so we moved it to the appendix. See section 9.3 for the proof.
This insight allows us to do less computations without missing a bordered matrix. If we do not find any possible rows for a decomposition a^2+b^2, then we will also not find a possible row for a different decomposition (as long as we run the program with the same parameter *depth*). However, we do not know whether the above result also holds for the number of *compatible* rows. If that was the case, then we could disregard testing different decompositions completely and just stick to one fixed decomposition which would greatly reduce the amount of computations needed.

Our algorithm seems to be exponential in the parameter *depth* while the parameters

n, a and b have less influence on the runtime. These parameters mainly determine the number of values for c that we need to check. Since $v = n^2 + n + 1$ grows asymptotically faster than $k = n + 1$, higher values for n give a tighter restriction on the possible values for c. If n, a and b are fixed, doubling the parameter *depth* corresponds roughly to multiplying the runtime by a factor of 4.

Constructing a bordered matrix with four added rows and columns is much harder because in order to find a possible row we have to find five suitable values (one for the first v columns and four for the rest). We do not have an efficient test to see whether or not a possible row can start with the value c. For bordered matrices with two added rows and columns this came down to one test.
What we can do is implement a test similar to what we describe in the appendix in section 9.3, i.e. we can check whether a sphere and a hyperplane intersect. However, although this test can rule out certain values immediately, the condition it checks is only necessary. So we do not know whether a value that passes the test can actually be the first element of a possible row. If it can, we also do not know how to compute a possible row as there are still four unknowns left. We implemented a simple brute force algorithm to search for possible rows for a matrix with four added columns. However, it takes a long time to finish even for small inputs and we did not find a bordered matrix using it.

7 Projective planes of small order and related conjectures

In this chapter we want to give a little insight into a problem that we have not dealt with in this thesis. We are mainly concerned with whether a projective plane of order n exists or not, but we have not dealt with the question how many non-isomorphic planes of a given order exist. There is a detailed article by Moorhouse about projective planes of order less than 32 and we do not intend to repeat all of its contents here. We will state some of the results and talk a little about related problems and conjectures. For further details on projective planes of small order see Moorhouse's article [40] and the list on his website [42] where the reader can find incidence tables, generators of the automorphism group, orbit lengths and some further information for all known projective planes of small order.

First, all projective planes of order less than 8 are desarguesian. So for the orders $q = 2$, 3, 4, 5, 7 and 8, the projective plane $PG(2, q)$ is the only projective plane of order q up to isomorphism. The smallest non-desarguesian projective plane has order 9. There are four different projective planes of order 9 up to isomorphism. One is the desarguesian plane $PG(2, 9)$ and another one is the Hughes plane of order 9 that we described in chapter 4. The other two planes are the smallest Hall plane and its dual. Lam, Kolesova and Thiel proved in 1991 that these are in fact all projective planes of order 9 [32]. It is interesting to note that the Hall plane of order 9 and its dual are proven to be the only projective planes of Lenz-Barlotti class IVa.3 and IVb.3, respectively.

We have already stated that there exists no projective plane of order 10. So the list on Moorhouse's website is known to be complete only up to $n = 10$. However, there are complete classifications of some special cases. For example, all translation planes of orders 16, 25, 27 and 49 are completely classified (see [17], [11], [16] and [38] respectively). This is usually done by an exhaustive computer search. Since all translation planes of prime order are desarguesian, there is no need for a classification in these cases.

It stands out that in the list on Moorhouse's website, for every prime p there is only one type of projective plane of order p. This leads us to the so called *uniqueness conjecture*. It states that a finite projective plane of prime order must be desarguesian. We know that it holds for translation planes, but it is not known whether it holds for arbitrary projective planes. There also exists a slightly more general result: an *affine* plane of prime order that admits a collineation group that is transitive on the points is desarguesian. For a proof see the article by Hiramine [26]. Note that this is a generalisation of the result about translation planes as the collineations here do not have to be translations. In fact, it can be shown that an affine plane with a transitive collineation group need not be a translation plane.

