# On elliptic semiplanes, an algebraic problem in matrix theory, and weight enumeration of certain binary cyclic codes

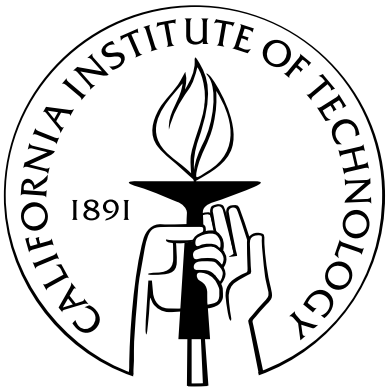
Thesis by

Brian Schroeder

In Partial Fulfillment of the Requirements

for the Degree of

Doctor of Philosophy




California Institute of Technology

Pasadena, California

2010

(Defended September 24, 2009)

# Acknowledgements

I could never have finished this work without the advice and support of so many amazing people. I wrote this alone, but the writing was only the final step.

Most of all, I would like to thank my parents, Duff and Vicki Schroeder. I could never have done this without you. Thank you for everything. You were right all along, Mom.

I would like to thank my adviser at Caltech for the past four years, Dr. Rick Wilson. Thank you for your advice and patience, working with me for all this time. I really appreciate everything you have done for me.

My mentor from Michigan State University (MSU), Dr. Jon Hall, helped me with the chapter on elliptic semiplanes, which was based on work we did while I was an undergraduate at MSU. Thank you, Dr. Hall.

My family, including my sisters Ashlee and Kenzee, my brother-in-law Loren, my grandparents Jo Bancroft, Keith Schroeder, Bev Schroeder, and everyone in my extended family, all offered me encouragement while I was working on this thesis. It was worth more than you know. Thank you all for believing in me.

# Abstract

An *elliptic semiplane* is a $\lambda$-fold of a symmetric 2-$(v, k, \lambda)$ design, where parallelism is transitive. We prove existence and uniqueness of a 3-fold cover of a 2-$(15, 7, 3)$ design, and give several constructions. Then we prove that the automorphism group is $3 \cdot Alt(7)$. The corresponding bipartite graph is a minimal graph with valency 7 and girth 6, which has automorphism group $3 \cdot Sym(7)$.

A polynomial with real coefficients is called *formally positive* if all of the coefficients are positive. We conjecture that the determinant of a matrix appearing in the proof of the van der Waerden conjecture due to Egorychev [5] is formally positive in all cases, and we prove a restricted version of this conjecture. This is closely related to a problem concerning a certain generalization of Latin rectangles.

Let $\omega$ be a primitive $n$th root of unity over $GF(2)$, and let $m_i(x)$ be the minimal polynomial of $\omega^i$. The code of length $n = 2^r - 1$ generated by $m_1(x)m_t(x)$ is denoted $C_r^t$. We give a recursive formula for the number of codewords of weight 4 in $C_r^{11}$ for each $r$.

# Contents

# List of Tables

# List of Figures

# Chapter 1

# Introduction

In this thesis, we examine three separate topics in combinatorics. The topics covered range from Latin rectangles and more general objects, polynomial eigenvalues of matrices, binary cyclic codes, and design and graph theory.

In Chapter 2 we consider a matrix found in the first proofs of the van der Waerden conjecture about permanents of doubly stochastic matrices. The original proofs consider the signs of the eigenvalues of a certain $n \times n$ matrix, using analysis to show that the number of positive and negative eigenvalues does not change under certain continuous operations on the entries of the matrix. The eigenvalues are shown to satisfy the desired conditions when all variables lie on the unit interval. We aim towards a proof that does not use analysis, but instead uses an algebraic and combinatorial approach. In a restricted setting we show the stronger result that the determinant is a polynomial in the variables with all positive coefficients.

Our approach relates this problem to a problem about generalized Latin rectangles. More specifically, we consider $m \times n$ arrays with entries from $\{1, \ldots, n\}$, first row $1, 2, \ldots, n$, second row a permutation of the set $\{1, \ldots, n\}$, and arbitrary later rows that satisfy the condition that no entry is repeated in any column. We are interested in counting the difference between the number of those arrays with odd and even permutations in the second row.

