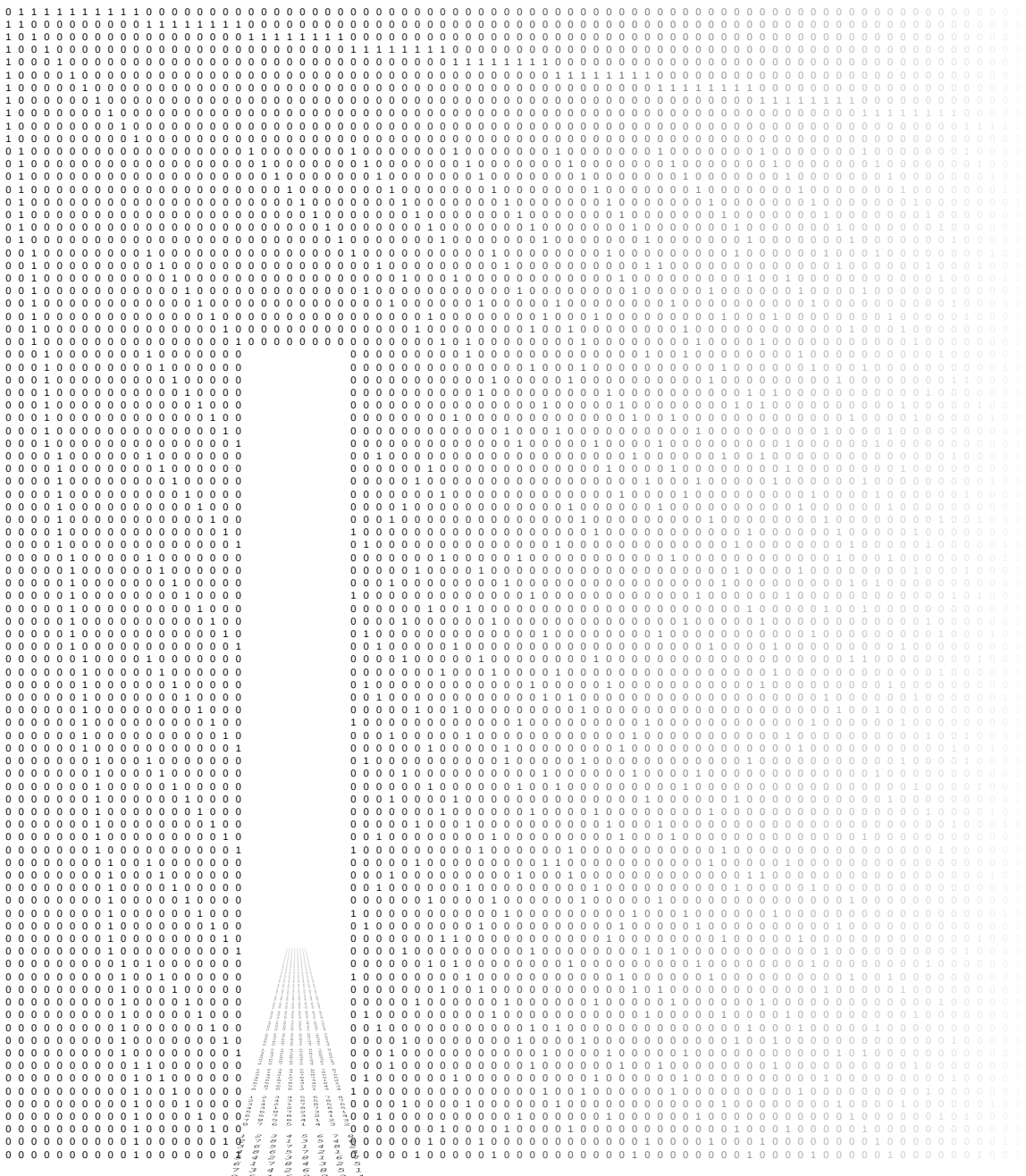
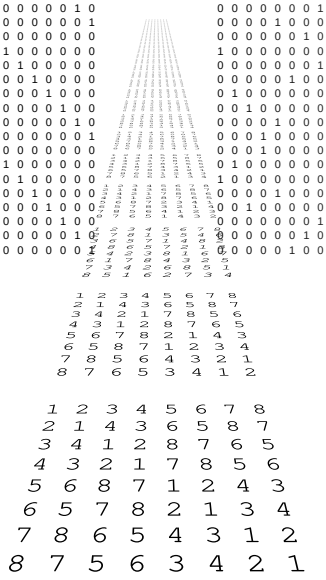
Generating Finite Projective Planes from Non-Paratopic Latin Squares



Marcel J.G. Gorissen



Generating Finite Projective Planes

from

Non-Paratopic Latin Squares

Marcel J.G. Gorissen

Januari 2007
Thesis Supervisor: dr. W. Bosma
Second Reader: prof. A. van Rooij
Radboud University Nijmegen
Faculteit Natuurwetenschappen, Wiskunde en Informatica
IMAPP Computer Algebra
Toernooiveld 1
6525 ED Nijmegen

To my parents

Preface

This thesis marks the end of an era. After having been a student for nearly a decade, the time has come to move on.

While I was preparing for my last exams in August, it became clear to me that I wanted to graduate in computer algebra under the supervision of dr. W. Bosma. The subject of finite projective planes was by far the most appealing of three possibilities. It was the article "A Computer Search for Finite Projective Planes of Order 9"[11] by C.W.H. Lam et al. that drew my attention and acted as fuel for this thesis. The main subject of this thesis is the generation of all non-isomorphic finite projective planes of arbitrary order n, by means of non-paratopic Latin squares of order $n-1$. For me, this has turned out to be feasible up to finite projective planes of order 8.

The past five months, though sometimes hectic, have been very satisfying. They have left me with an eagerness towards learning and understanding new things and also helped me grow into my role of a young professional. Many people helped me during this transition, to whom I want to express my gratitude. Some of them have played such an important role that they deserve some words here.

Wieb Bosma was my thesis supervisor and his office is only three meters from my working space, as he is now well aware. On an average day I would barge in at least five times and harass him with new ideas, computer outputs, bad jokes, or my craving for espresso. On these occasions Wieb was always patient, enthusiastic and ready for a 'shot'. Most of all, he had great confidence in me, for which I am grateful.

I would like to thank prof. A. van Rooij for being my second reader, a sounding board and a friendly and inspiring person.

Daan Wanrooy is a LaTeX oracle and a loyal friend, he has become like a brother to me. Thanks for everything, Daan.

I thank Willy and Trees for all they have done for me and my fellow students.

This thesis is dedicated to my parents, who have always believed in me and made me feel loved; no words can express my gratitude towards them, so I will keep it simple. Thank you.

Last, but certainly not least, I thank my girlfriend and soul-mate Maartje. You bring out the best in me.
Thank you with a big L.

December 2006 *Marcel Gorissen*

Contents

Preface **v**

Introduction **1**

1 Finite Projective Planes **3**
1.1 Introduction . . . 3
1.2 Finite Projective Planes . . . 3
1.3 Survey/Overview . . . 10
1.4 Constructions . . . 12
1.5 Stating my Goal . . . 14

2 Latin Squares **15**
2.1 Introduction . . . 15
2.2 Latin Squares . . . 15
2.3 Transversals . . . 17
2.4 Constructing an Invariant . . . 20
2.5 Generating Representatives . . . 23

3 Exhaustive Searching for Planes **25**
3.1 Introduction . . . 25
3.2 The Partial Incidence Matrix . . . 25
3.3 Paratopic Squares vs. Isomorphic Planes . . . 28
3.4 Backtracking . . . 30
3.5 Results . . . 34

A Encore: Fingerprinting **41**

B Magma Code **45**

C Data **51**

Bibliography **53**

List of Notations **55**

Index **57**

Introduction

The subjects of finite projective planes and Latin squares have a lot of similarities. The first of these similarities is the age; both are hundreds of years old. The second is their beauty; Latin squares and finite projective planes are relatively easy to define and comprehend, but the many questions they give rise to are often difficult to answer. Furthermore, for both subjects, there exists a growing number of open problems, some of which are almost as old as the subject itself. Finally, the subjects of Latin squares and finite projective planes are strongly connected to each other as well as to many other mathematical subjects. These subjects include the theory of quasi-groups and loops, difference sets, nets, combinatorial designs, error-correcting codes and finite fields. We will be exploring the connection between classes of paratopic Latin squares and classes of isomorphic finite projective planes.

In Chapter 1 we explore the subject of finite projective planes. We give some relevant definitions and properties, and define isomorphism between finite projective planes. Then we give a short survey of the progress made in this field and give constructions for the finite projective planes of order 9. In the final section of Chapter 1, we state the goal of this thesis, which is to review, understand, reproduce, generalize and perhaps even improve Lam's method [11] for an exhaustive search for all classes of isomorphic finite projective planes of order 9.

Chapter 2 is on Latin squares. The important concept of transversals is explored and equivalences are treated. An invariant for Latin squares under paratopy is constructed and with this, a method for generating a representative Latin square for each main class is explained.

In the third and final chapter, we reveal a beautiful correspondence between Latin squares of order $n-1$ and finite projective planes of order n. Using a backtrack program, we generate all finite projective planes of order less than 9 by means of this correspondence.

As an encore, the fingerprint invariant for finite projective planes is given in Appendix A. Some of the more relevant programs used and other data can be found in the appendices as well.

Chapter 1

Finite Projective Planes

Summary

We define finite projective planes and describe properties such as duality and isomorphism. A short survey is given on related findings from the past century and we give constructions for the four 'distinct' finite projective planes of order 9*. The goal of this thesis is formulated in the final section of this chapter.*

1.1 Introduction

Well over 2000 years ago, Euclid wrote his Elements, in which he attempted to deductively organize mathematics. He axiomatized plane geometry by five well known postulates of which four seem obvious. The fifth postulate in its best known form (Playfair's Axiom) states that for every line and every point not on this line, there exists a unique line parallel to the given line and passing through the given point. For years, people have tried to deduce this fifth postulate from the other four, but failed. The reason they all failed was that it cannot be deduced.

In the beginning of the nineteenth century, mathematicians realized that consistent geometries could be created in which Euclid's fifth postulate does not hold. This was the birth of non-Euclidean geometry, the study of consistent geometries with a set of postulates different from Euclid's. One of these non-Euclidean geometries has been developed by the German mathematician Bernhard Riemann. In this geometry there exist no parallel lines. We will work with planes in such a geometry, the so-called projective planes.

1.2 Finite Projective Planes

A plane can intuitively be seen as a set of points and a set of lines which are related in some way. We will use lower-case letters for points (usually

p, q, r, s, a, b, c, d) and denote the set of points by $\mathcal{P}$. Lines will be denoted by capital letters (usually L, M, N) and the set of lines will be denoted by $\mathcal{L}$. All we need now is a relation between the points and the lines. For this we will use the incidence set $\mathcal{I}$. The incidence set $\mathcal{I}$ will be a subset of $\mathcal{P} \times \mathcal{L}$ and the pair (p, L) will be an element of $\mathcal{I}$ if and only if p and L are incident. Being incident in this context means that the point p "lies on" the line L and the line L "passes through" the point p. Furthermore, we will assume that a line is not a point and vice versa. Thus $\mathcal{P} \bigcap \mathcal{L} = \varnothing$. Now a proper definition of a plane can be given.

Definition 1 A *plane* Σ is a triple $(\mathcal{P}, \mathcal{L}, \mathcal{I})$ such that $\mathcal{P}, \mathcal{L}$ and $\mathcal{I}$ are sets, $\mathcal{P} \bigcap \mathcal{L} = \varnothing$, $\mathcal{P} \bigcup \mathcal{L} \neq \varnothing$, and $\mathcal{I} \subseteq \mathcal{P} \times \mathcal{L}$.

We defined that a point p and a line L are incident if and only if $(p, L) \in \mathcal{I}$, but we will more often use the phrases "p lies on L" and "L passes through p" in this case.

Definition 2 Two or more points are *collinear* when they lie on a common line. Two or more lines are *concurrent* when they pass through a common point.

Definition 3 Two lines L and M are *parallel* when they are not concurrent.

Definition 4 If p, q, r, s are four points no three of which are collinear, then the quadruple p, q, r, s is called a *four-point*.

We now have a large enough vocabulary for the definition of a projective plane. Equivalent definitions will be omitted here, because they are of little relevance for this thesis. We will mention only the best known alternative definition here, which is that projective planes arise from the addition of a special line at infinity to an affine plane, in which parallel lines exist. The formal definition we will use is the following.

Definition 5 A *projective plane* π is a plane $(\mathcal{P}, \mathcal{L}, \mathcal{I})$ such that

P1: There is a unique line passing through two given points.

P2: There is a unique point lying on two given lines.

P3: There exist four distinct points, no three of which lie on the same line (i.e. there exists a four-point).

It can be shown that the postulates P1, P2 and P3 imply the following redundant postulate (P4).

(P4): There exist four distinct lines, no three of which pass through the same point.

Notice that interchanging the words "point(s)" by "line(s)" and "lie on" by "pass through" and "lying on" by "passing through" in the definition of a projective plane gives exactly the same postulates (albeit in a different order). This phenomenon is called *duality*.

Duality is a principle often used in mathematics and it has many applications. In this case, a consequence of duality is that the logical values of a proper statement and its dual statement are the same. We will use it to prove the following theorem which shows that in a projective plane, the number of lines passing through an arbitrary point equals the number of points lying on an arbitrary line.

In projective planes, every two points p, q lie on a unique line, which we will denote by pq or qp.

Theorem 1 *Let p and p' be two points and let L and L' be two lines of a projective plane π. Then there exist bijections between the points on L and the points on L', between the lines through p and the lines through p', and between the points on L and the lines through p.*

Proof. Let L and L' be two distinct lines of a projective plane π. There exists a point r of π not on L or L'. (For if all points of π are on L or L', then there are points a, b on L and points c, d on L' such that a, b, c, d is a four-point. But this implies that the lines ac and bd pass through a common point not on L or L'). Now from this point r we may establish a bijection between the points on L and the points on L'. For if p is a point on L, then the unique line rp passes through a unique point p' on L'. This mapping is a bijection between all points on L and all points on L'.

Note that the second assertion of the theorem is the dual of the first one. We know that the principle of duality holds for the class of projective planes, so the second assertion of the theorem holds also.

Now for the third assertion let r be a point of π not on L. Then there is a bijection between the points on L and the lines through r by definition. This is also valid if the point is on L because of the second assertion of the theorem. □

Note that it follows from the proof of Theorem 1 that at least three distinct points are on each line of π and at least three distinct lines pass through each point of π. We will prove that when there are a finite number of points on a line of a projective plane, this number determines the number of points on any line, the number of lines through any point and the number of lines and points of a projective plane completely.

Definition 6 A *finite projective plane* is a projective plane $(\mathcal{P}, \mathcal{L}, \mathcal{I})$ for which $\mathcal{P} \bigcup \mathcal{L}$ is finite.

Let $n \in \{2, 3, \ldots\}$ and let L be a line of the finite projective plane π with exactly $n+1$ points on it. It follows from Theorem 1 that each line of π has also exactly $n+1$ points on it and each point of π lies on exactly $n+1$ lines.

Definition 7 For a finite projective plane π with a line L on which there lie exactly $n+1$ points, the *order* of the finite projective plane π is defined as the integer n.