There is a coding theoretic approach to the uniqueness conjecture by Bagchi [3]. We give a brief description. Let Π be a projective plane, A be any of its incidence matrices and C be the vector space generated by the columns of A over $\mathbb{F}_p$ for some prime number p. Then C is called the *p-ary code* of Π. The key object of Bagchi's approach is the *complete weight enumerator*. Let X_i be a variable for every element $i \in \mathbb{F}_p$. For an element $c \in C$ let $k_i(c)$ denote the number of times the element $i \in \mathbb{F}_p$ appears in c. Then the complete weight enumerator of C is defined by

$$f(C) = \sum_{c \in C} \prod_{i=0}^{p-1} X_i^{k_i(c)},$$

where all variables commute with each other. The complete weight enumerator contains much information about the p-ary code and is independent of the incidence matrix A that was used to construct C. Bagchi proved the following result:

7.1 Theorem (Bagchi, theorem 4.5 in [3]). *Let Π be a projective plane of order p for a prime p such that the complete weight enumerator of its p-ary code is the same as the complete weight enumerator of the p-ary code of $PG(2,p)$. If $p > 2^9$, then Π is isomorphic to $PG(2,p)$.*

This gives us an alternate way of proving that a projective plane of prime order p is isomorphic to $PG(2,p)$. We decided to include this result because coding theoretic approaches seem to be a strong technique for tackling problems about projective planes. The non-existence of a projective plane of order 10 was also proven by coding-theoretic means. We cannot say whether this result will be vital in proving or disproving the uniqueness conjecture, but we can imagine that it might be important.

Another conjecture related to projective planes and codes is the *Hamada-Sachar conjecture*. It is about the p-rank of a design D, i.e. the rank of an incidence matrix of D when viewed over the field $\mathbb{F}_p$. The statement of the conjecture is the following:

7.2 Conjecture (Conjecture 6.9.1 in [2]). *Every projective plane of order p^s, p a prime, has p-rank at least $\binom{p+1}{2}^s + 1$ with equality if and only if it is desarguesian.*

Hamada made a more general conjecture which was disproved by Tonchev [54]. However, the narrower conjecture above, stated indepently by Sachar, is still undecided. Although the conjecture has no direct connection to the prime power conjecture, we included it to further show the connections between projective planes and coding theory. We would not be surprised if progress on one conjecture also benefited the other.

8 Summary and conclusion

This thesis aimed to give an overview of the prime power conjecture including its history. We have seen that the prime power conjecture is proven for a rich class of projective planes called translation planes and all known finite non-translation planes have prime power order as well. Since there are only a few ways known to construct non-translation planes, it can be argued that the difficulty of the prime power conjecture is due to the fact that we do not know non-translation planes well enough.

The strongest non-existence result about projective planes that we know is the Bruck-Ryser theorem. It is a simple criterion and excludes an infinite set of orders. Apart from the projective plane of order 10, every ruled out value is due to the Bruck-Ryser theorem. We have also seen that coding theoretic approaches yielded many strong results about projective planes. The existence of a projective plane of order 10 could not be ruled out by the Bruck-Ryser theorem. However, the non-existence was ultimately shown using coding theoretic techniques. Furthermore, as this thesis approaches the prime power conjecture mainly from a combinatorial point of view, many techniques like coordinatisation have been left out. There are various ways to approach projective planes. Different perspectives are always helpful to tackle problems from different angles and especially coordinatisation and coding theory have proven themselves to be especially useful when dealing with projective planes.

Our main goal was to analyse the approach by Xu using bordered matrices. The first attempt using rectangular bordered matrices does not work. However, in theory we can use the same approach using square bordered matrices. The main problem with this is the runtime. Small bordered matrices can be computed fairly quickly, but computing bigger bordered matrices is hard.
It can be argued that finding a “big“ bordered matrix is not easier than just listing all possible incidence matrices. As long as we cannot compute bordered matrices with more than two added rows and columns effectively, it is not really a viable method to tackle the prime power conjecture. We can try to find a small bordered matrix, but we do not know in advance whether it even exists. This is another disadvantage of this approach. It is possible that there exist only bordered matrices such that the equation obtained from the Bruck-Ryser-Chowla theorem is solvable or that there exist no bordered matrices at all. In these cases the question of the existence of the underlying projective plane cannot be settled using bordered matrices.
Furthermore, while the number of possible incidence matrices for a projective plane is finite, allowing an exhaustive search to solve the problem, we cannot do this for bordered matrices because there are infinitely many possibilities. However, bordered matrices with