In Chapter 3 we consider a generalization of binary BCH codes. In particular we consider those codes generated by the minimal polynomials of two roots of unity over $GF(2)$. A recent result of Hernando and McGuire [8] gives a solution to the problem

of which families of two root codes have an infinite family of 2-error correcting codes of increasing lengths. We consider the problem of enumerating the number of codewords of weight 4 for those two root codes which are *not* 2-error correcting. In particular, we find a formula for the number of codewords of weight 4 in the code generated by the first and 11th powers of a primitive root of unity over $GF(2)$ with length $2^r - 1$, in terms of $r$.

Finally, in Chapter 4, we give a proof of the existence and uniqueness of an elliptic semiplane on 45 points. We give an algebraic construction of the associated graph using the line graph of the Petersen graph. Then we use these two constructions to give a proof that the automorphism group of the elliptic semiplane is $3 \cdot Alt_7$, the nonsplit central extension of $Alt_7$, and the automorphism group of the bipartite graph is $3 \cdot Sym_7$.

We then briefly turn to the subject of cages. It is known that the cage with valency 7 and girth 6 has 90 vertices, and it was constructed by O'Keefe and Wong [18]. Our construction of the cage is simpler and does not appeal to a computer search. But we are only able to show uniqueness of the cage under the condition that the cage is also a 3-cover. A computer search is still required to to show uniqueness of the cage in general.

# Chapter 2

# Formal Positivity of Eigenvalues of a Matrix

## 2.1 Preliminaries

### 2.1.1 Conjecture of van der Waerden concerning permanents

The determinant of a square matrix is a well-known function, in which the sum depends on the sign of the permutations. If we remove the sign of the permutation, we get another function, the permanent, which has also been the object of much study.

**Definition 2.1.1.** *Let $A$ be an $n \times n$ matrix with entries $a_{ij}$ for $i = 1, \ldots, n$ and $j = 1, \ldots, n$. Then the* permanent *of $A$, denoted* per $A$*, is defined as*

$$\text{per } A = \sum_{\sigma \in S_n} a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)},$$

*where $S_n$ is the symmetric group on $\{1, \ldots, n\}$.*

The main conjecture about the permanent, which is now a theorem, is the so-called van der Waerden's permanent conjecture. The conjecture concerns the value of the permanent of doubly stochastic matrices.

**Definition 2.1.2.** *Let $A$ be an $n \times n$ matrix. Then $A$ is called* doubly stochastic *if and only if the following conditions hold:*

(i) *each entry of $A$ is a real number in the closed interval* $[0, 1]$,

(ii) *for each row, the sum of the entries in that row is* 1, *and*

(iii) *for each column, the sum of the entries in that column is* 1.

The long standing conjecture, which was proven in 1981 is the following theorem.

**Theorem 2.1.3** (van der Waerden's permanent conjecture)**.** *Let $A$ be an $n \times n$ doubly stochastic matrix. Then* per $A \geq n!/n^n$, *and equality holds if and only if every entry of $A$ is* $1/n$.

*Proof.* See [5] and [6] for the two original proofs. □

The results in the next section are related to a conjecture which would generalize part of the proof given in [5].

### 2.1.2 Generalized Latin rectangles

In this paper, we will consider a type of generalization of Latin rectangles for which there does not appear to be consistent terminology in the literature. For reference, we will define most of the terms here.

We will be using somewhat nonstandard terminology. A column-subLatin rectangle does not necessarily satisfy the condition that each row contains each symbol exactly once.

**Definition 2.1.4.** *Let $M$ be an $r \times n$ matrix with $r \geq 2$. Then $M$ is a* reduced column-subLatin rectangle *if and only if the following conditions hold:*

(i) *each entry of $M$ is in the set* $\{1, \ldots, n\}$,

(ii) *the first row of $M$ is* $(1, 2, \ldots)$, *the identity permutation on* $\{1, \ldots, n\}$,

(iii) *the second row of $M$ is a permutation of* $\{1, \ldots, n\}$, *and*

(iv) *the matrix $M$ satisfies the column subLatin condition, that is, no symbol occurs more than once in any column.*

**Definition 2.1.5.** *A reduced column-subLatin rectangle $M$ is called* second-even *or* second-odd *as the second row is an even or odd permutation, respectively. A Latin rectangle is called* even *or* odd *as the product of the row permutations is an even or odd permutation.*

### 2.1.3 Formally positive polynomials

We call a polynomial formally positive if each of its coefficients is positive. To be precise, we give the following definition.