Theorem 2 *Let π be a finite projective plane of order n. Then the total number of points on an arbitrary line of π as well as the total number of lines through an arbitrary point of π equals $n+1$. Moreover, π has a totality of n^2+n+1 points and n^2+n+1 lines.*

Proof. The first assertion of the theorem follows immediately from Theorem 1 and the definition of order.

Let p be a point of π. Then there are exactly $n+1$ lines through p and there are exactly n points on each of these lines in addition to p. Hence π has a totality of $n(n+1)+1 = n^2+n+1$ points.

The dual statement gives us that π has a totality of n^2+n+1 lines. □

Theorem 3 *The following statements are equivalent for $n \geq 2$:*

i) π is a finite projective plane of order n.

ii) π is a plane in which:

- *Every line contains $n+1$ points.*
- *Every point lies on $n+1$ lines.*
- *Any two distinct lines intersect in exactly one point.*
- *Any two distinct points lie on exactly one line.*

Proof. The equivalence follows easily from the definitions and Theorem 2. □

An alternative and very useful way to represent a finite projective plane π is by means of an incidence matrix A_π. This is a square $(0,1)$-matrix[1] of which the rows correspond to the lines and the columns correspond to the points of π. The entry $(A_\pi)_{ij}$ is 1 if and only if point j is on line i. This representation depends on a chosen numbering of the lines and points of π. When we speak of *the* incidence matrix A_π of a finite projective plane π, we assume a fixed numbering. Further on, it will become clear that different numberings result in isomorphic planes.

[1] A matrix over $\mathbb{Z}$ with only entries 0 and 1.

The following theorem gives the connection between a finite projective plane π and the incidence matrix A_π. Here we use the word *weight* for the number of 1's in a row or a column. The inner product is the standard inner product for row or column vectors over $\mathbb{Q}$.

Theorem 4 *A finite projective plane π has order n if and only if its incidence matrix A_π is a square matrix of size n^2+n+1, all columns and rows of A_π have weight $n+1$ and the inner product of any two distinct rows or any two distinct columns in A_π is 1.*

Proof. The proof follows easily from the definitions. □

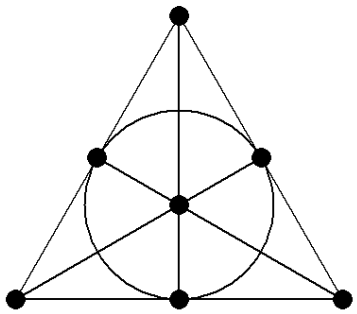


Figure 1.1: *The finite projective plane of order 2, the Fano plane.*

An easy way to verify that an arbitrary square $(0,1)$-matrix of size n^2+n+1 is an incidence matrix of a finite projective plane is given by the following theorem. In the proof we will use Theorem 13 which will be proved in Chapter 3.

Theorem 5 *Let A be a square $(0,1)$-matrix of size n^2+n+1, where $n \geq 2$. Then A is the incidence matrix of a finite projective plane of order n if and only if $AA^T = nI+J$ where I and J are the identity matrix of size n^2+n+1 and the all-ones matrix of size n^2+n+1 respectively.*

Proof. Suppose A is a square $(0,1)$-matrix of size n^2+n+1, where $n \geq 2$ and A is the incidence matrix of a finite projective plane of order n. Let $1 \leq i,j \leq n^2+n+1$. Rows i and j of A have inner product 1, so $(AA^T)_{ij} = 1$ if $i \neq j$. The inner product of a row of A with itself is $n+1$, so $(AA^T)_{ii} = n+1$ for $1 \leq i \leq n^2+n+1$. Hence $AA^T = nI+J$.

Suppose A is a square $(0,1)$-matrix of size n^2+n+1, where $n \geq 2$ and $AA^T = nI+J$. From this equality we have that the inner product of any row of A with itself is $n+1$ which can only mean that it contains $n+1$ ones.

Also, the inner product of any two distinct rows of A is 1. By the dual of Theorem 13 we find that each column of A contains exactly $n+1$ ones and the inner product of any two distinct columns is exactly 1. Hence A is the incidence matrix of a finite projective plane of order n. □

$$\begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Figure 1.2: *An incidence matrix of the Fano plane.*

We earlier mentioned and used the principle of duality, but have not yet formally defined the dual of a plane. We will do this here.

Definition 8 Let $\Sigma = (\mathcal{P}, \mathcal{L}, \mathcal{I})$ be a plane. Then the triple $(\mathcal{L}, \mathcal{P}, \mathcal{I}^{-1})$ (where $\mathcal{I}^{-1} = \{(L, p) : (p, L) \in \mathcal{I}\}$) is called the *dual plane* of Σ. We denote this by Σ^d.

The dual π^d of a finite projective plane π can very easily be given if you have an incidence matrix A_π of the plane π. By interchanging the roles of points and lines, we interchange the roles of the columns and rows of A_π. Thus the finite projective plane π^d is the plane with incidence matrix A_π^T.

By now, the question arises whether or not for every order n there exists such a finite projective plane. Furthermore, if a finite projective plane does exist for certain order, is it the only one? We will therefore need a way to determine if two finite projective planes are 'different' or 'alike' in some sense. For this purpose we introduce the mathematical property of isomorphism.

Definition 9 Finite projective planes $\pi = (\mathcal{P}, \mathcal{L}, \mathcal{I})$ and $\pi' = (\mathcal{P}', \mathcal{L}', \mathcal{I}')$ are *isomorphic* if and only if there exist mappings f and F such that f is a bijection between $\mathcal{P}$ and $\mathcal{P}'$, F is a bijection between $\mathcal{L}$ and $\mathcal{L}'$, and $(p, L) \in \mathcal{I}$ if and only if $(f(p), F(L)) \in \mathcal{I}'$.

We indicate the fact that two planes π and π' are isomorphic by writing $\pi \sim \pi'$. The isomorphism is the ordered pair (f, F). We can also formulate an equivalent definition of isomorphism using only one map f mapping the points of π onto the points of π'.

Remark 1 Let π and π' be finite projective planes. There exists a bijective mapping f between $\mathcal{P}$ and $\mathcal{P}'$ preserving collinearity if and only if π and π' are isomorphic.

It is immediately clear that the relabeling of points and lines in a finite projective plane correspond to row and column permutations in the incidence matrix. Therefore, two finite projective planes are isomorphic when their incidence matrices can be transformed into each other by row and column permutations. If a finite projective plane is isomorphic to its dual plane, it is called *self-dual*.

It follows that a finite projective plane is self-dual if its incidence matrix can be transformed into a symmetric incidence matrix by row and column permutations.

The Fano plane as given in figure 1.1 on page 7 and figure 1.2 on page 8 is self-dual, because mirroring the incidence matrix in the fourth row (which just takes some row permutations) gives a symmetric incidence matrix. Figure 1.3 and figure 1.4 show two more self-dual finite projective planes.

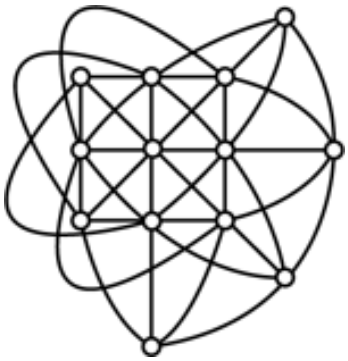


Figure 1.3: *The finite projective plane of order* 3.

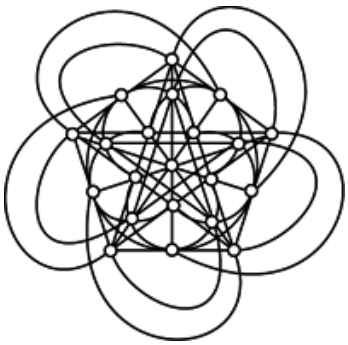


Figure 1.4: *The finite projective plane of order* 4.

1.3 Survey/Overview

In 1899, David Hilbert was one of the first to coordinatize finite projective geometries by means of vector spaces over finite fields. By means of this coordinatization for every finite field of order q, a finite projective plane of order q can be constructed. Due to this construction an infinite family of finite projective planes of any prime power order is known. These are the *Desarguesian*[2] or so-called classical finite projective planes.

One year later, in 1900, a French amateur mathematician named Gaston Tarry proved that there does not exist a pair of orthogonal Latin squares of order 6. The non-existence of such a pair strengthened the conjecture, made by Leonhard Euler in 1782, stating that there exists no pair of orthogonal Latin squares of order n if $n \equiv 2 \bmod 4$. The importance of Tarry's work and Euler's conjecture for the theory of finite projective planes will become clear in a moment.

Using the algebraic constructions of Leonard Dickson in 1905, Oswald Veblen and Joseph Wedderburn were the first to create non-Desarguesian finite projective planes in 1907. Similar algebraic ideas have resulted in the discovery of more finite projective planes over the years, among which were the three non-Desarguesian planes of order 9. These are the *left nearfield* plane, the *right nearfield* plane and the *Hughes* plane, which will be constructed in the following section.

In 1938, the connection between Latin squares and finite projective planes was made. It was the Indian Raj Chandra Bose who proved that there exists a finite projective plane of order $n \geq 2$ if and only if there exists a complete set of $n-1$ mutually orthogonal Latin squares of order n. Together with Tarry's result, this proves the non-existence of a finite projective plane of order 6. If Euler's conjecture were true, Bose's theorem would also prove the non-existence of finite projective planes with orders $n = 10, 14, 18, 22, \ldots$.

In 1949, an important step was made by Richard Bruck and Herbert Ryser. Together they showed that a finite projective plane of order $n \equiv 1, 2 \bmod 4$ can only exist if n is the sum of two integer squares. This theorem only leaves a small, but infinite set of orders we know nothing about.

Ten years later, in 1959, Bose and Sharad-Chandra S. Shrikhande disproved Euler's conjecture by finding a pair of orthogonal Latin squares of order 22. Later that same year, Ernest Tilden Parker found a pair of orthogonal Latin squares of order 10 and together with Bose and Shrikhande he proved that Euler's conjecture was false for all $n > 6$.

After Clement Lam had shown in 1988 that the four finite projective planes of order 9 are the only ones, he announced his proof of the non-

[2]Desarguesian planes satisfy Desargues' Theorem. Planes satisfying this theorem contain a Desargues configuration, which has 10 points and lines, and every point lies on 3 lines and on every line are 3 points.

existence of a finite projective plane of order 10 in 1989. In both cases he used supercomputers for his computations.

Table 1.1 gives the number of finite projective planes (up to isomorphisms) of small order, as far as we know them.

order n	relevant decomposition	# of planes of order n up to isomorphism	important contributors
2	2^1	1	–
3	3^1	1	–
4	2^2	1	–
5	5^1	1	–
6	2 mod 4	0	Bose,Tarry[16]
7	7^1	1	–
8	2^3	1	–
9	3^2	4	Lam-Kolesova-Thiel[11]
10	$1^2 + 3^2 \equiv 2 \bmod 4$	0	Lam-Thiel-Swiercz[10]
11	11^1	≥ 1	–
12	–	≥ 0	–
13	13^1	≥ 1	–
14	2 mod 4	0	Bruck-Ryser[1][14]
15	–	≥ 0	–
16	2^4	≥ 22	Dempwolff-Reifart
17	17^1	≥ 1	–
18	$3^2 + 3^2 \equiv 2 \bmod 4$	≥ 0	–
19	19^1	≥ 1	–
20	–	≥ 0	–
21	1 mod 4	0	Bruck-Ryser[1][14]
22	2 mod 4	0	Bruck-Ryser[1][14]
23	23^1	≥ 1	–
24	–	≥ 0	–
25	5^2	≥ 193	Czerwinski-Oakden
26	$1^2 + 5^2 \equiv 2 \bmod 4$	≥ 0	–
27	3^3	≥ 13	Dempwolff
28	–	≥ 0	–
29	29^1	≥ 1	–
30	2 mod 4	0	Bruck-Ryser[1][14]
31	31^1	≥ 1	–

Table 1.1: *The number of finite projective planes of small order.*

1.4 Constructions

In this section we will give constructions for the four finite projective planes of order 9. We will not prove that they are indeed finite projective planes, for it is a tedious work which brings no greater understanding of the subject. In fact, this entire section can be skipped as it is not essential for the rest of this thesis and is given here for the sake of completeness.

The first construction gives us the Desarguesian plane and can easily be generalized for all prime power orders.

Constructing π_{F_9}

π_{F_9} is the Desarguesian finite projective plane of order 9. It can be constructed from a field with 9 elements.
We form the plane π_{F_9} as follows:

$$\begin{aligned}
\mathcal{P} &= \{[x,y,z] : x,y,z \in \mathbb{F}_9 \text{ and not } x=y=z=0\} \text{ where} \\
&\quad [x,y,z] = [x',y',z'] \iff \exists r \in \mathbb{F}_9^* \text{ such that } x = rx', y = ry', z = rz'. \\
\mathcal{L} &= \{\langle a,b,c\rangle : a,b,c \in \mathbb{F}_9 \text{ and not } a=b=c=0\} \text{ where} \\
&\quad \langle a,b,c\rangle = \langle a',b',c'\rangle \iff \exists s \in \mathbb{F}_9^* \text{ such that } a = sa', b = sb', c = sc'. \\
\mathcal{I} &\ni ([x,y,z],\langle a,b,c\rangle) \iff ax+by+cz = 0.
\end{aligned}$$

Constructing π_{H_9}

This plane π_{H_9} is usually referred to as the "Hughes plane" of order 9.
We construct the plane π_{H_9} as follows:

$$\begin{aligned}
\mathcal{P} &= \{a_i, b_i, c_i, d_i, e_i, f_i, g_i : i = 0, \ldots, 12\} \\
\mathcal{L} &= \{L_i : i = 0, \ldots, 90\} \text{ where :} \\
L_{7i} &= \{a_i, a_{i+3}, a_{i+4}, a_{i+11}, b_i, c_i, d_i, e_i, f_i, g_i\} \\
L_{7i+1} &= \{a_i, b_{i+1}, b_{i+6}, b_{i+12}, e_{i+4}, e_{i+5}, f_{i+3}, f_{i+7}, g_{i+8}, g_{i+11}\} \\
L_{7i+2} &= \{a_i, c_{i+1}, c_{i+6}, c_{i+12}, g_{i+4}, g_{i+5}, e_{i+3}, e_{i+7}, f_{i+8}, f_{i+11}\} \\
L_{7i+3} &= \{a_i, d_{i+1}, d_{i+6}, d_{i+12}, f_{i+4}, f_{i+5}, g_{i+3}, g_{i+7}, e_{i+8}, e_{i+11}\} \\
L_{7i+4} &= \{a_i, e_{i+1}, e_{i+6}, e_{i+12}, b_{i+4}, b_{i+5}, c_{i+3}, c_{i+7}, d_{i+8}, d_{i+11}\} \\
L_{7i+5} &= \{a_i, f_{i+1}, f_{i+6}, f_{i+12}, d_{i+4}, d_{i+5}, b_{i+3}, b_{i+7}, c_{i+8}, c_{i+11}\} \\
L_{7i+6} &= \{a_i, g_{i+1}, g_{i+6}, g_{i+12}, c_{i+4}, c_{i+5}, d_{i+3}, d_{i+7}, b_{i+8}, b_{i+11}\} \\
\mathcal{I} &= \{(p,L) : p \in \mathcal{P}, L \in \mathcal{L} \text{ and } p \in L\}
\end{aligned}$$

Constructing π_{N_9}

The right nearfield plane π_{N_9} is occasionally referred to as the Veblen-Wedderburn plane of order 9 since the right nearfield $(N_9, +, \cdot)$ it is related to is a Veblen-Wedderburn system. The right nearfield satisfies all field axioms, except for the *left* distributivity and commutativity of the multiplication. Table 1.2 gives the addition (which is the same as for $\mathbb{F}_9$) and the multiplication in this right nearfield where $N_9 = \{0, 1, 2, a, b, c, d, e, f\}$.