two added rows and columns can be computed easily (if they exist). It does not hurt to check for small bordered matrices and run our SageMath program for different inputs since the function terminates quickly as long as the parameter *depth* is not too high. We can also say in advance which inputs would lead to unsolvable equations if we found a bordered matrix, eliminating unnecessary computations. After all, it takes only one bordered matrix to prove the non-existence of a projective plane.
Our computations did not return any bordered matrices. It is possible that we could have found a bordered matrix by using different inputs for our function. We could imagine that further work about bordered matrices could lead to faster algorithms. However, it could also be impossible to disprove the existence of a projective plane using bordered matrices. We do not believe that this approach can solve the prime power conjecture completely but we can imagine that the non-existence of some projective planes can be shown using bordered matrices.

9 Appendix

9.1 The SageMath program for bordered matrices

Here we describe our SageMath function “border2$(n, a, b, depth)$“ in a little more detail. Recall that we assume that a projective plane of order n exists. Let A be any of its incidence matrices. We take two rational numbers a and b with $a \neq 0$ and add two constant columns with these numbers to the right of A. First, the program checks whether $a^2 + b^2$ is an integer. This can prevent mistakes like typos in the input. Adding a row to this augmented matrix looks like this

$$\begin{pmatrix} & & & a & b \\ & A & & \vdots & \vdots \\ & & & a & b \\ c & \cdots & c & d & e \end{pmatrix}$$

and the relevant equations for adding a row are

$$vc^2 + d^2 + e^2 = k + a^2 + b^2, \quad kc + ad + be = 1 + a^2 + b^2.$$

We compute all rational numbers c with denominator less than or equal to *depth* that satisfy

$$vc^2 \leq k + a^2 + b^2 \iff |c| \leq \sqrt{\frac{k + a^2 + b^2}{v}}.$$

Since we have $a > 0$, we can solve the second equation for d

$$kc + ad + be = 1 + a^2 + b^2 \iff d = \frac{1 + a^2 + b^2 - kc - be}{a}$$

and substitute the result for d in the first equation. Rearranging all terms containing e to the right, completing the square and rearranging all remaining terms to the left side of the equation leaves us with

$$\frac{(-va^2 - k^2)c^2 + 2kc(1 + a^2 + b^2) + a^2(k + a^2 + b^2) - (1 + a^2 + b^2)^2}{a^2 + b^2} + \left(\frac{kbc - b(1 + a^2 + b^2)}{a^2 + b^2}\right)^2$$
$$= \left(e + \frac{kbc - b(1 + a^2 + b^2)}{a^2 + b^2}\right)^2.$$

In this equation the only variable on the left side is c and the right side is a square. The program now checks whether the left hand side returns a rational square when plugging in a value for c. If so, then we have found a possible row and we can compute the two corresponding values for e and the associated value for d. The program then checks whether the row is compatible with any row that was already computed. If it finds a compatible row, it prints it together with the newly computed row and if not, it saves the row and goes on to the next value for c.

9.2 Integers as sums of two squares

Here we give the pairs of rational numbers that we used as input for our function "border2($n, a, b, depth$)". We need to write the integers 1, 2, 4, 5, 8 and 9 as the sum of two rational squares. Equivalently, we can view this as searching non-zero integer solutions to the equation

$$x^2 + y^2 = kz^2$$

for $k \in \{1, 2, 4, 5, 8, 9\}$. If (x, y, z) is a non-trivial integer solution, then we can write

$$\left(\frac{x}{z}\right)^2 + \left(\frac{y}{z}\right)^2 = k,$$

so we get a decomposition of the integer k as the sum of two rational squares. We see that we can restrict ourselves to triples (x, y, z) such that x, y and z do not share a common factor.