**Definition 2.1.6.** *Let $f$ be a polynomial with real coefficients and commutative variables taken from the set $S$. Write $f$ as a sum of monomials, in reduced form, that is, such that no two monomials have the same product of variables.*

*For a finite product $p$ of positive integral powers of variables from $S$, let $f_p$ denote the coefficient on $p$ in $f$.*

*If for every $p$, $f_p = 0$, then $f$ is called* formally zero.

*If for every $p$, $f_p \geq 0$, and $f$ is not formally zero, then $f$ is called* formally positive.

*If for every $p$, $f_p \leq 0$, and $f$ is not formally zero, then $f$ is called* formally negative.

There are a few facts about formally positive polynomials which are easily seen to be true.

**Proposition 2.1.7.** *Let $M$ be the set of formally positive polynomials with variable set $S$. Then the following are true:*

(a) *Let $f, g \in M$. Then $f+g \in M$. That is, $M$ is closed under polynomial addition.*

(b) *Let $f, g \in M$. Then $fg \in M$. That is, $M$ is closed under polynomial multiplication.*

(c) *Let $f \in M$, $c \in \mathbb{R}$, $c > 0$. Then $cf \in M$. That is, $M$ is closed under scalar multiplication.*

(d) *Let $f \in M$, and let $g : S \to \mathbb{R}$ be a function such that $g(s) > 0$ for each $s \in S$. Let $f(g)$ represent the evaluation of $f$ with $s = g(s)$ for each $s \in S$. Then $f(g) > 0$.*

### 2.1.4 Interlacing of eigenvalues

The general interlacing of eigenvalues Lemma proven in [24] is the following.

**Lemma 2.1.8.** *Let $A$ be a symmetric matrix of order $n$ with eigenvalues*

$$\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n.$$

*Suppose $N$ is an $m \times n$ real matrix such that $NN^T = I_m$, so $m \leq n$. Let $B := NAN^T$, and let*

$$\mu_1 \geq \mu_2 \geq \cdots \geq \mu_m$$

*be the eigenvalues of $B$. Then the eigenvalues of $B$ interlace those of $A$, in the sense that*

$$\lambda_i \geq \mu_i \geq \lambda_{n-m+i}$$

*for $i = 1, 2, \ldots, m$.*

In our situation, the matrices are upper left principal submatrices, and we apply Lemma 2.1.8 repeatedly to examine the signs of the eigenvalues of the full matrix.

**Lemma 2.1.9.** *Let $A$ be a symmetric matrix of order $n$ and for each $r = 2, \ldots, n$ let $A_r$ be the upper left $r \times r$ principal submatrix of $A$. Suppose that $\det A_r$ is negative for each even $r$ and positive for each odd $r$. Then $A$ has $n - 1$ negative eigenvalues and one positive eigenvalue.*

*Proof.* For each $r = 2, \ldots, n$, let the eigenvalues of $A_r$ be

$$\lambda_{r1} \geq \lambda_{r2} \geq \cdots \geq \lambda rr.$$

For each $n > r \geq 2$, let $N_r$ be the $r \times (r + 1)$ matrix given by

$$N_r = (I_r | o_r),$$

where $o_r$ is the $r$-dimensional column zero vector. We have $A_r = N_r A_{r+1} N_r^T$. So by

Lemma 2.1.8, we have

$$\lambda_{r+1,i} \geq \lambda_{r,i} \geq \lambda_{r+1,i+1}$$

for $i = 1, \ldots, r$.

Now $\lambda_{21}\lambda_{22} < 0$ since $\det A_2 < 0$, so

$$\lambda_{21} > 0 > \lambda_{22}.$$

By way of induction, suppose that for some $2 \leq r < n$ we know that

$$\lambda_{r,1} > 0 > \lambda_{r,2} \geq \cdots \geq \lambda_{r,r}.$$

Then we have

$$\lambda_{r+1,1} \geq \lambda_{r,1} > 0,$$

and $0 > \lambda_{r,i} \geq \lambda r + 1, i + 1$ for each $i = 2, \ldots, r$. So the product

$$\lambda_{r+1,1}\lambda_{r+1,3} \cdots \lambda_{r+1,r+1}$$

has the same sign as $\det A_r$. But $\det A_{r+1}$ has the opposite sign of $\det A_r$, so $\lambda_{r+1,2} < 0$, and we have

$$\lambda_{r+1,1} \geq \lambda_{r,1} > 0 > \lambda_{r+1,2} \geq \lambda_{r,2} \geq \cdots \geq \lambda_{r,r} \geq \lambda_{r+1,r+1}.$$

This completes the proof. □

Note that, in the case of Lemma 2.1.9, the determinant of $A_1$ is not relevant to determining the signs of the eigenvalues of $A$. In our later application, we will in fact have $\det A_1 = 0$.