$+$	0	1	2	a	b	c	d	e	f
0	0	1	2	a	b	c	d	e	f
1	1	2	0	b	c	a	e	f	d
2	2	0	1	c	a	b	f	d	e
a	a	b	c	d	e	f	0	1	2
b	b	c	a	e	f	d	1	2	0
c	c	a	b	f	d	e	2	0	1
d	d	e	f	0	1	2	a	b	c
e	e	f	d	1	2	0	b	c	a
f	f	d	e	2	0	1	c	a	b

$\cdot$	0	1	2	a	b	c	d	e	f
0	0	0	0	0	0	0	0	0	0
1	0	1	2	a	b	c	d	e	f
2	0	2	1	d	f	e	a	c	b
a	0	a	d	2	e	b	1	f	c
b	0	b	f	c	2	d	e	a	1
c	0	c	e	f	a	2	b	1	d
d	0	d	a	1	c	f	2	b	e
e	0	e	c	b	d	1	f	2	a
f	0	f	b	e	1	a	c	d	2

Table 1.2: *Addition and multiplication in the right nearfield.*

The right nearfield plane of order 9 can now be constructed in the following manner:

$$\begin{aligned}
\mathcal{P} &= \{[x, y, 1] : x, y \in N_9\} \cup \{[1, x, 0] : x \in N_9\} \cup \{[0, 1, 0]\} \\
\mathcal{L} &= \{\langle m, 1, k\rangle : m, k \in N_9\} \cup \{\langle 1, 0, k\rangle : k \in N_9\} \cup \{\langle 0, 0, 1\rangle\} \\
\mathcal{I} &= \{([x, y, z], \langle m, n, k\rangle) : xm + yn + zk = 0\}
\end{aligned}$$

Constructing $\pi_{N_9'}$

The plane $\pi_{N_9'}$ is the left nearfield plane of order 9. The construction is the same as for the right nearfield plane except that it is constructed over a left nearfield in which the multiplication does not satisfy *right* distributivity and commutativity.

This left nearfield is isomorphic to the dual of the right nearfield, which is not self-dual. Therefore, dualization of the right nearfield plane is another way of constructing a plane isomorphic to the left nearfield plane.

1.5 Stating my Goal

In their paper "A computer search for finite projective planes of order 9" [11] dating from 1991, Lam, Kolesova and Thiel reported on their exhaustive search for finite projective planes of order 9. By means of a computer search they showed that every finite projective plane of order 9 is isomorphic to one of the four known planes of order 9. Their search started by generating all $283,657$ non-isomorphic Latin squares of order 8. They showed that each Latin square determines 27 columns of the incidence matrix which they first tried to complete to 40 columns. Only 21 of these $283,657$ partial incidence matrices could be completed to 40 columns, which gave rise to 326 matrices of 40 columns and 91 rows. 325 of these matrices could be completed to a 91×91 incidence matrix of a finite projective plane of order 9. They compared the these planes with the four known planes and found no new ones. Furthermore, they gave evidence for the correctness of their methods and programs.

The goal I set myself was to review, understand, reproduce, generalize and perhaps even improve this method.

Actually, the paper that drew my attention to finite projective planes was another publication by C.W.H. Lam, the celebrated article "The search for a finite projective plane of order 10" [10]. In this paper he describes the search for a finite projective plane of order 10, and how he proved[3] after years of heavy computing on supercomputers that such a plane does not exist. Despite the excellent exposition, the method used in the article gives no clear leads on how to reproduce his findings. The main reason for this is that many computations have been done by different persons spread over many years. Lam's article [11] concerning the planes of order 9 did give some leads on how to arrange a search method on the one hand, but left enough space for my own ideas on the other. This has resulted in the re-invention of the wheel on several occasions, but also in my own optimized program which, in principle[4], can handle every order n.

[3] This is not a proof in the traditional mathematical sense. It is impossible for any human to check all the calculations. Furthermore, programming mistakes are easily made and untraceable random computing errors are likely to occur during such long computations.

[4] Given enough time and computational power.

Chapter 2

Latin Squares

Summary

In this chapter we explore Latin squares, using two different representations, and define equivalence relations between them. We define transversals and use these to construct an invariant for Latin squares under paratopy. With this invariant we generate a list of representative Latin squares.

2.1 Introduction

The subject of Latin squares is already very old and there are many unsolved problems concerning them. The name Latin square dates from the time of Euler, of whom we will tell more in one of the following sections. The mathematical attention for Latin squares has increased a lot in the past century, because of the realization of connections with many branches of mathematics. Practical applications such as the formation of statistical designs and the construction of error-correcting codes have given this attention an extra impulse. The reason for us to study them, is the remarkable way they appear in incidence matrices of finite projective planes.

2.2 Latin Squares

Definition 10 A *Latin square* of order n is an n-by-n array L with the property that each row and each column contains each of the symbols $1, 2, \ldots, n$ exactly once.

A Latin square is said to be a *reduced* Latin square when the symbols in the first row and in the first column appear in natural order. Sometimes we will not use the above defined square representation for Latin squares, but work with the *orthogonal array representation* which is defined as the set of n^2 ordered triples (i, j, L_{ij}) with $1 \leq i, j \leq n$ and $L_{ij} \in \{1, \ldots, n\}$.

$$\begin{bmatrix} 2 & 4 & 3 & 1 \\ 1 & 2 & 4 & 3 \\ 3 & 1 & 2 & 4 \\ 4 & 3 & 1 & 2 \end{bmatrix} \qquad \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \\ 3 & 1 & 4 & 2 \\ 4 & 3 & 2 & 1 \end{bmatrix}$$

$$\{(1,1,2),(1,2,4),(1,3,3),(1,4,1),(2,1,1),(2,2,2),(2,3,4),(2,4,3),$$
$$(3,1,3),(3,2,1),(3,3,2),(3,4,4),(4,1,4),(4,2,3),(4,3,1),(4,4,2)\}$$

Figure 2.1: *A Latin square, a reduced Latin square and an orthogonal representation of the first.*

It is easily seen that swapping some rows in a Latin square will again result in a Latin square. This property also holds for swapping columns and swapping symbols. Latin squares that can be transformed into each other by permuting rows, permuting columns and permuting symbols are equivalent in some sense. Let us formalize this property.

Definition 11 Two Latin squares are said to be *isotopic* if one can be transformed into the other by rearranging rows, rearranging columns and permuting symbols. These $n!^3$ operations are called *isotopies* or *isotopy operations* and this isotopic relation divides the Latin squares into equivalence classes, called the *isotopy classes*.

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 5 & 1 & 4 \\ 3 & 5 & 4 & 2 & 1 \\ 4 & 1 & 2 & 5 & 3 \\ 5 & 4 & 1 & 3 & 2 \end{bmatrix} \qquad \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 3 & 1 \\ 3 & 5 & 2 & 1 & 4 \\ 4 & 3 & 1 & 5 & 2 \\ 5 & 1 & 4 & 2 & 3 \end{bmatrix}$$

Figure 2.2: *Two isotopic reduced Latin squares.(permute row 2 and 3, column 2 and 3, symbol 2 and 3).*

Transposing is an operation which has a similar effect on Latin squares. It will always result in a Latin square. Taking a closer look at this transpose operation reveals us that nothing really happened to the square, except for rows and columns changing roles. Translating this to a Latin square in the orthogonal array representation, we see that for every triple in it, the first and second element have been permuted. More generally, permuting the three elements in a triple and permuting all the other triples in the same way, yields a Latin square. These 3! operations (including the identity) merge isotopy classes into even larger classes called *main classes*. These operations are called the *conjugacy operations* and two squares from the same main class are called *paratopic*. These operations can be denoted as a permutation of

the symbols R,C,S which stand for rows, columns and symbols respectively. This way, transposing the Latin square can be denoted[1] in shorthand by RC.

$$\begin{bmatrix} 2 & 4 & 3 & 1 \\ 1 & 2 & 4 & 3 \\ 3 & 1 & 2 & 4 \\ 4 & 3 & 1 & 2 \end{bmatrix} \quad \begin{bmatrix} 2 & 1 & 3 & 4 \\ 4 & 2 & 1 & 3 \\ 3 & 4 & 2 & 1 \\ 1 & 3 & 4 & 2 \end{bmatrix} \quad \begin{bmatrix} 2 & 3 & 4 & 1 \\ 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \\ 4 & 1 & 2 & 3 \end{bmatrix}$$

$$\begin{bmatrix} 2 & 1 & 3 & 4 \\ 3 & 2 & 4 & 1 \\ 4 & 3 & 1 & 2 \\ 1 & 4 & 2 & 3 \end{bmatrix} \quad \begin{bmatrix} 4 & 1 & 2 & 3 \\ 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \\ 2 & 3 & 4 & 1 \end{bmatrix} \quad \begin{bmatrix} 4 & 1 & 3 & 2 \\ 1 & 2 & 4 & 3 \\ 2 & 3 & 1 & 4 \\ 3 & 4 & 2 & 1 \end{bmatrix}$$

Figure 2.3: *The identity,* RC, RS, RSC, RCS, CS.

2.3 Transversals

In 1782 Euler posed the following question: "Can 36 officers be arranged in a 6 by 6 square so that each of six regiments and each of six ranks appear in each row and column exactly once?"[2]. We can translate his question into the question whether or not two Latin squares L and L' of order 6 exist, with the property that the set of n^2 ordered pairs (L_{ij}, L'_{ij}) are all different.

Two Latin squares of equal order with this property are called *orthogonal (mates)* and the pair is called a *Graeco-Latin square*[3]. A set of two or more Latin squares which are pairwise orthogonal is known as a set of *mutually orthogonal Latin squares*, or MOLS for short.

This theory will lead us to the definition of a (partial) transversal. We consider the n locations or cells of a Latin square of order n which are filled with a fixed symbol, say k. We know from the definition of a Latin square that k occurs in each row and each column exactly once. A Latin square orthogonal to this one will need to have n different symbols in each of these cells. Such a "path" through a Latin square which visits each row, each column and each symbol exactly once, is called a *transversal*.

Definition 12 A *transversal* of a Latin square of order n is a set of n ordered triples such that in each position of the triple the numbers in $\{1 \dots n\}$ occur exactly once.

[1] RSC means that rows become symbols, symbols become columns and columns become rows (read from left to right). In this notation RC=CR and RSC=SCR=CRS etc.

[2] No. Tarry [16]. See also page 10

[3] Euler denoted the 6 ranks by the Greek letters $\alpha, \beta, \gamma, \delta, \varepsilon, \zeta$ and the 6 regiments by the Latin letters a, b, c, d, e, f.

$$\begin{bmatrix} \boxed{1} & \mathbf{2} & 3 & 4 & \underline{5} \\ 2 & \boxed{\underline{3}} & 5 & \mathbf{1} & 4 \\ 3 & 5 & \boxed{\mathbf{4}} & \underline{2} & 1 \\ \underline{4} & 1 & 2 & \boxed{5} & \mathbf{3} \\ \mathbf{5} & 4 & \underline{1} & 3 & \boxed{2} \end{bmatrix}$$

$$\boxed{t_1} = \{(1,1,1),(2,2,3),(3,3,4),(4,4,5),(5,5,2)\}$$

$$\mathbf{t_2} = \{(1,2,2),(2,4,1),(3,3,4),(4,5,3),(5,1,5)\}$$

$$\underline{t_3} = \{(1,5,5),(2,2,3),(3,4,2),(4,1,4),(5,3,1)\}$$

Figure 2.4: *A Latin square with 15 transversals of which 3 are given.*

It is immediately obvious from the remarks at the beginning of this section that a Latin square has an orthogonal mate if and only if it has n disjoint transversals. Furthermore, we shall see that a set of MOLS of order n can contain at most $n-1$ Latin squares. Such a set of $n-1$ MOLS of order n is called *complete*.

Theorem 6 *Let $L_1, L_2, \ldots, L_m$ be a set of m mutually orthogonal Latin squares of order $n \geq 3$. Then*

$$m \leq n-1.$$

Proof. Let $L_1, L_2, \ldots, L_m$ be a set of m orthogonal Latin squares of order $n \geq 3$. We begin by permuting the *symbols* of each of the Latin squares so that the first row of each of the squares is in natural order. This does not destroy the orthogonality of the set. Now consider the m symbols that are in the $(2,1)$ position of the Latin squares. These m symbols must be distinct, for otherwise there are at least two squares with the same symbol, say k, in position $(2,1)$ but this symbol is also in position $(1,k)$ for both of the squares, which contradicts the orthogonality of the set. Nor can this symbol be 1, because for each of the squares there is already a 1 in the first column. Hence $m \leq n-1$. □

At this point we will give the first connection between finite projective planes and Latin squares. This connection is not the one we will be using later on, and is well known. A proof of the following theorem can be found in [5][14][7].

Theorem 7 *There exists a finite projective plane of order n if and only if there exists a complete set of $n-1$ mutually orthogonal Latin squares of order n.*

For now, we will give orthogonality a rest and return to transversals. We will define a variant on transversals, the *k*-S-*transversal*.

Definition 13 Let $0 \leq k < n$. A *k*-S-*transversal* of a Latin square of order n is a set of n ordered triples such that in the first (R) and second (C) position of the triple the numbers in $\{1 \dots n\}$ occur exactly once. In the third (S) position, exactly $n - k$ distinct symbols are required.

Again some examples to clarify this definition:

$$\begin{bmatrix} 1 & \boxed{2} & \underline{3} & 4 \\ \boxed{2} & \underline{4} & 1 & 3 \\ 3 & 1 & \boxed{4} & \underline{2} \\ \underline{4} & 3 & 2 & \boxed{1} \end{bmatrix} \quad \begin{bmatrix} \boxed{1} & 2 & 3 & \underline{4} \\ 2 & \boxed{4} & \underline{1} & 3 \\ 3 & \underline{1} & \boxed{4} & 2 \\ \underline{4} & 3 & 2 & \boxed{1} \end{bmatrix} \quad \begin{bmatrix} \boxed{1} & \underline{2} & 3 & 4 \\ \underline{2} & 4 & \boxed{1} & 3 \\ 3 & \boxed{1} & 4 & \underline{2} \\ 4 & 3 & \underline{2} & \boxed{1} \end{bmatrix}$$

Figure 2.5: *Two* 1-S-*transversals, two* 2-S-*transversals and two* 3-S-*transversals.*

Notice that the Latin square in figure 2.5 has no 0-S-transversals, which are the ordinary transversals. Some questions that come to mind are: How many transversals does a Latin square have? Do paratopic Latin squares have the same number of transversals?

The following theorem shows that the answer to the last question is positive for the ordinary (0-S-)transversals.