For computing integer solutions, we just try all values for z up to a given bound and check whether we can write the integer kz^2 as the sum of two integer squares. We then choose the ten smallest solutions with respect to z.

1 :

a	1	$\frac{3}{5}$	$\frac{5}{13}$	$\frac{8}{17}$	$\frac{7}{25}$	$\frac{20}{29}$	$\frac{12}{37}$	$\frac{9}{41}$	$\frac{28}{53}$	$\frac{11}{61}$
b	0	$\frac{4}{5}$	$\frac{12}{13}$	$\frac{15}{17}$	$\frac{24}{25}$	$\frac{21}{29}$	$\frac{35}{37}$	$\frac{40}{41}$	$\frac{45}{53}$	$\frac{60}{61}$

2 :

a	1	$\frac{1}{5}$	$\frac{7}{13}$	$\frac{7}{17}$	$\frac{17}{25}$	$\frac{1}{29}$	$\frac{23}{37}$	$\frac{31}{41}$	$\frac{17}{53}$	$\frac{49}{61}$
b	1	$\frac{7}{5}$	$\frac{17}{13}$	$\frac{23}{17}$	$\frac{31}{25}$	$\frac{41}{29}$	$\frac{47}{37}$	$\frac{49}{41}$	$\frac{73}{53}$	$\frac{71}{61}$

4 :

a	2	$\frac{6}{5}$	$\frac{10}{13}$	$\frac{16}{17}$	$\frac{14}{25}$	$\frac{40}{29}$	$\frac{24}{37}$	$\frac{18}{41}$	$\frac{56}{53}$	$\frac{22}{61}$
b	0	$\frac{8}{5}$	$\frac{24}{13}$	$\frac{30}{17}$	$\frac{48}{25}$	$\frac{42}{29}$	$\frac{70}{37}$	$\frac{80}{41}$	$\frac{90}{53}$	$\frac{120}{61}$

5 :

a	2	$\frac{2}{5}$	$\frac{2}{13}$	$\frac{19}{13}$	$\frac{1}{17}$	$\frac{22}{17}$	$\frac{38}{25}$	$\frac{19}{29}$	$\frac{22}{29}$	$\frac{11}{37}$
b	1	$\frac{11}{5}$	$\frac{29}{13}$	$\frac{22}{13}$	$\frac{38}{17}$	$\frac{31}{17}$	$\frac{41}{25}$	$\frac{62}{29}$	$\frac{61}{29}$	$\frac{82}{37}$

8 :

a	2	$\frac{2}{5}$	$\frac{14}{13}$	$\frac{14}{17}$	$\frac{34}{25}$	$\frac{2}{29}$	$\frac{46}{37}$	$\frac{62}{41}$	$\frac{34}{53}$	$\frac{98}{61}$
b	2	$\frac{14}{5}$	$\frac{34}{13}$	$\frac{46}{17}$	$\frac{62}{25}$	$\frac{82}{29}$	$\frac{94}{37}$	$\frac{98}{41}$	$\frac{146}{53}$	$\frac{142}{61}$

9 :

a	3	$\frac{9}{5}$	$\frac{15}{13}$	$\frac{24}{17}$	$\frac{21}{25}$	$\frac{60}{29}$	$\frac{36}{37}$	$\frac{27}{41}$	$\frac{84}{53}$	$\frac{33}{61}$
b	0	$\frac{12}{5}$	$\frac{36}{13}$	$\frac{45}{17}$	$\frac{72}{25}$	$\frac{63}{29}$	$\frac{105}{37}$	$\frac{120}{41}$	$\frac{135}{53}$	$\frac{180}{61}$

It stands out that the same numbers turn up as denominators of the fractions. All denominators are equal to 1 modulo 4 and are the sum of two squares. It is easy to prove that this is always the case if the fractions are in lowest terms.