Let $n \geq 2$ and let $Q$ be the matrix such that

$$\boldsymbol{x}Q\boldsymbol{y}^T = \text{per } (\boldsymbol{a}_1, \ldots, \boldsymbol{a}_{n-2}, \boldsymbol{x}, \boldsymbol{y}),$$

where

$$\boldsymbol{a}_i = (a_{i1}, a_{i2}, \ldots, a_{in})$$

and per $(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_{n-2}, \boldsymbol{x}, \boldsymbol{y})$ denotes the permanent of the $n \times n$ matrix with row vectors given by the parameters, as defined in Definition 2.1.1. In Egorychev's proof of the van der Waerden conjecture, and in related proofs, an important step is equivalent to showing that when each of the $a_{ij}$ are positive, $n-1$ of the eigenvalues of $Q$ are negative, and the other is positive.

## 2.2 Problems Concerning Column-subLatin Rectangles and Eigenvalues of $Q$

We conjecture that the following statement is true.

**Conjecture 2.2.1** (Determinant Form)**.** *Let $m \geq 2$ and let $A$ be the upper left $m \times m$ submatrix of $Q$. Then $(-1)^{m-1} \det A$ is formally positive and not formally zero as a polynomial in the $n(n-2)$ variables $a_{ij}$, $i = 1, \ldots, n-2$, $j = 1, \ldots, n$.*

We can apply Lemma 2.1.9 to Conjecture 2.2.1 to show the same result from Egorychev's proof, under less restrictive conditions and without using complex analysis.

We first make an observation which relates Conjecture 2.2.1 to reduced column-subLatin rectangles. Let $\boldsymbol{v}_i = (v_{i1}, v_{i2}, \ldots, v_{in})$ for each $i = 1, \ldots, n-2$ be a vector of nonnegative integers. Let $o$ and $e$ be the number of second-odd and second-even, respectively, reduced column-subLatin $n \times n$ rectangles with $m(2+i, j) = v_{ij}$, where $m(r, j)$ denotes the multiplicity of $j$ in row $r$ for each $1 \leq r, j \leq n$. Then $e - o$ is the coefficient on

$$\prod_{i=1}^{n-2} \prod_{j=1}^{n} a_{ij}^{v_{ij}}$$

in $\det Q$.

So we have the following, which is equivalent to the case of Conjecture 2.2.1 where $m = n$.

**Conjecture 2.2.2** (Rectangle Form)**.** *Let $n \geq 2$ and for each $i = 1, \ldots, n-2$, and each $j = 1, \ldots, n$, let $v_{ij}$ be a nonnegative integer. Let $o$ and $e$, respectively, be the number of odd and even reduced column-subLatin $n \times n$ rectangles, with $v_{ij}$ the multiplicity of $j$ in row $2+i$. Then $e - o \geq 0$ if $n$ is odd, and $e - o \leq 0$ if $n$ is even.*

It is natural to consider a modification of the problem of Conjecture 2.2.2 to column-subLatin rectangles with a smaller number of rows. For $k+2$ rows, this is equivalent to the problem of Conjecture 2.2.1 where for each $i > k$, we set $\boldsymbol{a}_i = (1, 1, \ldots, 1)$.

We make clear the relationship between the two conjectures by separating the two statements. In each we have $n \geq m \geq 2$, and $1 \leq k \leq n-2$.

**Statement 2.2.3** (Statement $P(n, m, k)$)**.** *Let $Q$ be the matrix such that*

$$\boldsymbol{x} Q \boldsymbol{y}^T = \text{per } (\boldsymbol{a}_1, \ldots, bfa_{n-2}, \boldsymbol{x}, \boldsymbol{y}),$$

*where*

$$\boldsymbol{a}_i = (a_{i1}, a_{i2}, \ldots, a_{in}),$$

*for each $i = 1, \ldots, k$, and $\boldsymbol{a}_i = (1, 1, \ldots, 1)$ for each $i = k+1, \ldots, n-2$. Let $A$ be the upper left principal $m \times m$ submatrix of $Q$. Then $(-1)^{m-1} \det A$ is formally positive.*