Theorem 8 *Latin squares in the same main class have the same number of transversals.*

Proof. Let L and L' be two paratopic Latin squares of order n. Assume that L has m transversals, which we defined as a set of n ordered triples. Recall that by definition the numbers $1, \dots, n$ appear exactly once in each of the three positions. The isotopy operations permute the numbers in each of the three positions amongst themselves. Hence the resulting set of triples is also a transversal. The 6 conjugacy operations permute the three positions for each triple in the same way. This also results in a transversal, so the paratopic operations transform each transversal of L into a transversal of L'. Thus paratopic Latin squares have the same number of transversals. □

Theorem 8 shows us that the paratopic operations do not change the number of transversals of a Latin square. The number of transversals of Latin squares is said to be *invariant* under the paratopic operations. Let us give a formal definition of invariance in this context.

Definition 14 Consider the collection of Latin squares $\mathbb{L}$ with an equivalence relation r on it. A map V on $\mathbb{L}$ is said to be *invariant under* r if for all $L, L' \in \mathbb{L}$ the following holds: if LrL', then $V(L) = V(L')$.

It is easily seen that the number of k-s-transversals is not invariant under the paratopic operations if $k > 0$. In the following section we describe a way of creating an invariant under the paratopic operations out of k-s-transversals. The purpose of all this is to be able to distinguish the 283657 main classes.

2.4 Constructing an Invariant

Suppose someone gives you two Latin squares of order n and asks if they belong to the same isotopy class. The first thing that comes to mind is to start doing row, column and symbol permutations and see if you can transform one into the other. Obviously, this can be a lot of work, especially for large n.

If you were asked if they are from the same main class, you would have had an even bigger problem, because of the 6 conjugacy operations.

Further on in this thesis, we will need one Latin square from every main class. To generate such a list of representatives, we will need a way of recognizing paratopic Latin squares. For this reason, we will return to the transversals and build sufficiently strong invariants out of them. We will use the k-s-transversals, which include the ordinary transversals for $k = 0$.

Consider a Latin square L with m k-s-transversals. These k-s-transversals can be seen as *monomial* matrices, a generalization of permutation matrices where the non-zero entries can differ from 1. When we throw away the symbol information, this gives us m permutation matrices P_i. Consider the multiset[4] of entries of $M = \sum_{i=1}^{m} P_i$. The sum of permutation matrices M tells us for each cell of L, in how many k-s-transversals it occurs.

$$\begin{bmatrix} \underline{1} & 2 & 3 & \mathbf{4} & \boxed{5} \\ \mathbf{2} & 4 & \boxed{1} & \underline{5} & 3 \\ 3 & 5 & \underline{4} & \boxed{2} & \mathbf{1} \\ \boxed{4} & 1 & \mathbf{5} & 3 & \underline{2} \\ 5 & \boxed{\underline{\mathbf{3}}} & 2 & 1 & 4 \end{bmatrix} \qquad \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 3 & 0 & 0 & 0 \end{pmatrix} \qquad \{*0^{12}, 1^{12}, 3*\}$$

Figure 2.6: *A Latin square L with three* 0-s-*transversals, its* 0-s-*matrix $M_0(L)$ and $\mathcal{M}(M_0(L))$.*

[4]Example: The multiset of $[37, 0, 4, 37]$ is $\{*0^1, 4^1, 37^2*\}$

This multiset is obviously invariant under isotopy, but not yet under conjugacy operations. We see that it is invariant under 2 of these conjugacy operations, namely under the identity and under the transposing of the square RC. We can include the other 4 by constructing multisets of the remaining conjugates of L in the same manner and considering a set of these 5 multisets. This number can even be further reduced to a set of 3 multisets when we realize that again RC does not change the multiset and that all conjugacy operations can be expressed as products of RC, RS and CS. Let us formalize this.

Definition 15 Let $n \geq 1$ and $m \geq 0$ and $0 \leq k < n$. Let L be a Latin square of order n with m k-S-transversals $t_1, \ldots, t_m$. Let P_l be the square permutation matrix of order n with $(P_l)_{ij} = 1$ if and only if $(i, j, \bullet) \in t_l$, for $1 \leq i, j \leq n$ and $1 \leq l \leq m$. We define the k-S-*matrix of* L as:

$$M_k(L) = \begin{cases} \sum_{l=1}^{m} P_l & m > 0 \\ 0 \cdot I_n & m = 0 \end{cases}$$

From now on we will use the notation L^{RC} for the transpose of L, and in the same way use $L^{\text{RS}}, L^{\text{CS}}, L^{\text{RCS}}, L^{\text{RSC}}$. Furthermore, we will use the notation $\mathcal{M}(M)$ for the multiset of entries of the matrix M.

Definition 16 Let L be a Latin square of order n and $0 \leq k < n$. We define the k-S-*structure of* L , notation $\mathcal{S}_k(L)$, as the set of multisets of entries of $M_k(L), M_k(L^{\text{RS}})$ and $M_k(L^{\text{CS}})$.
So

$$\mathcal{S}_k(L) = \{\mathcal{M}(M_k(L)) \ , \ \mathcal{M}(M_k(L^{\text{RS}})) \ , \ \mathcal{M}(M_k(L^{\text{CS}}))\}.$$

Remark 2 If L is a Latin square of order n then:

$\mathcal{S}_0(L)$ is a set containing a single multiset.

$\mathcal{S}_{n-1}(L) = \{\{*1^{n^2}*\}\}$.

Lemma 1 *The k-S-structure of a Latin square is invariant under isotopy.*

Proof. Let $n > 0$ and $0 \leq k < n$. Let L be a Latin square of order n and $\mathcal{S}_k(L)$ its k-S-structure. Consider the cell of L with position (i, j), where $1 \leq i, j \leq n$. Suppose this cell occurs in exactly m k-S-transversals of L, where $m \geq 0$. Row, column and symbol permutations relocate this cell in the Latin square, but do not change the fact that it occurs in m k-S-transversals. This holds for every Latin square, in particular for L^{RS} and L^{CS}.

We have that $M_k(L), M_k(L^{\text{RS}})$ and $M_k(L^{\text{CS}})$ may change under isotopy, but their multisets will not. Thus $\mathcal{S}_k(L)$ is invariant under isotopy. □

Lemma 2 *Let $n > 0$ and $0 \leq k < n$. For every Latin square L of order n we have that $\mathcal{M}(M_k(L^{\text{RC}})) = \mathcal{M}(M_k(L))$.*

Proof. Let L be a Latin square of order n and $0 \leq k < n$. Notice that transposing L also permutes the rows and columns in its k-s-transversals. Therefore, $M_k(L^{\text{RC}}) = (M_k(L))^T$. Now, it is clear that $\mathcal{M}(M_k(L^{\text{RC}})) = \mathcal{M}((M_k(L))^T) = \mathcal{M}(M_k(L))$. □

Lemma 3 *For a Latin square, the following equalities hold:*

i) $L = (L^{\text{RS}})^{\text{RS}} = (L^{\text{RC}})^{\text{RC}} = (L^{\text{CS}})^{\text{CS}} = (L^{\text{RSC}})^{\text{RCS}} = (L^{\text{RCS}})^{\text{RSC}}$

ii) $L^{\text{RS}} = (L^{\text{RSC}})^{\text{RC}} = (L^{\text{RCS}})^{\text{CS}} = (L^{\text{CS}})^{\text{RSC}} = (L^{\text{RC}})^{\text{RCS}}$

iii) $L^{\text{RC}} = (L^{\text{RCS}})^{\text{RS}} = (L^{\text{RSC}})^{\text{CS}} = (L^{\text{RS}})^{\text{RSC}} = (L^{\text{CS}})^{\text{RCS}}$

iv) $L^{\text{CS}} = (L^{\text{RSC}})^{\text{RS}} = (L^{\text{RCS}})^{\text{RC}} = (L^{\text{RC}})^{\text{RSC}} = (L^{\text{RS}})^{\text{RCS}}$

v) $L^{\text{RSC}} = (L^{\text{CS}})^{\text{RS}} = (L^{\text{RS}})^{\text{RC}} = (L^{\text{RC}})^{\text{CS}} = (L^{\text{RCS}})^{\text{RCS}}$

vi) $L^{\text{RCS}} = (L^{\text{RC}})^{\text{RS}} = (L^{\text{CS}})^{\text{RC}} = (L^{\text{RS}})^{\text{CS}} = (L^{\text{RSC}})^{\text{RSC}}$

Proof. The proof of this lemma is a straightforward but tedious check of identities between permutations of three elements. □

Lemma 4 *The k-s-structure of a Latin square is invariant under conjugacy.*

Proof. Let $n > 0$ and $0 \leq k < n$. Let L be a Latin square of order n and $\mathcal{S}_k(L)$ its k-s-structure. Let us consider the k-s-structure of L^{RCS}:

$$\begin{aligned}
\mathcal{S}_k(L^{\text{RCS}}) &= \{\mathcal{M}(M_k(L^{\text{RCS}})) \,,\, \mathcal{M}(M_k((L^{\text{RCS}})^{\text{RS}})) \,,\, \mathcal{M}(M_k((L^{\text{RCS}})^{\text{CS}}))\} \\
&\overset{lem.\ 3}{=} \{\mathcal{M}(M_k((L^{\text{CS}})^{\text{RC}})) \,,\, \mathcal{M}(M_k(L^{\text{RC}})) \,,\, \mathcal{M}(M_k(L^{\text{RS}}))\} \\
&\overset{lem.\ 2}{=} \{\mathcal{M}(M_k(L^{\text{CS}})) \,,\, \mathcal{M}(M_k(L)) \,,\, \mathcal{M}(M_k(L^{\text{RS}}))\} \\
&= \mathcal{S}_k(L)
\end{aligned}$$

We see that the k-s-structure of L^{RCS} is the same as the k-s-structure of L. The other five cases follow from similar arguments. Hence $\mathcal{S}_k(L^{\text{RCS}}) = \mathcal{S}_k(L^{\text{RSC}}) = \mathcal{S}_k(L^{\text{SC}}) = \mathcal{S}_k(L^{\text{RC}}) = \mathcal{S}_k(L^{\text{RS}}) = \mathcal{S}_k(L)$. Thus the k-s-structure of a Latin square is invariant under conjugacy. □

Theorem 9 *The k-s-structure is an invariant for Latin squares under paratopy.*

Proof. This follows directly from Lemma 1 and Lemma 4. □

$$L = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 1 & 7 & 4 & 5 & 6 \\ 3 & 1 & 6 & 5 & 7 & 4 & 2 \\ 4 & 6 & 2 & 1 & 3 & 7 & 5 \\ 5 & 7 & 4 & 2 & 6 & 3 & 1 \\ 6 & 5 & 7 & 3 & 1 & 2 & 4 \\ 7 & 4 & 5 & 6 & 2 & 1 & 3 \end{bmatrix}$$

$$\mathcal{S}_0(L) = \{\{*0^2, 1^4, 2^{10}, 3^{17}, 4^8, 5^2, 6^5, 7*\}\}$$

$$\begin{aligned}\mathcal{S}_1(L) = \{&\{*55, 57^2, 58, 59, 61^2, 62, 63^3, 64, 65^8, 67^4, 68^2, 69^8, 70, 71^2, 73^6, 75^3, 76, 77^2*\},\\ &\{*55, 57, 58, 59, 61, 62^3, 63^3, 64^3, 65, 66^5, 67^5, 68^3, 69^6, 70^2, 71^2, 72^3, 73^3, 75^2, 76, 77, 79*\},\\ &\{*56^2, 57, 58, 59^2, 61, 62, 63^3, 64^2, 65^3, 66^2, 67^7, 68^4, 69^3, 70^2, 71^2, 72^4, 73^3, 74^2, 75, 76, 77, 79*\}\}\end{aligned}$$

Figure 2.7: *A Latin square of order* 7 *and its* 0-S-*structure and* 1-S-*structure.*

2.5 Generating Representatives

In the previous section we constructed an invariant for Latin squares under paratopy. Here, we will use this k-S-structure for generating our own list of representative Latin squares. We start by noticing that every main class contains a Latin square in reduced form. Our approach for generating representatives will be by generating these reduced Latin squares and using our k-S-structure for distinction between main classes. A big problem with this approach is the large number of reduced Latin squares, as can be seen in table 2.1.

n	red. Latin Sq.	main classes	$\mathcal{S}_0(L)$	$(\mathcal{S}_0(L), \mathcal{S}_1(L))$	$(\mathcal{S}_0(L), \mathcal{S}_1(L), \mathcal{S}_2(L))$
1	1	1	1	-	-
2	1	1	1	1	-
3	1	1	1	1	1
4	4	2	2	2	2
5	56	2	2	2	2
6	9408	12	6	12	12
7	16942080	147	147	147	147
8	535281401856	283657	283503	283636	283657

Table 2.1: *Discriminatory abilities of the* k-S-*structure.*

The program I wrote for the generation of all reduced Latin squares is a backtrack program. It completes the first incomplete row from the top and then starts on the next one. During this completion, it will ensure that the first column always is in natural order. The input when searching for all reduced Latin squares of order 8 is `(8,[[1,2,3,4,5,6,7,8]])`, with in the first position the order and in second the square known so far. All Latin squares with reduced first column would be given when the input

was `(8,[[]])`. A way of reducing the search for our representatives is to decrease the number of Latin squares we need to search through. Using the isotopic operations, we can narrow down the number of possible second rows (beginning with a 2) to 13 for Latin squares of order 8. These 13 cases start deeper in the search tree and give more restrictions, therefore we gain a lot. Each of these cases yield approximately 250 million Latin squares and therefore we 'only' have to search in 3.25 billion Latin squares instead of 535 billion reduced Latin squares. Using our k-s-structures and the fact that the number of main classes are known for small order, we can generate a list of representative Latin squares. Appendix C gives such lists for Latin squares up to order 7 as generated by Brendan McKay.

Chapter 3

Exhaustive Searching for Planes

Summary

A connection between the incidence matrix of a finite projective plane of order n and Latin squares of order $n-1$ is explored. We show how non-paratopic Latin squares can be used when searching an incidence matrix of a finite projective plane. The program is explained and results are given.

3.1 Introduction

Latin squares and finite projective planes are strongly related to each other. We saw in Theorem 7 the well-known connection between a complete set of mutually orthogonal Latin squares of order n and a finite projective plane of the same order. Searching for such sets is very time-consuming, partly because of the fact that the number of Latin squares grows extremely fast when increasing the order. Fortunately there is also a less well known tie between Latin squares of order $n-1$ and finite projective planes of order n for us to explore and exploit.

3.2 The Partial Incidence Matrix

In section 1.2 we showed how a finite projective plane π can be represented by an incidence matrix A_π. We will now show that this incidence matrix can be transformed into normalized form N_π by permuting rows and permuting columns. Such permutations yield a renaming of lines and points in the plane π, which results in an isomorphic plane.