9.3 The existence of possible rows

Here we give the proof that the number of possible rows for a matrix A augmented with a and b does not depend on the specific decomposition $a^2 + b^2$.
Consider the equations for a possible row. If we augment the rows of A with the numbers a and b and want to know whether there exists a possible row starting with c, we have to solve the equations

$$vc^2 + d^2 + e^2 = k + a^2 + b^2, \quad kc + ad + be = 1 + a^2 + b^2$$

in which the only unknowns are d and e. If we call them x and y and rearrange the equations, we get

$$x^2 + y^2 = r^2, \quad ax + by = s$$

for some rational numbers r and s with $r \geq 0$. A rational solution (x, y) gives us a possible row. Viewing the equations in the euclidean space $\mathbb{R}^2$, the first equation represents a circle centred at the origin and second equation represents a line L (since a and b cannot be both equal to zero). They can intersect in either 0, 1 or 2 points depending only on the distance of L to the origin. From linear algebra, we know that the distance of L to the origin is given by the formula

$$\frac{|s|}{\sqrt{a^2 + b^2}}.$$

Now note what happens when we switch from the decomposition $a^2 + b^2$ to a decomposition $\widetilde{a}^2 + \widetilde{b}^2$ with $a^2 + b^2 = \widetilde{a}^2 + \widetilde{b}^2$. For the same value of c, we get the equations

$$x^2 + y^2 = r, \quad \widetilde{a}x + \widetilde{b}y = s,$$

i.e. the values r and s stay the same. The number of solutions again only depends on the distance of the line $\widetilde{L}$ defined by the second equation to the origin. This distance is

$$\frac{|s|}{\sqrt{\widetilde{a}^2 + \widetilde{b}^2}} = \frac{|s|}{\sqrt{a^2 + b^2}}.$$

As this distance is the same as the distance of L to the origin, it follows that the number of solutions for the decomposition $a^2 + b^2$ is the same as the number of solutions for the decomposition $\widetilde{a}^2 + \widetilde{b}^2$.

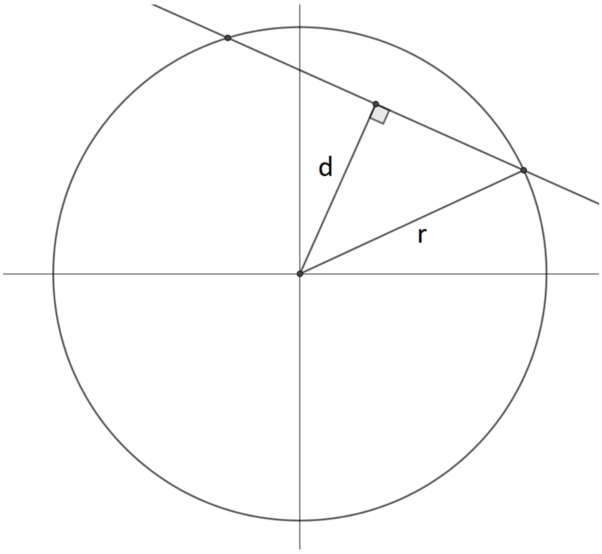
Note that we have only proved that there exists the same number of *real* solutions. We also have to prove that there exists the same number of *rational* solutions. We will prove this by showing that *if* there exists a rational solution for a given decomposition, *then* the solutions for all other decompositions are rational as well.

Consider again the system of equations for a possible row starting with c for a matrix that was augmented with the rational numbers a and b

$$x^2 + y^2 = r^2, \quad ax + by = s$$

with $r = k + a^2 + b^2 - vc^2$ and $s = 1 + a^2 + b^2 - kc$ and assume it is solvable over the real numbers.

The first equation represents a circle with radius r centred at the origin and the second equation represents a line orthogonal to the vector (a, b). The setup is visualized in the following figure:



.

We start by computing where the line and the circle intersect. The distance of the line to the origin, denoted as d, is given by

$$d = \frac{|s|}{\sqrt{a^2+b^2}}.$$

To get to the intersection points, we can start at the origin, walk in the direction of the vector (a,b) until we hit the line, and then walk along the line until we hit the circle. As the vector $(b,-a)$ is orthogonal to the vector (a,b), the intersection can be calculated as

$$\begin{pmatrix} x \\ y \end{pmatrix} = \frac{d}{\sqrt{a^2+b^2}} \begin{pmatrix} a \\ b \end{pmatrix} \pm \frac{\sqrt{r^2-d^2}}{\sqrt{a^2+b^2}} \begin{pmatrix} b \\ -a \end{pmatrix}.$$