**Statement 2.2.4** (Statement $R(n, k)$)**.** *Suppose $V_1, \ldots, V_k$ are multisets of size $n$ with elements from $\{1, \ldots, n\}$. Consider all $(k+2) \times n$ reduced column-subLatin rectangles with row $2+i$ a permutation of $V_i$ for each $i = 1, \ldots, k$. Let $e$ be the number of such rectangles which are row-even and let $o$ be the number of them which are second-odd. Then $(-1)^{n-1}(e-o) \geq 0$, and further, for some choice of multisets $V_1, \ldots, V_k$, we have $(-1)^{n-1}(e-o) > 0$.*

By our discussion, we know that $P(n, n, k)$ is true if and only if $R(n, k)$ is true. Conjecture 2.2.2 is equivalent to the statement that for all $n$, $R(n, n-2)$ is true, and Conjecture 2.2.1 is equivalent to the statement that for all $n$ and for all $m$, $P(n, m, n-2)$ is true.

## 2.3 The case $P(n, m, 1)$

We consider Conjecture 2.2.1 in the case where $\boldsymbol{a}_i = (1, 1, \ldots, 1)$ for each $i = 2, \ldots, n-2$. We let $\boldsymbol{a}_1 = (a_1, \ldots, a_n)$ to simplify the notation. Let $s = a_1 + \cdots + a_n$. In this case we have

$$Q = \begin{bmatrix} 0 & s - a_1 - a_2 & s - a_1 - a_3 & \cdots & s - a_1 - a_n \\ s - a_2 - a_1 & 0 & s - a_2 - a_3 & \cdots & s - a_2 - a_n \\ \vdots & & \ddots & & \vdots \\ s - a_n - a_1 & s - a_n - a_2 & \cdots & s - a_n - a_{n-1} & 0 \end{bmatrix}.$$

In this section we will prove the Conjecture 2.2.1 in this special case. Our main theorem is the following.

**Theorem 2.3.1.** *The statement $P(n, m, 1)$ is true for all $n \geq m \geq 3$.*

This Theorem will follow from the special case $n = m$, by the following Lemma, because in this case there is a simple relationship between the entries of the upper left principal submatrices.

**Lemma 2.3.2.** *For each $n \geq m \geq 3$, the statement $P(m, m, 1)$ implies $P(n, m, 1)$.*

*Proof.* For $1 \leq i, j \leq m$, let $c$ be the $(i, j)$ entry of the $m \times m$ matrix $Q$ and $d$ be the upper left $m \times m$ submatrix of the $n \times n$ matrix $Q$ (which is in fact the same as the $(i, j)$ entry of the $n \times n$ matrix). If $i = j$ then $c = d = 0$, and otherwise

$$c + \sum_{i=m+1}^{n} a_i = d,$$

where $c$ is a linear combination of exactly $m - 2$ of the $a_i$. Perform the substitution

$$b_\ell = a_\ell + \frac{1}{m-2} \sum_{i=m+1}^{n} a_i,$$

for each $\ell = 1, \ldots, m$ on $d$. Then $c$ is just $d$ with each variable $a_\ell$ replaced by $b_\ell$ for each $\ell = 1, \ldots, m$. This substitution does not depend on the choice of $(i, j)$, so it can

be performed simultaneously on all entries. It is also a formally positive substitution, and reduces $P(n, m, 1)$ to $P(m, m, 1)$. □

**Theorem 2.3.3.** *The statement $P(n, n, 1)$ is true for all $n \geq 3$.*

We now immediately have the following Corollary.

**Corollary 2.3.4.** *Let $\boldsymbol{v} = (v_1, \ldots, v_n)$ be a vector of nonnegative integers. Let $o$ and $e$ be the number of odd and even, respectively, reduced column-subLatin $3 \times n$ rectangles with symbol $j$ appearing $v_j$ times in row 3 for each $j = 1, \ldots, n$. Then $e - o \geq 0$ if $n$ is odd and $e - o \leq 0$ if $n$ is even.*

In fact, $e - o$ in Corollary 2.3.4 is the coefficient on $\prod_{j=1}^{n} a_j^{v_j}$ in $\det Q$. So this is equivalent to $P(n, n, 1)$.