Consider a finite projective plane π of order n and its incidence matrix A_π. Recall that every row and every column has length n^2+n+1, contains

$n+1$ ones, and every two rows and every two columns have exactly one 1 in the same column and row respectively. We can permute rows and columns in such a way, that the 3×3 sub-matrix in the top left corner is $\left(\begin{smallmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{smallmatrix}\right)$. By permuting all but the first three columns and all but the first three rows, we can obtain the following form:

	1	2	3	4	…	$n+2$	$n+3$	…	$2n+1$	$2n+2$	…	$3n$	$3n+1$	…	n^2+n+1
1	0	1	1	1	…	1									
2	1	1	0				1	…	1					0	
3	1	0	1							1	…	1			
4	1														
⋮	⋮				?			?			?			?	
n+2	1														
n+3		1													
⋮		⋮			?			?			?			?	
2n+1		1													
2n+2			1												
⋮			⋮		?			?			?			?	
3n			1												
3n+1															
⋮		0			?			?			?			?	
4n-1															
4n															
⋮		⋮			?			?			?			?	
n^2+2															
n^2+3															
⋮		0			?			?			?			?	
n^2+n+1															

Figure 3.1: *Normalizing the partial incidence matrix.*

In the same manner, by observing incidences and weights, we can fix even more entries of this matrix. For instance, rows 4 to $n+2$ are incident with rows 2 and 3 in the first column. Therefore, these rows can have only

zeros in columns $n+3$ to $3n$, because otherwise they would have more than one 1 in the same column as row 2 or 3. In the related plane this would mean that two lines intersect in more than one point, which is not allowed. On the other hand, these lines have not yet intersected with line 1 and the only place for them to do so is in columns 4 to $n+2$. Continuing this way, we can bring the incidence matrix in the following form only using row permutations and column permutations.

	1	2	3	4	…	n $+2$	n $+3$	…	$2n$ $+1$	$2n$ $+2$	…	$3n$	$3n$ $+1$	…	n^2+ $n+1$
1	0	1	1	1	…	1									
2	1	1	0				1	…	1				0		
3	1	0	1							1	…	1			
4	1			1											
⋮	⋮			⋱			0			0			?		
n+2	1					1									
n+3		1								1					
⋮		⋮		0			0			⋱			?		
2n+1		1										1			
2n+2			1				1								
⋮			⋮	0			⋱			0			?		
3n			1						1						
3n+1				1			1								
⋮		0		⋮			⋱			B_1			?		
4n-1				1					1						
4n															
⋮	⋮			⋮			⋮			⋮			?		
n^2+2															
n^2+3						1	1								
⋮		0				⋮	⋱			B_{n-1}			?		
n^2+n+1						1			1						

Figure 3.2: *A partial incidence matrix in normal form.*

We now see that we can bring each incidence matrix of a finite projective plane of order n into this normalized form. In this normalized form, the columns 1 to $3n$ are completely known, except for the $n-1$ sub-matrices B_i. But we can deduce some information about these $n-1$ square matrices of size $n-1$.

Consider one of these sub-matrices, say B_i. Each of its rows must intersect row 3 once, so each row of B_i contains exactly one 1. Likewise, each of the columns $2n+2$ to $3n$ must intersect once with column $3+i$, so each column of B_i contains exactly one 1. Hence B_i is a permutation matrix. Furthermore, we can show that adding these $n-1$ permutation matrices results in an all-ones matrix.

Consider the k-th column in the range $2n+2$ to $3n$. The intersections with the columns $n+3$ to $2n+1$ gives us that in all B_i k-th columns must be distinct. This argument holds for all columns $2n+2$ to $3n$. Thus, the B_i's are $n-1$ square permutation matrices of size $n-1$ which, when summed, form the all-ones matrix J_{n-1}.

In the next section we will see that the sequence of these sub-matrices can be identified with a Latin square of order $n-1$ and vice versa.

3.3 Paratopic Squares vs. Isomorphic Planes

There are several ways to associate the sequence $B_1, \ldots, B_{n-1}$ with a Latin square. One obvious way, which we will not be using, is defining the Latin square L as $1 \cdot B_1 + 2 \cdot B_2 + \cdots + (n-1) \cdot B_{n-1}$. The correspondence we will be using can be given as follows:

$$(B_i)_{kj} = 1 \iff (L)_{ij} = k.$$

Thus, there is a 1 in row k, column j of B_i if and only if there is a k in row i and column j of the Latin square.

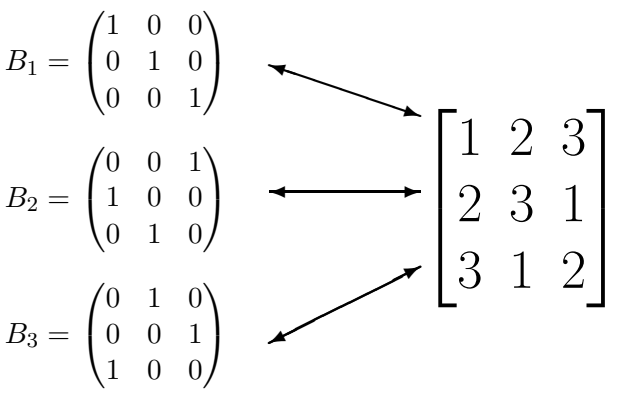


Figure 3.3: *An example of how the sub-matrices B_i of order 3 relate to a Latin square of order 3.*

We now have that every finite projective plane π of order n can be translated into an incidence matrix A_π which can be normalized into N_π which represents a plane isomorphic to π. This normalized incidence matrix contains $n-1$ permutation matrices which can be interpreted as a Latin square of order $n-1$. Trying to reverse this chain gives us a way to generate all projective planes of a certain order.

Suppose we know a normalized incidence matrix only up to column $3n$ and do not know the $n-1$ permutation matrices. If we fill this gap with the permutation matrices belonging to an arbitrary Latin square of order $n-1$, this gives us a partial incidence matrix which possibly can be extended to a complete incidence matrix. Trying all Latin squares of order $n-1$ will give us all possible normalized incidence matrices and thus, up to isomorphisms, all finite projective planes of order n.

Because of the large number of Latin squares, trying all of them out would be too hard for high orders. We will show now that paratopic Latin squares will give isomorphic finite projective planes. Therefore we only have to try one Latin square from each main class, a so-called representative. This reduces our search enormously.

Theorem 10 *Partial incidence matrices from* isotopic *Latin squares can be transformed into each other by row permutations and column permutations. Therefore, if a Latin square gives rise to a complete incidence matrix of a finite projective plane, an isotopic Latin square will give rise to an isomorphic plane.*

Proof. Let L_1 and L_2 be two isotopic Latin squares of order $n-1$, and N^{L_1} and N^{L_2} the partial incidence matrices belonging to these squares. L_1 can be transformed into L_2 by permuting rows, columns and symbols. Permuting rows in L_2 means permuting blocks B_i in N^{L_2}, which can be achieved by permuting related row blocks. Re-transforming the partial matrix in its normal form without changing the blocks B_i can now be done by permuting columns in the range 4 to $n+2$ and rows 4 to $n+2$. Permuting columns in the Latin square results in permutations of columns in the blocks B_i. These can be achieved by permuting columns in the partial incidence matrix. Restoring the normal form can be done by permutations in the rows 4 to $n+2$. Restoring normality after symbol permutations can be done by permuting columns in the range $n+3$ to $2n+1$ and rows $2n+2$ to $3n$. All operations used to bring back the partial incidence matrix into its normal form are row permutations or column permutations. Therefore, if N^{L_1} can be completed, N^{L_2} can be completed to an isomorphic finite projective plane. □

Theorem 11 *Partial incidence matrices from* paratopic *Latin squares can be transformed into each other by row permutations and column permutations. Therefore, if a Latin square gives rise to a complete incidence matrix of a finite projective plane, an isotopic Latin square will give rise to an isomorphic plane.*

Proof. Let L_1 and L_2 be two paratopic Latin squares of order $n-1$, and N^{L_1} and N^{L_2} the partial incidence matrices belonging to these squares. In the partial incidence matrix, permuting columns 1 and 3 translates to the Latin square as rows and symbols changing roles, RS. Consider a partial incidence matrix with columns 1 and 3 swapped. To restore the normal form, we subsequently permute rows 1 and 2, column blocks 4 to $n+2$ and $n+3$ to $2n+1$, row blocks 4 to $n+2$ and $2n+2$ to $3n$. Finally, we permute rows $3n+1$ to n^2+n+1 to obtain the normal form. When doing this we notice that every k-th row of the i-th permutation block becomes the i-th row of the k-th block. Hence $(B_i)_{kj} \longrightarrow (B_k)_{ij}$, which translates to the Latin squares as $(L)_{ij} = k \longrightarrow (L)_{kj} = i$. This is RS. The other cases can be shown in a similar manner. □

3.4 Backtracking

Summarizing the previous sections, we see that every Latin square can be embedded in a partial incidence matrix, which can possibly be completed to an incidence matrix belonging to a finite projective plane. Furthermore, we proved that Latin squares from the same main class yield, if any, isomorphic finite projective planes.

The idea for the exhaustive generation of finite projective planes is as follows. Take one Latin square from each main class and embed it in a partial incidence matrix. Try to complete this incidence matrix and if this yields a complete incidence matrix, check for isomorphism with known finite projective planes of that order.

Below, we first describe the basic structure of our program and then we take a look at each stage in greater detail.

1. Generate or recall a list of possible 'append-able' columns to the (unembedded) partial incidence matrix of order n.
2. Get a Latin square of order $n-1$ from a list of main class representatives.
3. Prune the generated list with the extra restrictions given by the embedded Latin square.
4. Generate a so-called compatibility matrix H.

5. Use backtracking to complete the partial incidence matrix by appending possible columns.

6. If any complete incidence matrices are found, check for isomorphism with the known planes of order n.

1. Generating possible columns.
Once we have fixed the plane order n, we know exactly what the partial incidence matrix looks like, except for the $n-1$ blocks in which we will embed our Latin squares.

Based on this partial incidence matrix, we can deduce some restrictions on the columns we want to try to append. We already know that such a column must contain exactly $n+1$ ones. The following restrictions can be found also: In the range 1 to 3 there can only be zeros, in the range 4 to $n+2$ there is exactly one 1 (because of incidence with the first column), say in the i-th position of this range. Likewise, there is exactly one 1 in the range $n+3$ to $2n+1$, say in the j-th position of this range, and exactly one 1 in the range $2n+2$ to $3n$, say in the k-th position of this range. Furthermore, the range belonging to the i-th block cannot contain a 1, neither can each k-th position in the block ranges. All these restrictions reduce the number of possible rows from the total number of rows with $n+1$ ones, which is $\binom{n^2+n+1}{n+1}$, to $(n-1)^3 \cdot (n-2)!$ possible rows.

Because of the small number of non-zeros in these rows, we used a different way to store and represent them. We translated each possible column into an element of $\{0, 1, \ldots, n-1\}^{n+2}$ in the following way. Consider a column without its first three zeros and divide it in $(n-1)$-blocks. These $n+2$ blocks relate to the $n+2$ positions of the alternative representation, which we will call a *reduced column*. This position contains a zero if the related block contains only zeros, and otherwise it contains the row number of the one in that block. A small example for $n = 4$ is given below.

$$(0,0,0;0,1,0;1,0,0;1,0,0;0,1,0;0,0,0;0,0,1)^T = [2,1,1,2,0,3]^T$$

In theory, generating these possible columns only needs to be done once per order. In practice, reading in these 2580480 columns for $n = 9$ takes considerably more time than generating them, which takes under 5 minutes.

2. Choosing a representative square.
In Section 2.5 we explained a method of generating a list of Latin squares, each of which represents a main class. This was done by using invariants. This phase of the program is nothing more than reading the first non-processed Latin square from this list.

3. Pruning the list of possible columns.
We now can translate the chosen Latin square into the permutation matrices B_i, and deduce some more restrictions on the possible columns. For example, a 1 in the $(1,1)$ position of B_1, results in rejection of reduced columns with a one in the second and fourth position. Maximal usage of such restrictions yields us a relatively small set of possible columns. For $n = 9$ this number varies from 3000 to 4500. The set of columns is sorted lexicographically for convenient usage later on.

4. Creating the compatibility matrix.
The compatibility matrix H is a $(0,1)$-matrix in upper triangle form. Its size equals the number of possible columns found in stage 3. For $j > i$, there is a 1 in position (i,j) of the matrix H if and only if the i-th and j-th column from the sorted set have inner product 1. Because of this matrix, we do not have to calculate any inner products during the backtrack any more, but merely a lookup in our compatibility matrix.

5. Backtracking for a complete incidence matrix.
Backtracking can be a really time-consuming process. The most difficult part is finding a balance in reducing the number of nodes by adding tests on the one hand, and reducing the time spent in a node by decreasing the number of tests on the other. In our case, we do not have to worry about this, because of the following theorem.

Theorem 12 *Let $n \in \mathbb{N}_{>0}$. If N is a $(0,1)$-matrix with n^2+n+1 rows and at least $n+2$ columns, with the property that each column contains $n+1$ ones and any two distinct columns have inner product 1, then*

1. *Each row contains $n+1$ ones at most.*
2. *The inner product of any two distinct rows is at most 1.*

Proof. 1. Suppose there exists a row which contains at least than $n+2$ ones. Consider $n+2$ columns $K_1, K_2, \ldots, K_{n+2}$ that contain these ones. Each of these columns has n remaining ones, which can be located in any of the remaining n^2+n positions. We notice that there are $n(n+2)$ ones in n^2+n possible positions. Because of the pigeonhole principle are there at least two ones in the same row. But we already had a row where these two columns both had ones. Contradiction. Therefore, each row contains at most $n+1$ ones.
2. Suppose there exist two distinct rows with inner product exceeding 1. Now, there must be two distinct columns with twice a one in the same row. Contradiction. We see that the inner product of any two distinct rows is at most 1. □

We see now that we can append any column, as long as it has weight $n+1$ and inner product 1 with all columns of the partial incidence matrix. The set of reduced columns we created earlier has these properties. This means we can append the first column from this set, then append the first column from this set which has inner product 1 with it, then append the first column from this set which has inner product 1 with both of them, and so on. Checking the columns for their inner products is done by means of a search in the compatibility matrix H. There are two possible outcomes when using this method, the first being completion of the incidence matrix to n^2+n+1 columns, and the second is exhaustion of the set of possible columns which fulfill the increasing number of restrictions. In both these cases we go back a step and try the next possible column, the actual backtracking. We do not really have to continue until the set of columns is completely empty, but can stop when there are fewer possible columns left than columns are needed to complete the incidence matrix. Finally, when a complete incidence matrix has been found, we need to be sure that it has all the properties needed for a finite projective plane.

Theorem 13 *Let $n \in \mathbb{N}_{>0}$. If N is a square $(0,1)$-matrix of size n^2+n+1 with the property that each column contains $n+1$ ones and any two distinct columns have inner product 1, then*

1. *Each row contains exactly $n+1$ ones.*

2. *The inner product of any two distinct rows is exactly 1.*

Proof. 1. Suppose there exists a row, say i, which contains $k < n+1$ ones. There are (n^2+n+1) columns with each $n+1$ ones, so there are a total of $(n+1)(n^2+n+1)$ ones in the matrix. The rows which are not i together have a total of $(n+1)(n^2+n+1)-k$ ones. These ones are divided over n^2+n rows. By applying the pigeonhole principle we see that there must be a row which contains $\lceil \frac{(n+1)(n^2+n+1)-k}{n^2+n} \rceil = \lceil (n+1) + \frac{(n+1-k)}{n^2+n} \rceil > n+1$ ones. This contradicts Theorem 12, so there exists no row with less than $n+1$ ones. From Theorem 12 we know that there exists no row with more than $n+1$ ones either. Therefore, every row contains exactly $n+1$ ones.
2. Suppose there exist two rows, say i and j, with inner product 0. Let $k_1, \ldots, k_{n+1}$ be the $n+1$ columns containing the ones of row i. These $n+1$ columns each have n remaining ones, which gives a total of $n(n+1)$ ones. These ones can be in arbitrary rows, but not in row i and j. This leaves us with n^2+n-1 rows. Applying the pigeonhole principle once more, we see that there must be two columns from $k_1, \ldots, k_{n+1}$ with ones in the same row. But there already were two ones in row i, which gives a contradiction. Therefore there can not exist two rows with inner product 0. Together with Theorem 12 we now see that the inner product of any two distinct rows is exactly 1. □

Because of Theorem 13, we know that if our program returns a completed matrix, then it must be an incidence matrix of a finite projective plane. The only thing we still need to know is which class of isomorphic finite projective planes it belongs to.