So the first coordinate is given by

$$x = \frac{|s|}{a^2+b^2} \cdot a \pm \frac{\sqrt{r^2-d^2}}{\sqrt{a^2+b^2}} \cdot b.$$

This number is rational if and only if the number

$$\frac{\sqrt{r^2-d^2}}{\sqrt{a^2+b^2}}$$

is rational. We see that this number only depends on a^2+b^2 because this is true for r and d. Thus, it follows that if this number is rational for a decomposition a^2+b^2, it is rational for all decompositions $\widetilde{a}^2+\widetilde{b}^2$ with $a^2+b^2=\widetilde{a}^2+\widetilde{b}^2$. This means that if the solution for one decomposition is rational, it is rational for all decompositions.
In order to finish the proof, we have to mention that the set of possibles values for c that we test also only depends on a^2+b^2 and not on the specific values of a and b. So for different decompositions we test the same values for c and every value gives the same number of possible rows. Thus, the total number of possible rows is the same.

Note that this approach gives us an alternative way to compute bordered matrices. To check if a possible row can start with the value c, we have to check if the number

$$\frac{\sqrt{r^2-d^2}}{\sqrt{a^2+b^2}}$$

is rational. If it is, we can compute the rest of the row with the formula above. If not, there is no possible row starting with c. There is no significant difference in the runtime of this algorithm compared to the one we described in section 9.1.
This idea can also be generalised to bigger bordered matrices by considering the intersection of a sphere and a hyperplane. If there exist no intersections for a given value c, then there cannot be a possible row starting with c. This gives us a preliminary test to quickly rule out some values. However, note that the existence of intersection points is only a necessary but not a sufficient criterion for the existence of a possible row.

References

[1] Johannes André. “Über nicht-Desarguessche Ebenen mit transitiver Translationsgruppe”. In: *Mathematische Zeitschrift vol. 60* (1954), pp. 156–186.

[2] Edward Ferdinand Assmus Jr. and Jennifer D. Key. *Designs and their Codes.* Cambridge University Press, 1992.

[3] Bhaskar Bagchi. “A coding theoretic approach to the uniqueness conjecture for projective planes of prime order”. In: *Designs, Codes and Cryptography vol. 87* (2019), pp. 2375–2389.

[4] Adriano Barlotti. “Le possibili configurazioni del sistema delle coppie punto-retta (A, a) per cui un piano grafico risulta (A, a)-transitivo.” In: *Bollettino dell'Unione Matematica Italiana vol. 12* (1957), pp. 212–226.

[5] Albrecht Beutelspacher. *Einführung in die endliche Geometrie I.* Bibliographisches Institut, 1982.

[6] Aart Blokhuis, Dieter Jungnickel, and Bernhard Schmidt. “Proof of the prime power conjecture for projective planes of order n with abelian collineation groups of order n^2”. In: *Proceedings of the American Mathematical Society vol. 130 no. 5* (2002), pp. 1473–1476.

[7] Raj Chandra Bose. “On the Application of the Properties of Galois Fields to the Problem of Construction of Hyper-Græco-Latin Squares”. In: *Sankhyā: The Indian Journal of Statistics vol. 3* (1938), pp. 323–338.

[8] Richard Hubert Bruck and Herbert John Ryser. “The nonexistence of certain finite projective planes”. In: *Canadian Journal of Mathematics vol. 1* (1949), pp. 88–93.

[9] Sarvadaman Chowla and Herbert John Ryser. “Combinatorial problems”. In: *Canadian Journal of Mathematics vol. 2* (1950), pp. 93–99.

[10] Robert S. Coulter and Rex W. Matthews. “Planar Functions and Planes of Lenz-Barlotti Class II”. In: *Designs, Codes and Cryptography vol. 10* (1997), pp. 167–184.

[11] Terry Czerwinski and David Oakden. “The translation planes of order twenty-five”. In: *Journal of Combinatorial Theory, Series A vol. 59* (1992), pp. 193–217.