The case of $\boldsymbol{v} = (1, 1, \ldots, 1)$ corresponds to the difference between the number of even and odd $3 \times n$ reduced row Latin rectangles, by this

**Proposition 2.3.5.** *For each $n$, let $d_o(n)$ and $d_e(n)$ be the number of $3 \times n$ reduced row Latin rectangles with odd and even second row, respectively. Also let $c_o(n)$ and $c_e(n)$ be the number of $3 \times n$ reduced row Latin rectangles with the product of the second and third row permutations even and odd, respectively. Then $d_e(n) - d_o(n) = c_e(n) - c_o(n)$.*

To prove this proposition, we require the following Lemma.

**Lemma 2.3.6.** *The number of reduced $3 \times n$ Latin rectangles with odd second row and even third row is the same as the number of those with odd second row and odd third row.*

*Proof.* Let $\sigma \in S_n$ be an odd derangement, and let $P_\sigma$ be the permutation matrix corresponding to $\sigma$. Let

$$M_\sigma = J - I - P_\sigma.$$

Then $M_\sigma$ is a 0-1 matrix and $\det M_\sigma$ is the difference between the number of even derangements disjoint from $\sigma$ and the number of odd derangements disjoint from $\sigma$. It will suffice to show that $\det M_\sigma = 0$.

Let $m_1^{e_1} \cdots m_k^{e_k}$ be the cycle type of $\sigma$. A cycle of length $m$ can be written as a product of $m-1$ transpositions. So $\sigma$ can be written as a product of $\sum_{i=1}^{k} e_i(m_i - 1)$ transpositions. Since $\sigma$ is odd, at least one $m_i$ must be even. Let $(a_1, \ldots, a_m)$ be an even cycle in the disjoint cycle decomposition of $\sigma$.

Consider the rows corresponding to $a_1, \ldots, a_n$ in the matrix $M_\sigma$. Row $a_i$ contains a 1 in every position, except $a_i$ and $a_{i+1}$ (where we allow that $n+1 = 1$), and a 0 in positions $a_i$ and $a_{i+1}$. Consider the sum of all odd terms in this cycle, that is rows $a_1, a_3, a_5, \ldots, a_{n-1}$. Among these, each row contains a 1 in all positions disjoint from $a_1, a_2, \ldots, a_n$ and for every position among the $a_1, \ldots, a_n$, exactly one row contains a 0 and the rest contain 1. Therefore, the sum of these rows contains $n/2$ in each position disjoint from the $n$-cycle and $n/2 - 1$ in each position among the $n$-cycle. Similarly, the sum of the rows corresponding to even positions in the $n$-cycle is the same. That is, we have established a non-trivial linear dependence among the rows of $M_\sigma$. Therefore, $\det M_\sigma = 0$. □

*Proof of* Proposition 2.3.5. Let $b_{ee}(n), b_{eo}(n), b_{oe}(n)$, and $b_{oo}(n)$ be the number of $3 \times n$ reduced row Latin rectangles where the second row is even or odd as the first subscript is e or o, and the third row is even or odd as the second subscript is e or o.

We have

$$\begin{aligned} d_e(n) &= b_{ee}(n) + b_{eo}(n), \\ d_o(n) &= b_{oe}(n) + b_{oo}(n), \\ c_e(n) &= b_{ee}(n) + b_{oo}(n), \\ c_o(n) &= b_{oe}(n) + b_{eo}(n). \end{aligned}$$

Also it is clear that $b_{oe}(n) = b_{eo}(n)$, since the second and third rows can be swapped. So we have

$$d_e(n) - d_o(n) = b_{ee}(n) - b_{oo}(n),$$

and

$$c_e(n) - c_o(n) = b_{ee}(n) - 2b_{oe}(n) + b_{oo}(n).$$

The proposition is therefore equivalent to $b_{oe}(n) = b_{oo}(n)$. Therefore it follows from Lemma 2.3.6 □

In the special case where the third row is a permutation, Corollary 2.3.4 follows from a result of Zeng [26]:

**Proposition 2.3.7.** *[26] Let $S_{k,n}$ denote the difference between the number of even reduced Latin rectangles of size $k \times n$ and the number of odd ones. We have*

$$1 + \sum_{n \geq 1} S_{3,n} \frac{t^n}{n!} = e^{2t} \left[ \frac{(1-t)^2}{1+t} + \frac{t}{(1+t)^2} \right].$$