6. Isomorphism testing.
The final stage in the program is to test the finite projective planes we found, against known finite projective planes of that order for isomorphism. This is a feature in MAGMA which I used. A different way would be by means of the fingerprint-invariant which is explained in Appendix A. The problem with using this invariant is that it will possibly not distinguish two non-isomorphic planes with order $n \geq 11$.

3.5 Results

In this section we will first analyze the results of our computer programs. Afterwards, we will compare the overall outcome of this thesis with the goal stated in Section 1.5. We also give some suggestions for further research in this field.

Computational Results

The Latin squares of order 2 have one main class. It takes approximately 0.020 seconds to run the program as described in Section 3.4 and one complete incidence matrix is found. Isomorphism testing shows that it is isomorphic to the Desarguesian finite projective plane of order 3. See table 3.1.

Latin Sq. of order 2		
sq. nr.	# poss. col.	# gen. planes
1	4	1

Latin Sq. of order 3		
sq. nr.	# poss. col.	# gen. planes
1	9	1

Table 3.1: *Information on the search with Latin squares of order* 2 *and* 3.

The Latin squares of order 3 have one main class. It takes approximately 0.030 seconds to run the program and one complete incidence matrix is found. It is isomorphic to the Desarguesian finite projective plane of order 4. See table 3.1.

The Latin squares of order 4 have two main classes. It takes approximately 0.050 seconds to run the program for a single representative and for one class (number 2), two complete incidence matrices are found. Both are isomorphic to the Desarguesian finite projective plane of order 5. See table 3.2.

Latin Sq. of order 4		
sq. nr.	# poss. col.	# gen. planes
1	32	0
2	32	2

Latin Sq. of order 5		
sq. nr.	# poss. col.	# gen. planes
1	75	0
2	79	0

Table 3.2: *Information on the search with Latin squares of order* 4 *and* 5.

The Latin squares of order 5 have two main classes. It takes approximately 0.230 seconds to run the program for a single representative. No complete incidence matrices are found. We see again that there are no finite projective planes of order 6. See table 3.2.

The Latin squares of order 6 have 12 main classes. It takes approximately 6 seconds (depends on the number of possible columns) to run the program for a single representative and for one class (number 4), two complete incidence matrices are found. Both are isomorphic to the Desarguesian finite projective plane of order 7. See table 3.3.

Latin Sq. of order 6		
sq. nr.	# poss. col.	# gen. planes
1	248	0
2	216	0
3	324	0
4	288	2
5	264	0
6	264	0
7	288	0
8	296	0
9	308	0
10	304	0
11	280	0
12	288	0

Table 3.3: *Information on the search with Latin squares of order* 6.

The Latin squares of order 7 have 147 main classes. It takes approximately 20 minutes to run the program for number 38 which gives the fewest possible columns and 26 minutes for number 37 which gives the most possible columns. For one class (number 38), two complete incidence matrices are found. Both are isomorphic to the Desarguesian finite projective plane of order 8. See table 3.4 on page 37.

Latin squares of order 8 are partitioned into 283657 main classes. The first representative allows 3072 possible columns. Some educated guessing led to the approximation of 10 days of computation time on 'Bommel' for this first case. Therefore we ran it on 'Sickbock' which has much less memory, but a faster processor. The program finished in approximately 3.5 days and found no complete incidence matrices for the first of the 283657 representatives. Figure 3.4 gives the time spent in seconds in each of the 3072 branches of the search tree.

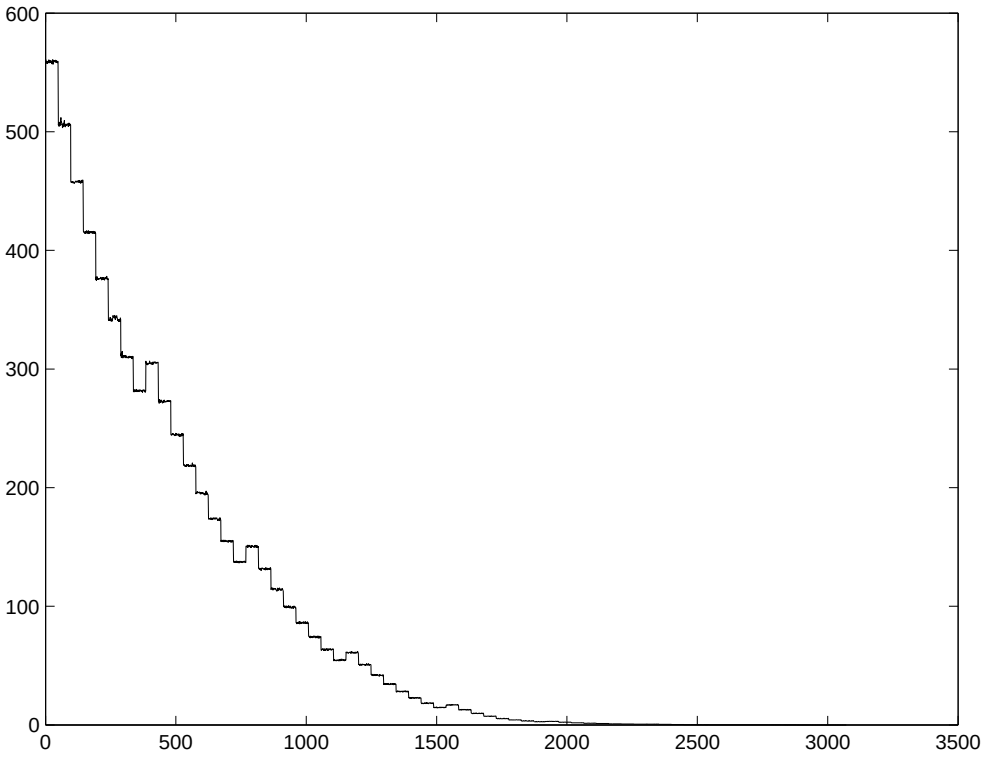


Figure 3.4: *Time spent in each of the* 3072 *branches.*

Latin Sq. of order 7								
sq. nr.	# poss. col.	# gen. planes	sq. nr.	# poss. col.	# gen. planes	sq. nr.	# poss. col.	# gen. planes
1	1113	0	50	1075	0	99	1068	0
2	1101	0	51	1084	0	100	1078	0
3	1095	0	52	1057	0	101	1088	0
4	985	0	53	1072	0	102	1092	0
5	1077	0	54	1094	0	103	1097	0
6	1057	0	55	1098	0	104	1083	0
7	1098	0	56	1089	0	105	1089	0
8	1097	0	57	1109	0	106	1083	0
9	1082	0	58	1066	0	107	1079	0
10	1100	0	59	1105	0	108	1096	0
11	1079	0	60	1077	0	109	1072	0
12	1090	0	61	1119	0	110	1107	0
13	1100	0	62	1074	0	111	1079	0
14	1089	0	63	1087	0	112	1095	0
15	1098	0	64	1074	0	113	1082	0
16	1112	0	65	1091	0	114	1094	0
17	1093	0	66	1093	0	115	1077	0
18	1107	0	67	1091	0	116	1068	0
19	1075	0	68	1085	0	117	1074	0
20	1123	0	69	1069	0	118	1083	0
21	1091	0	70	1062	0	119	1096	0
22	1094	0	71	1096	0	120	1104	0
23	1114	0	72	1103	0	121	1096	0
24	1087	0	73	1082	0	122	1104	0
25	1045	0	74	1102	0	123	1073	0
26	1080	0	75	1108	0	124	1073	0
27	1087	0	76	1093	0	125	1097	0
28	1120	0	77	1088	0	126	1122	0
29	1098	0	78	1078	0	127	1090	0
30	1117	0	79	1077	0	128	1101	0
31	1105	0	80	1076	0	129	1083	0
32	1095	0	81	1119	0	130	1073	0
33	1102	0	82	1067	0	131	1117	0
34	1100	0	83	1081	0	132	1107	0
35	1045	0	84	1093	0	133	1090	0
36	1087	0	85	1081	0	134	1109	0
37	1125	0	86	1106	0	135	1097	0
38	931	2	87	1104	0	136	1091	0
39	1143	0	88	1067	0	137	1048	0
40	1093	0	89	1079	0	138	1074	0
41	1091	0	90	1089	0	139	1065	0
42	1089	0	91	1091	0	140	1073	0
43	1055	0	92	1096	0	141	1103	0
44	1103	0	93	1057	0	142	1094	0
45	1108	0	94	1057	0	143	1065	0
46	1092	0	95	1093	0	144	1077	0
47	1073	0	96	1118	0	145	1078	0
48	1073	0	97	1095	0	146	1083	0
49	1092	0	98	1037	0	147	1089	0

Table 3.4: *Information on the search with Latin squares of order* 7.

Personal Results

Let us return to the goal I set for myself. This was to review, understand, reproduce, generalize and perhaps even improve this method. While working on this master's thesis I have studied various books and articles on the subject of finite projective planes and Latin squares. These are both subjects with many mathematical facets some of which I have neglected completely and others studied in greater detail. On the subject of projective planes, books by Stevenson [15], Dembowski [3], Hughes and Piper [7], Ryser [14] and articles by Lam [11][10], Parker and Killgrove [13], Hall, Swift and Killgrove [6], and Bruck and Ryser [1] were consulted most. Books on Latin squares used are by Dénes and Keedwell [5][4] and the articles by Kolesova, Lam, Thiel [9] and Tarry [16]. Books and articles that were consulted for computational reasons are by McKay [12], Knuth [8] and the online MAGMA-Help.

This research has given me more insight in both subjects, and has in particular increased my knowledge on the connection between (incidence matrices of) finite projective planes and Latin squares. Once the subject was more familiar, I started implementing some of the algorithms in MAGMA and could easily generalize them to work for every order n. In my eyes, the greatest (computational) breakthrough was made when I realized that most of the tests in the backtrack program were unnecessary, and was able to prove this.

The question whether or not I improved Lam's method remains. On the one hand, Lam was able to compute all 283657 Latin square representatives of order 8 within reasonable time whereas I needed almost 4 days to compute a single representative, which is not really an improvement. On the other hand, Lam used a supercomputer and their program was modified to optimize the vectoring capability of such a supercomputer. This will speed up computations a lot. Furthermore, my program works best when it is instructed to search for a *complete* incidence matrix. Although it can just as easily compute incidence matrices up to a fixed number of columns by means of a variable, as Lam does first, this reduces[1] the effectiveness of my program. I see no purpose in doing this the way Lam did, but then I only know the basic outlines of his program. This leads me to the following conclusion on my achievement.

I think I did a pretty good job, I learned a lot, I tackled most hurdles on my own and this has resulted in something I am proud of. Yet the infeasibility for the finite projective planes of order 9 stings a bit.

[1] A set of m possible append-able columns can be rejected if there are more than m columns to be done. Therefore, the lower the bound, the less you throw away. We see that when the bound is set lower than maximal, the search tree can contain more nodes than in the case with the maximal bound.

Suggestions for Further Research

The partial incidence matrix for a finite projective plane of order n we used for our programs is divided in square blocks of size $n-1$ (except for the first three rows and columns). When a complete incidence matrix is found, by adding columns in lexicographical order, we see that this block structure occurs in the entire matrix, as can be seen in figure 3.5.

0 1 1	1 1 1 1	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0
1 1 0	0 0 0 0	1 1 1 1	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0
1 0 1	0 0 0 0	0 0 0 0	1 1 1 1	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0
1 0 0	1 0 0 0	0 0 0 0	0 0 0 0	1 1 1 1	0 0 0 0	0 0 0 0	0 0 0 0
1 0 0	0 1 0 0	0 0 0 0	0 0 0 0	0 0 0 0	1 1 1 1	0 0 0 0	0 0 0 0
1 0 0	0 0 1 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0	1 1 1 1	0 0 0 0
1 0 0	0 0 0 1	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0	0 0 0 0	1 1 1 1
0 1 0	0 0 0 0	0 0 0 0	1 0 0 0	1 0 0 0	1 0 0 0	1 0 0 0	1 0 0 0
0 1 0	0 0 0 0	0 0 0 0	0 1 0 0	0 1 0 0	0 1 0 0	0 1 0 0	0 1 0 0
0 1 0	0 0 0 0	0 0 0 0	0 0 1 0	0 0 1 0	0 0 1 0	0 0 1 0	0 0 1 0
0 1 0	0 0 0 0	0 0 0 0	0 0 0 1	0 0 0 1	0 0 0 1	0 0 0 1	0 0 0 1
0 0 1	0 0 0 0	1 0 0 0	0 0 0 0	0 0 0 1	0 1 0 0	0 0 1 0	1 0 0 0
0 0 1	0 0 0 0	0 1 0 0	0 0 0 0	0 0 1 0	0 0 0 1	1 0 0 0	0 1 0 0
0 0 1	0 0 0 0	0 0 1 0	0 0 0 0	0 1 0 0	1 0 0 0	0 0 0 1	0 0 1 0
0 0 1	0 0 0 0	0 0 0 1	0 0 0 0	1 0 0 0	0 0 1 0	0 1 0 0	0 0 0 1
0 0 0	1 0 0 0	1 0 0 0	1 0 0 0	0 0 0 0	0 0 0 1	0 1 0 0	0 0 1 0
0 0 0	1 0 0 0	0 1 0 0	0 1 0 0	0 0 0 0	0 0 1 0	0 0 0 1	1 0 0 0
0 0 0	1 0 0 0	0 0 1 0	0 0 1 0	0 0 0 0	0 1 0 0	1 0 0 0	0 0 0 1
0 0 0	1 0 0 0	0 0 0 1	0 0 0 1	0 0 0 0	1 0 0 0	0 0 1 0	0 1 0 0
0 0 0	0 1 0 0	1 0 0 0	0 0 1 0	1 0 0 0	0 0 0 0	0 0 0 1	0 1 0 0
0 0 0	0 1 0 0	0 1 0 0	1 0 0 0	0 1 0 0	0 0 0 0	0 0 1 0	0 0 0 1
0 0 0	0 1 0 0	0 0 1 0	0 0 0 1	0 0 1 0	0 0 0 0	0 1 0 0	1 0 0 0
0 0 0	0 1 0 0	0 0 0 1	0 1 0 0	0 0 0 1	0 0 0 0	1 0 0 0	0 0 1 0
0 0 0	0 0 1 0	1 0 0 0	0 1 0 0	0 0 1 0	1 0 0 0	0 0 0 0	0 0 0 1
0 0 0	0 0 1 0	0 1 0 0	0 0 0 1	1 0 0 0	0 1 0 0	0 0 0 0	0 0 1 0
0 0 0	0 0 1 0	0 0 1 0	1 0 0 0	0 0 0 1	0 0 1 0	0 0 0 0	0 1 0 0
0 0 0	0 0 1 0	0 0 0 1	0 0 1 0	0 1 0 0	0 0 0 1	0 0 0 0	1 0 0 0
0 0 0	0 0 0 1	1 0 0 0	0 0 0 1	0 1 0 0	0 0 1 0	1 0 0 0	0 0 0 0
0 0 0	0 0 0 1	0 1 0 0	0 0 1 0	0 0 0 1	1 0 0 0	0 1 0 0	0 0 0 0
0 0 0	0 0 0 1	0 0 1 0	0 1 0 0	1 0 0 0	0 0 0 1	0 0 1 0	0 0 0 0
0 0 0	0 0 0 1	0 0 0 1	1 0 0 0	0 0 1 0	0 1 0 0	0 0 0 1	0 0 0 0

Table 3.5: *A completed incidence matrix of a finite projective plane of order* 5.