[12] Shrikrishna Gopalrao Dani and Athanase Papadopoulos. *Geometry in History.* Springer, 2019.

[13] Peter Dembowski. *Finite Geometries.* Springer, 1968.

[14] Peter Dembowski. “Gruppentheoretische Kennzeichnungen der endlichen desarguesschen Ebenen”. In: *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg vol. 29* (1965), pp. 92–106.

[15] Peter Dembowski and Theodore Gleason Ostrom. “Planes of order n with collineation groups of order n^2”. In: *Mathematische Zeitschrift vol. 103* (1968), pp. 239–258.

[16] Ulrich Dempwolff. “Translation planes of order 27”. In: *Designs, Codes and Cryptography vol. 2* (1994), pp. 105–121.

[17] Ulrich Dempwolff and Arthur Reifart. “The classification of the translation planes of order 16, I”. In: *Geometriae Dedicata vol. 15* (1983), pp. 137–153.

[18] Inkscape Developers. *Inkscape (Version 1.0).* 2020. URL: `https://inkscape.org`.

[19] Gino Fano. “Sui postulati fondamentali della geometria proiettiva”. In: *Giornale di Matematiche vol. 30* (1892), pp. 106–132.

[20] Raúl Figueroa. “A family of not (V, l)-transitive projective planes of order $q^3, q \not\equiv 1 \pmod 3$ and $q > 2$”. In: *Mathematische Zeitschrift vol. 181* (1982), pp. 471–479.

[21] Theo Grundhöfer. “A synthetic construction of the Figueroa planes”. In: *Journal of Geometry vol. 26* (1986), pp. 191–201.

[22] Marshall Hall. “Projective Planes”. In: *Transactions of the American Mathematical Society vol. 54* (1943), pp. 229–277.

[23] Marshall Hall and John Wilkinson. “Ternary and binary codes for a plane of order 12”. In: *Journal of Combinatorial Theory, Series A vol. 36* (1984), pp. 183–203.

[24] Christoph Hering and Hans-Jörg Schaeffer. “On the new projective planes of R. Figueroa”. In: *Combinatorial Theory. Lecture Notes in Mathematics vol. 969.* 1982, pp. 187–190.

[25] Christoph H. Hering and William M. Kantor. “On the Lenz-Barlotti Classification of Projective Planes”. In: *Archiv der Mathematik vol. 22* (1971), pp. 221–224.

[26] Yutaka Hiramine. “A conjecture on affine planes of prime order”. In: *Journal of Combinatorial Theory, Series A vol. 52* (1989), pp. 44–50.

[27] Daniel R. Hughes. “A Class of Non-Desarguesian Projective Planes”. In: *Canadian Journal of Mathematics vol. 9* (1957), pp. 378–388.

[28] Daniel R. Hughes and Fred C. Piper. *Projective Planes.* Springer, 1973.

[29] Norman Lloyd Johnson, Vikram Jha, and Mauro Biliotti. *Handbook of Finite Translation Planes.* Chapman and Hall/CRC, 2007.

[30] Dieter Jungnickel and Marialuisa J. de Resmini. “Another case of the prime power conjecture for finite projective planes”. In: *Advances in Geometry vol. 2* (2002), pp. 215–218.

[31] Clement Wing Hong Lam. “The Search for a Finite Projective Plane of Order 10”. In: *The American Mathematical Monthly vol. 98 no. 4* (1991), pp. 305–318.

[32] Clement Wing Hong Lam, Galina Kolesova, and Larry Thiel. “A computer search for finite projective planes of order 9”. In: *Discrete Mathematics vol. 92* (1991), pp. 187–195.

[33] Eric S. Lander. *Symmetric Designs: An Algebraic Approach.* Cambridge University Press, 1983.

[34] Hanfried Lenz. “Kleiner Desarguesscher Satz und Dualität in projektiven Ebenen”. In: *Jahresbericht der Deutschen Mathematiker-Vereinigung vol. 57* (1954), pp. 20–31.

[35] William Judson LeVeque. *Topics in number theory vol. 1.* 3rd ed. 2 vols. Addison-Wesley Publishing Company, 1965.