Let us denote these square sub-matrices of size $n-1$ by $C_{i,j}$, where $1 \leq i, j \leq n+2$. The blocks $C_{1,1}$ up to $C_{n+2,3}$ were fixed by the normalized form, and include the chosen Latin square. The blocks $C_{1,4}$ up to $C_{2,n+2}$ follow automatically from the lexicographical order of appending the columns.

In a similar way as was done on page 28, we can now show that, for all $4 \leq l \leq n+2$, the blocks $C_{k,l}$ with $3 \leq k \leq n+2$ are also permutation matrices. Furthermore, they give Latin squares in a manner that is almost similar to the one of page 28. The same thing holds for the row blocks.

The question that arises is the following. Do these 'new found' Latin squares relate to the Latin square that was used in the search for the plane? Our guess is that they do. When looking at some small order examples, it appeared that the completed incidence matrices of the Desarguesian finite projective planes had even more structure. The aforementioned blocks were the exact same permutation blocks as formed our Latin square (and of course the all-zero block). When this is the case, the blocks $C_{3,3}$ up to $C_{n+2,n+2}$ form a block-Latin square of order n.

The biggest problems in the field of finite projective planes remain the following. Must every finite projective plane have prime power order? Must every plane of prime power order be Desarguesian?

In the field of Latin squares, the question for a formula for the number of Latin squares of order n remains unanswered. Lower bounds and upper bounds are known, but they are far apart for large n.

Appendix A

Encore: Fingerprinting

Here, we will give an isomorphism invariant for finite projective planes, the so-called *fingerprint*. The definition of this invariant is due to J.H. Conway. More on this fingerprint can be found in [2].

Given a finite projective plane π of order n, let B be the square matrix of size n^2+n+1 with entries B_{ij} defined as follows. For each line i we choose an arbitrary labeling $1, 2, \ldots, n+1$ of the $n+1$ points on i. Likewise, for each point j choose an arbitrary labeling $1, 2, \ldots, n+1$ of the $n+1$ lines through j. Now each line and each point has $n+1$ labels. For each non-incident line-point pair (i, j) the incidence relation and the labelings provide a bijection between the $n+1$ points on i and the $n+1$ lines through j. Relative to the chosen labeling, this gives a permutation σ_{ij} of order $n+1$. We define B_{ij} to be the sign[1] of the permutation σ_{ij} if j is not on i, and 0 if j is on i. In shorthand, using the incidence matrix A_π:

$$B_{ij} = \begin{cases} 0 & : \quad (A_\pi)_{ij} = 1 \\ \operatorname{sgn}(\sigma_{ij}) & : \quad (A_\pi)_{ij} = 0 \end{cases}$$

Definition 17 Let π be a finite projective plane of order n. The *fingerprint* $\mathcal{F}(\pi)$ of π is the multiset of absolute values of entries of BB^T.

Lemma 5 *The fingerprint $\mathcal{F}(\pi)$ of a finite projective plane π of order n is independent of the labeling of points and lines described above.*

Proof. Let π be a finite projective plane of order n with points j and lines i, where $j, i \in \{1, 2, \ldots, n^2+n+1\}$. Let, for each j, an arbitrary labeling of the lines through j be given and, for each i, an arbitrary labeling of the points on i be given. Consider the matrix B and the matrix BB^T for this given labeling. The k-th column of B corresponds to the point k and contains $\operatorname{sgn}(\sigma_{ik})$ in the i-th position if line i and point k are non-incident, and 0 if

[1] The sign of a permutation σ of order $n+1$ is defined as $(-1)^{\#\{(k,l):1\leq k<l\leq n+1, \sigma(k)>\sigma(l)\}}$.

they are incident. Consider two arbitrary lines through k. Both these lines have been labeled by point k. Suppose we interchange these two labels. This results in a transposition in the permutations $\sigma_{\bullet k}$. It is a well-known fact that a transposition changes the sign of a permutation, therefore this exchange of labels results in a change of sign for all $\mathrm{sgn}(\sigma_{ik})$ with line i non-incident with point k. We see that interchanging the labeling of two arbitrary lines results in a change of sign for all entries in a certain column (the point in which they meet and gave them their label) of B. It is easily verified that this does not change BB^T and therefore does not change the fingerprint $\mathcal{F}(\pi)$.

In a similar manner we see that interchanging the labels of two points results in a change of sign for all entries in a certain row of B corresponding to the line that contains both points and gave them their label. Suppose this happens in the k-th row of B. Now BB^T has changed, entries in the k-th row and k-th column have changed sign except for the (k,k)-entry. This has not changed the fingerprint $\mathcal{F}(\pi)$, because this is the multiset of the *absolute* values of entries of BB^T.

We now remark that any two arbitrary labelings can be transformed into each other by the described transpositions of line-labels and point-labels. Therefore the fingerprint $\mathcal{F}(\pi)$ is independent of the chosen labeling. □

Theorem 14 *The fingerprint is an isomorphism invariant of finite projective planes.*

Proof. Let π_1 and π_2 be two isomorphic finite projective planes of order n. Choose an arbitrary labeling of π_1. There exists a bijective mapping from the points of π_1 onto the points of π_2 that preserves collinearity (Remark 1 page 9). Applying this mapping to π_1 and all its labels gives us π_2 and a valid labeling on it.

With Lemma 5 we see now that π_1 and π_2 have the same fingerprint. The fingerprint is an isomorphism invariant of finite projective planes. □

$\mathcal{F}(\pi_{F_2})$	$\{*0^{42}, 4^{7}*\}$	$\mathcal{F}(\pi_{F_8})$	$\{*56^{5256}, 64^{73}*\}$
$\mathcal{F}(\pi_{F_3})$	$\{*0^{156}, 9^{13}*\}$	$\mathcal{F}(\pi_{F_9})$	$\{*0^{8190}, 81^{91}*\}$
$\mathcal{F}(\pi_{F_4})$	$\{*12^{420}, 16^{21}*\}$	$\mathcal{F}(\pi_{H_9})$	$\{*0^{858}, 8^{1404}, 12^{5616}, 72^{312}, 81^{91}*\}$
$\mathcal{F}(\pi_{F_5})$	$\{*0^{930}, 25^{31}*\}$	$\mathcal{F}(\pi_{N_9})$	$\{*68^{6480}, 72^{1710}, 81^{91}*\}$
$\mathcal{F}(\pi_{F_7})$	$\{*0^{3192}, 49^{57}*\}$	$\mathcal{F}(\pi_{N'_9})$	$\{*36^{80}, 56^{1620}, 72^{6490}, 81^{91}*\}$

Table A.1: *Fingerprints of all finite projective planes up to order* 9.

I wrote a program in MAGMA to compute fingerprints of finite projective planes and tested it on all known planes of order up to 27. We compared our results with known[2] fingerprints and were even able to correct some minor mistakes. In table A.1 we give fingerprints of all the finite projective planes up to order 9.

[2]See `http://www.uwyo.edu/moorhouse/pub/planes/`

Appendix B

Magma Code

In this appendix, some of the MAGMA code is given and briefly explained. We shall do this by walking through the program and functions in order of appearance when computing a small example. This example will be the fourth Latin square from a list of 12 non-paratopic representative Latin squares, see Appendix C.

We start by calling our main function EXPANDTOK with parameters (6,4,57), which are the order of the Latin square, the number of the chosen Latin square and the number of columns the incidence matrix should be completed to, respectively.

```
function expandtoK(lsqorde,nummer,K);
      lijstdun,INC:=initializer(lsqorde,nummer);
      Sort(~lijstdun);
      lijst2:=[];
      print "creating hulpmatrix";
      H:=hulpmatrix(lijstdun);
      indexset:=[1..#lijstdun];
      trackerK(lsqorde+1,K,~lijst2,~H,indexset,[]);
      return [converter(w,INC,lijstdun): w in lijst2];
end function;
```

The first thing this function does is call the function INITIALIZER with parameters (6,4), the order and the number.

```
function initializer(lsqorde,nummer);
   L:=readsquare(lsqorde,nummer);
   print "created latin square";
   INC:=square2inci(L);
   print "created partial incidence matrix";
   print "now creating list of possible columns";
   list:=COLGEN(lsqorde+1);
   print "found ",#list,"continue with first flushing";
   list:=uitdunnen(L,list);
   print #list,"left, creating final list";
```

```
   list:=superdunner(L,list);
   print "done, found ",#list;
   return list,INC;
end function;
```

The READSQUARE function reads the data for the fourth Latin square of order 6 from the list and returns the 6×6 Latin square `L` in matrix form. The function SQUARE2INCI returns `INC`, the partial incidence matrix, when `L` is inputed. Then COLGEN is called with input 7.

```
function COLGEN(n);
   R:=[];
   list:=[];
   n1:=[1..n-1];
   n2:=[1..n-2];
   SS:=SymmetricGroup(n-2);
   for k in n1 do
      E:=Exclude(n1,k);
      for e in [[E[s^g] : s in n2 ]:g in SS] do
         for i in n1 do
            for j in n1 do
               list cat:=[[i,j,k] cat Insert(e,i,0)];
            end for;
         end for;
      end for;
   end for;
   return list;
end function;
```

COLGEN(7) returns a `list` of 25920 columns that can possibly be appended, based on the unembedded partial incidence matrix. Next, the function UITDUNNEN with input (`L,list`) prunes the list of columns to 11124 columns, and the function SUPERDUNNER reduces this number even further to a maximum of 288 possible columns.

```
function uitdunnen(L,lijst);
   R:=[];
   n:=NumberOfRows(L)+1;
   n1:=[1..n-1];
   for t in [1..#lijst] do
      l:=lijst[t];
      for j in n1 do
         if l[2] eq j then
            for i in n1 do
               if l[3+i] eq L[i][j] then
               continue t;
               end if;
            end for;
         end if;
      end for;
         R cat:=[t];
```

```
   end for;
   return lijst[R];
end function;

function superdunner(L,lijstdun);
   shortcodedL:=generatecolumns(L);
   Z:=[l : l in lijstdun | codedLinprod(l,shortcodedL)];
   return Z;
end function;

function codedLinprod(R,shortcodedL);
   C:=[];
   numc:=#shortcodedL[1];
   for i in Exclude([1..#shortcodedL],R[2]) do
      c:=shortcodedL[i];
      w:=0;
      for j in [1..numc] do
         if (R[3+j] eq c[j]) then
               w+:=1;
            if w gt 1 then
               return false;
            end if;
         end if;
      end for;
      if w eq 1 then
         continue i;
      else
         return false;
      end if;
   end for;
   return true;
end function;
```

The function GENERATECOLUMNS creates from `L` a list of its 6 columns, which CODEDLINPROD uses to reject possible columns which do not fulfill the correct inner product requirements.

We now return to our function EXPANDTOK where we sort our list of 288 lexicographically, create an empty list `lijst2` in which we store the generated completed incidence matrix (if any) and call the function HULPMATRIX which returns the compatibility matrix `H`.

```
function hulpmatrix(lijst);
   N:=#lijst;
   r:=#lijst[1];
   hulpmat:=SparseMatrix(N,N);
   for i in [1..#lijst] do
      R:=lijst[i];
      for j in [i+1..#lijst] do
         w:=0;
```

```
         Q:=lijst[j];
         for t in [1..r] do
            if (R[t] eq Q[t]) and (R[t] ne 0) then
               w +:=1;
            end if;
            if w gt 1 then
               continue j;
            end if;
         end for;
         if w eq 1 then
            hulpmat[i][j]:=1;
         end if;
      end for;
   end for;
   return hulpmat;
end function;
```

Instead of working with the actual list of columns, we only work with their number in the sorted list, for this we use `indexset`. With the compatibility matrix `H` we have all the information we need. We call the backtrack procedure TRACKERK with input (`7,57,~ lijst2,~ H,indexset,[]`).

```
procedure trackerK(n,K,~leeg,~H,indexset,added);
   NC:=3*n+#added;
   if (NC eq K) then
      Append(~leeg,added);
      print "           ",#leeg;
   else
      for i in indexset do
         indexset2:=[k : k in indexset | H[i][k] eq 1];
         if (K-NC-1) le #indexset2 then
            trackerK(n,K,~leeg,~H,indexset2,Append(added,i));
         end if;
      end for;
   end if;
end procedure;
```

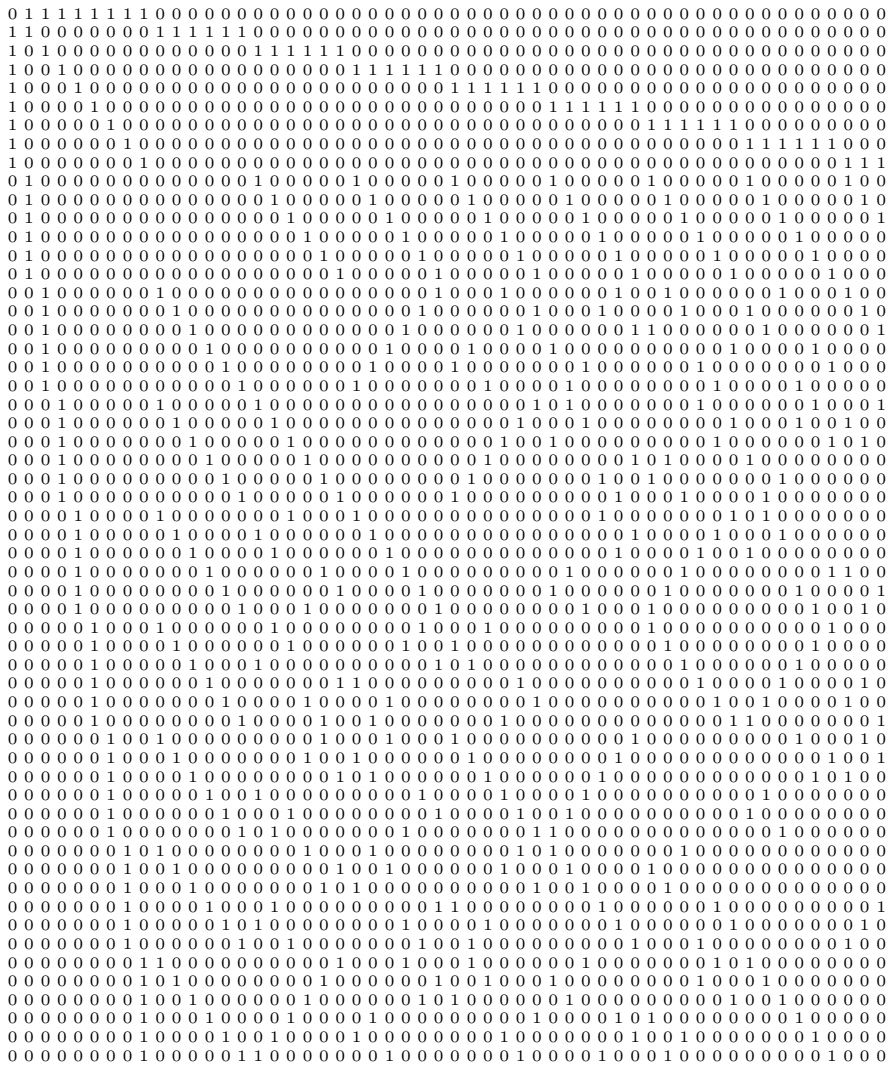
Within 5 seconds, TRACKERK finished its search and found 2 complete incidence matrices. The referenced variable `leeg` has become an array of two arrays of column numbers.

[[1, 12, 19, 30, 37, 48, 56, 62, 69, 76, 83, 89, 99, 105, 116, 125, 136, 142, 149, 155, 168, 169, 182, 188, 196, 207, 213, 220, 226, 237, 241, 252, 258, 271, 277, 288],
[7, 13, 24, 25, 36, 42, 49, 60, 66, 79, 85, 96, 104, 111, 117, 124, 130, 137, 150, 156, 167, 170, 181, 187, 195, 208, 214, 219, 225, 238, 243, 250, 259, 270, 279, 286]]

The function CONVERTER reconstructs the actual completed incidence matrices.

```
function converter(V,INC,lijstje);
   W:=Matrix(INC);
   for v in V do
      l:=lijstje[v];
      NULCOL:=ZeroMatrix(Integers(),#INC,1);
      for i in [1..#l] do
         if l[i] ne 0 then
               NULCOL[3+l[i]+(#lijstje[1]-3)*(i-1)][1]:=1;
         end if;
      end for;
      W:=HorizontalJoin(W,NULCOL);
      end for;
      return W;
end function;
```

One out of two completed incidence matrices of a finite projective plane of order 7 the program returns.



Appendix C

Data

These are the used representative Latin squares for the orders 4 to 7 as generated and stored[1] by Brendan McKay, encoded in the obvious way.

1 1234214334124321
2 1234241331424321

1 12345235143542141253541 32
2 12345241533542141532532 14

1 1234562143653561424652315316246425 13
2 1234562315643126454651325462136543 21
3 1234562315643126454653215461326542 13
4 1234562316453125644652135461326543 21
5 1234562316453452614165235623146541 32
6 1234562451633126454365125612346543 21
7 1234562451633126454562315643126315 24
8 1234562451633562414613255146326325 14
9 1234562451633642154365215126346513 42
10 1234562563143621454352615416326145 23
11 1234562643153561244352615416326125 43
12 1234562645313426154512635361246153 42

1 1234567214375637561424321675561732465724137465231
2 1234567215734635261744362715547162367432517615432
3 1234567217563436427154723156546137263574217516243
4 1234567231574631264754657231547361267421537561324
5 1234567231674531254764657213574263164713527563124
6 1234567231675431276454675213576243165413727453126
7 1234567231745631657424621375574263165731247456213
8 1234567231764531254764756231642713657132474631 52
9 1234567231764537264514175236564271364531727561324
10 1234567234167537621544153726547621365274317615342
11 1234567234175634276154756231516347265721437615324
12 1234567234175635674124173625542637167152347652143
13 1234567234567135274164162753571632464712357653142
14 1234567234571636274514173625541637267521347561243
15 1234567234617537652144153726567243165173427421653
16 1234567234715635716244613275542671367524317165342
17 1234567234761535764214163752612374675124374251 36
18 1234567235174636274154562173571623464753217143652
19 1234567235617436427514715623547321661273457561432
20 1234567235617436724154763251541763265217437145326
21 1234567235647131476254763152547231665217437615234
22 1234567235647137256144512736516724364731257641352
23 1234567235671435271464612375574162364732517165432
24 1234567235671435271464615273574263164713527163425
25 1234567235741631657244513672672341674123574261 53
26 1234567235764131457264673152576241365213747416235
27 1234567236147536457124753126547263165172437126354
28 1234567236175435271464675321514267367534127416235
29 1234567236517437214564652713547632161472357513642
30 1234567236571435416724627351571324661724357456123
31 1234567236714535467124175236562147367123547453621
32 1234567237165434621754625731574621365173427153426
33 1234567237514637564124167235561237464217537543621
34 1234567237561437461254152736562347164173527561243
35 1234567237615437452164652731542167365173427163425
36 1234567237645136257144563172574123664173257152643
37 1234567241537636427154376152576342161572437521634
38 1234567241567331724564526731564731267531247361245
39 1234567241675337651244351672567234161274357543216
40 1234567241735631726454526173564173267534217365214
41 1234567241735637561244673215536247161257437541632
42 1234567245367131472564615732576132463721457526413
43 1234567245367131657244376152564721367214357512346
44 1234567245617335617244372615562743167153427143256
45 1234567245671336274514712635534127665731247165342
46 1234567245673136712544512376536741267231457145623
47 1234567245673136712544715326516347265271437342615
48 1234567245713635614724673215574632163127547125643
49 1234567246175335476214623175571234661752347356412
50 1234567246317537564214521736564731261752437312654
51 1234567246375135416724715236562741363721457156324
52 1234567246537135716424357126562371467124357146253
53 1234567246715331462754715326567143263527417523614
54 1234567246715331562744573612571243663457217621345
55 1234567246715337416254652731531627465734127125346
56 1234567247135631426754765123561743265237417356214
57 1234567247135635476124613275516274367251347356421
58 1234567247135635624714127635561374267451237356214
59 1234567247135635674124352671571623461257437643125
60 1234567247163537251464562371514672363174527653214
61 1234567247361531562744765321562174365471327312456
62 1234567247613537526414613752534721665214737165324
63 1234567247631536571424512673516372467254317341256
64 1234567251367431257464367125574621364713527652431
65 1234567251367436417524376215576234164571237125436
66 1234567251374637461254167352567243163512747425613
67 1234567251637431572464623751574162364751327362415
68 1234567251637437621454357216547362161457327621453
69 1234567251673436451724367215517234667234517451623
70 1234567251734631264754652713537162467452317463152
71 1234567251734636521744375612576342164217537146235
72 1234567251743634762154625173536174267423517153624
73 1234567251764337514264376215546237161457327623154
74 1234567254617331276454362751567341267512347415326
75 1234567254637136721544315726516724367514327423615
76 1234567254713636712544753621512674363124757465312
77 1234567254713637652144176325624736352741741362 5
78 1234567254761337621544176325562347163517427415236
79 1234567254763136217454365172571342661723547456213
80 1234567256317434756214317256564271367214357156342
81 1234567256371436751424157326534627167214357412653
82 1234567256371437462514357126542167361724357615342
83 1234567256714331452764752631562714647135273164 25
84 1234567256741331426754726351547123663157427653124
85 1234567257134631564724623751571263463471257465213

[1] http://cs.anu.edu.au/~bdm/data/

86 1234567257134636521744763215541673263274517145623
87 1234567257143636527414367152572631461452737413625
88 1234567257361431674254716253564137264257317352146
89 1234567257364131562744725136564271363174527461325
90 1234567257613434217564312675516724367534217645312
91 1234567257631431576424315726546327167214537642135
92 1234567257631437614254652173514723663257417413652
93 1234567257631437624514623175514762363157427451236
94 1234567257631437624514623175531724661457237451632
95 1234567261573435724164167325542167367532417346152
96 1234567261734534561724723651534271665714237165234
97 1234567261734535461724761253517243664537217325614
98 1234567261743531657244376152572164364523717543216
99 1234567264175337651244357216541367261724357526341
100 1234567264175337651244527631531647264732157152346
101 1234567264537134761524152736572361463174257561243
102 1234567264573131672454512673537641267231547451326
103 1234567264715335716244316275546371267524317125346
104 1234567264735135726144365172572143664137257156243
105 1234567264735137216454165723572416651327474561 32
106 1234567265173431264754762153534761264753217513246
107 1234567265173437456124562371517342663172457426153
108 1234567265347134752164716325516274363471527521634
109 1234567265714334716254713256536247161457327526314
110 1234567265714335427164325671571623461734527461325
111 1234567265743135427164765123541637263712547123645
112 1234567267135437251464563712514267363574217416235
113 1234567267143537526414365172542731665137247146253
114 1234567267315435614724725613514723663527417416325
115 1234567267534134517264716253514763265231747362415
116 1234567271364536714524125736546732165421737356214
117 1234567271534634671254156273562714637245175416 32
118 1234567271563431527464376125546731265234717641253
119 1234567271563434672154573126512647363427517651342
120 1234567271635431674254652173547123663257417543612
121 1234567271643536751424127653536172464532717542316
122 1234567274163531652744653721537241665271437416352
123 1234567274163534562714613752537241665271437165324
124 1234567274513634612754572613562734161537247316452
125 1234567274531636274514516273536174264721357153624
126 1234567274561335672414312756567132464231757156432
127 1234567274613531526744675312536742164217537513246
128 1234567274613536712544365721542731665134727152643
129 1234567274615335714264365712542763161532747612345
130 1234567274631535716424365271561273461274537453126
131 1234567274635135217464372615561327464571237165432
132 1234567275164335761244367215514273664153727623451
133 1234567275364131764524615273536172464271357542316
134 1234567275364134271564612375537641265417237165234
135 1234567275641335217464317625564237161732547465132
136 1234567275641336752414317625514273665213747463152
137 1234567275643134216754672153534721665137247165342
138 1234567276134534567124625173517342663472517512634
139 1234567276134536721544156732541762365234717345216
140 1234567276135435461724652731517324663174257425613
141 1234567276145335726414356172562371464172357145326
142 1234567276341534561724175326561723463427517521643
143 1234567276345134572164516723562137463721457145632
144 1234567276513436524714526713541732663712457143652
145 1234567276514335764214357612562173461423757413256
146 1234567276534135427164623175547162363172547156432
147 1234567276543135267144652173537124664173257143652

Bibliography

[1] R.H. Bruck and H.J. Ryser, *The nonexistence of certain finite projective planes*, Canadian Journal of Mathematics **1** (1949), 88–93.

[2] C. Charnes, *Quadratic matrices and the translation planes of order* 5^5, Coding Theory, Design Theory, Group Theory, 1993, pp. 155–161.

[3] P. Dembowski, *Finite geometries*, first ed., Springer-Verlag, 1968.

[4] J. Dénes and A.D. Keedwell, *Latin squares and their applications*, first ed., English Universities Press Ltd., 1974.

[5] ———, *Latin squares*, first ed., North-Holland, 1991.

[6] Marshall Hall Jr., J.Dean Swift, and Raymond Killgrove, *On projective planes of order nine*, Mathematical Tables and Other Aids to Computation **13** (1959), no. 68, 233–246.

[7] Daniel R. Hughes and Fred C. Piper, *Projective planes*, first ed., Springer-Verlag, 1973.

[8] Donald E. Knuth, *Estimating the efficiency of backtrack programs*, Mathematics of Computation **29** (1975), no. 129, 121–136.

[9] G. Kolesova, C.W.H. Lam, and L. Thiel, *On the number of* 8×8 *latin squares*, Journal of Combinatorial Theory A **54** (1990), 143–148.

[10] C.W.H. Lam, *The search for a finite projective plane of order 10*, The American Mathematical Monthly **98** (1991), no. 4, 305–318.

[11] C.W.H. Lam, G. Kolesova, and L. Thiel, *A computer search for projective planes of order 9*, Discrete Mathematics **92** (1991), 187–195.

[12] Brendan D. McKay, *Isomorph-free exhaustive generation*, Journal of Algorithms **26** (1998), 306–324.

[13] E.T. Parker and R.B. Killgrove, *A note on projective planes of order nine*, Mathematics of Computation **18** (1964), no. 87, 506–508.

[14] Herbert John Ryser, *Combinatorial mathematics*, first ed., The Mathematical Association Of America, 1963.

[15] Frederick W. Stevenson, *Projective planes*, first ed., W.H. Freeman and Company, 1972.

[16] M.G. Tarry, *Le problème des 36 officiers*, Association Française pour l'Avancement des Sciences, compte rendu de la 29^{me} session **1** (1901), 170–203.

List of Notations

Notation	Description	
A_π	An incidence matrix for π	6
B_i	A square submatrix relating to a Latin square	28
H	The compatibility matrix	30
L^{RC}	The transpose of L	21
$M_k(L)$	The k-s-matrix of L	21
N_π	The normalized incidence matrix of π	25
Σ	A plane $(\mathcal{P}, \mathcal{L}, \mathcal{I})$	4
Σ^d	The dual of the plane Σ	8
$\mathbb{L}$	The collection of Latin squares	20
$\mathcal{F}(\pi)$	The fingerprint of a finite projective plane π	41
$\mathcal{I}$	The incidence set	4
$\mathcal{I}^{-1}$	The dual incidence set.	8
$\mathcal{L}$	Set of lines	4
$\mathcal{M}(M)$	The multiset of entries of the matrix M	21
$\mathcal{P}$	Set of points	4
$\mathcal{S}_k(L)$	The k-s-Structure of L	21
$\mathrm{sgn}(\sigma)$	The sign of the permutation σ	41
$\pi \sim \pi'$	Two isomorphic finite projective planes	8
π	A finite projective plane	4
π^d	The dual of π	8
π_{F_9}	The Desarguesian plane of order 9	12
π_{H_9}	The Hughes plane of order 9	12
$\pi_{N'_9}$	The left nearfield plane of order 9	13
π_{N_9}	The right nearfield plane of order 9	13
σ_{ij}	Permutation induced by line i and point j	41
$\{*\ldots*\}$	A multiset	20
RC	Rows and columns interchanging roles	17

Index

Class
    isotopy, 16
    main, 16
Collinear, 4
Complete, 18
Concurrent, 4
Conjugacy
    operations, 16

Dual
    plane, 8
    self-, 9
Duality, 5

Fingerprint, 41
Finite projective plane, 5
Four-point, 4

Graeco-Latin square, 17

Incidence matrix, 6
Invariant, 20
Isomorphic, 8
Isomorphism, 8
Isotopic, 16
Isotopy, 16
    classes, 16
    operations, 16

k-s-Matrix, 21
k-s-Structure, 21
k-s-Transversal, 19

Latin square, 15
    isotopic, 16
    orthogonal, 17
    paratopic, 16
    reduced, 15

Main classes, 16
Matrix
    $(0,1)$-, 6
    k-s-, 21
    monomial, 20
MOLS, 17
Monomial matrix, 20
Multiset, 20

Order, 6
Orthogonal, 17
Orthogonal array representation, 15

Parallel, 4
Paratopic, 16
Plane, 4
    dual, 8
    finite projective, 5
    order of, 6
    projective, 4
Projective plane, 4

Reduced, 15
Reduced column, 31

Self-dual, 9
Structure
    k-s-, 21

Transversal, 17
    k-s-, 19

Weight, 7