[36] Heinz Lüneburg. “Characterizations of the Generalized Hughes Planes”. In: *Canadian Journal of Mathematics vol. 28* (1976), pp. 376–402.

[37] Rudolf Mathon. “On a new projective plane of order 16”. In: *Second International Conference in Deinze.* Unpublished talk. 1992.

[38] Rudolf Mathon and Gordon F. Royle. “The translation planes of order 49”. In: *Designs, Codes and Cryptography vol. 5* (1995), pp. 57–72.

[39] Arnold Meyer. “Mathematische Mittheilungen”. In: *Vierteljahrschrift der Naturforschenden Gesellschaft in Zürich vol. 29* (1884), pp. 209–222.

[40] G. Eric Moorhouse. “On projective planes of order less than 32”. In: *Finite Geometries, Groups, and Computation.* De Gruyter, 2006, pp. 149–162.

[41] G. Eric Moorhouse. *Projective Planes of Order 16.* 2010. URL: `https://www.ericmoorhouse.org/pub/planes16/`.

[42] G. Eric Moorhouse. *Projective Planes of Small Order.* 2000. URL: `https://www.ericmoorhouse.org/pub/planes/`.

[43] G. Eric Moorhouse. “Reconstructing projective planes from semibiplanes”. In: *Coding Theory and Design Theory, Part II: Design Theory.* 1990, pp. 280–285.

[44] OEIS Foundation Inc. *The On-Line Encyclopedia of Integer Sequences. Entry A046712.* 2020. URL: `https://oeis.org/A046712`.

[45] Theodore Gleason Ostrom. “Finite Planes With a Single (p, L) Transitivity”. In: *Archiv der Mathematik vol. 15* (1964), pp. 378–384.

[46] Theodore Gleason Ostrom. “Semi-translation planes”. In: *Transactions of the American Mathematical Society vol. 111 no. 1* (1964), pp. 1–18.

[47] Theodore Gleason Ostrom. “Vector spaces and construction of finite projective planes”. In: *Archiv der Mathematik vol. 19* (1968), pp. 1–25.

[48] Luigi Antonio Rosati. “Su una nuova classe di piani grafici”. In: *Ricerche Mat vol. 13* (1964), pp. 39–55.

[49] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.0).* 2020. URL: `https://www.sagemath.org`.

[50] James Singer. “A Theorem in Finite Projective Geometry and Some Applications to Number Theory”. In: *Transactions of the American Mathematical Society vol. 43* (1938), pp. 377–385.

[51] Jill C. D. Spencer. “On the Lenz-Barlotti Classification of Projective Planes”. In: *The Quarterly Journal of Mathematics vol. 11* (1960), pp. 241–257.

[52] Karl Georg Christian von Staudt. *Beiträge zur Geometrie der Lage.* Korn, 1856, pp. 86–91.

[53] Gaston Tarry. “Le Probléme de 36 Officiers”. In: *Compte Rendu de l’Association Française pour l’Avancement des Sciences vol. 2* (1901), pp. 170–203.

[54] Vladimir D. Tonchev. “Quasi-symmetric 2-(31,7,7) designs and a revision of Hamada’s conjecture”. In: *Journal of Combinatorial Theory, Series A vol. 42* (1986), pp. 104–110.

[55] Oswald Veblen and William Henry Bussey. “Finite projective geometries”. In: *Transactions of the American Mathematical Society vol. 7* (1906), pp. 241–259.

[56] Asher Wagner. “On finite affine line transitive planes”. In: *Mathematische Zeitschrift vol. 87* (1965), pp. 1–11.

[57] Mingchun Xu. “A Computer Search for a Projective Plane of Order 12”. In: *2019 International Conference on Machine Learning, Big Data and Business Intelligence (MLBDBI).* 2019, pp. 5–8.

[58] Mingchun Xu. “The properties of the bordered matrix of symmetric block design”. In: *arXiv: General Mathematics* (2017). URL: https://arxiv.org/abs/1707.02208.

[59] Hans Zassenhaus. “Über endliche Fastkörper”. In: *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg vol. 11* (1935), pp. 187–220.