In fact,

$$\frac{(1-t)^2}{1+t} = 1 - 3t + 4t^2 - 4t^3 + 4t^4 - 4t^5 + \cdots,$$

$$\frac{t}{(1+t)^2} = t - 2t^2 + 3t^3 - 4t^4 + 5t^5 - 6t^6 + 7t^7 - \cdots.$$

So the coefficient on $t^m$ in

$$\sum_{n \geq 1} S_{3,n} \frac{t^n}{n!}$$

is

$$(-1)^{m-1}(m-4)$$

for $m \geq 2$. In particular the coefficient is

$$\begin{aligned} 2, &\quad m = 2, \\ -1, &\quad m = 3, \\ 0, &\quad m = 4, \\ (m-4), &\quad m \geq 5 \text{ odd}, \\ -(m-4), &\quad m \geq 5 \text{ even}. \end{aligned}$$

This proves the conjecture in the case where the third row is a permutation. Now we turn to the polynomial determinant interpretation of the problem to prove the other cases.

Adding each of rows $1, \ldots, n-1$ to row $n$, and factoring $(n-2)$ from row $n$, we have $\det Q = (n-2)\det Q'$ where

$$Q' = \begin{bmatrix} 0 & s-a_1-a_2 & s-a_1-a_3 & \cdots & s-a_1-a_n \\ s-a_2-a_1 & 0 & s-a_2-a_3 & \cdots & s-a_2-a_n \\ \vdots & & \ddots & & \vdots \\ s-a_1 & s-a_2 & \cdots & s-a_{n-1} & s-a_n \end{bmatrix}.$$

Now subtracting row $n$ from each of rows $1, \ldots, n-1$, row $i$ becomes a constant $-a_i$ except in the $i$th coordinate, where it is $a_i - s$, for each $i = 1, \ldots, n-1$. So, factoring $-1$ from each of rows $1, \ldots, n-1$, we have

$$\det Q = (-1)^{n-1}(n-2)\det Q'',$$

where

$$Q'' = \begin{bmatrix} s-a_1 & a_1 & a_1 & \cdots & a_1 & a_1 \\ a_2 & s-a_2 & a_2 & \cdots & a_2 & a_2 \\ a_3 & a_3 & s-a_3 & \cdots & a_3 & a_3 \\ \vdots & & & \ddots & \vdots & \vdots \\ a_{n-1} & a_{n-1} & a_{n-1} & \cdots & s-a_{n-1} & a_{n-1} \\ s-a_1 & s-a_2 & s-a_3 & \cdots & s-a_{n-1} & s-a_n \end{bmatrix}.$$

**Lemma 2.3.8.** *The determinant* $\det Q$ *and therefore also,* $\det Q''$ *is a symmetric polynomial of degree* $n$ *in the variables* $a_1, \ldots, a_n$.

*Proof.* Consider a transposition of the variables $a_i$ and $a_j$, $1 \leq i, j \leq n$ in the matrix $Q$. Call the new matrix $Q\{i,j\}$. Swapping rows $i$ and $j$, and columns $i$ and $j$ in $Q\{i,j\}$, gives the matrix $Q$. Since each column or row swap inverts the sign of the determinant, we have

$$\det Q = (-1)^2 \det(Q\{i,j\}) = \det(Q\{i,j\}).$$

Since $\det Q = (n-2)\det Q''$, both determinants are symmetric polynomials.

Each product in the determinant of $Q$ has $n$ factors, each of degree 1. Therefore, each product has degree $n$, and $\det Q$ has degree $n$. $\square$

To show that $\det Q''$ is formally positive, by Lemma 2.3.8, it suffices to show that $\det Q''$ is formally positive (mod $a_n$) and that the coefficient on $a_1 \cdots a_n$ is positive. By symmetry, formal positivity (mod $a_n$) shows formal positivity (mod $a_i$) for each $1 \leq i \leq n$, so the coefficient on every term not divisible by $a_1 \cdots a_n$ is positive. Then because the degree of $\det Q$ is $n$, the only term divisible by $a_1 \cdots a_n$ is $a_1 \cdots a_n$ itself.

We will show $\det Q''(\text{mod } a_n)$ is a formally positive polynomial by considering the cofactor expansion on row $n$.

For each $k = 1, \ldots, n-1$, let $R_k$ be the $(n-1) \times (n-1)$ matrix defined by

$$(R_k)_{ij} = \begin{cases} a_i, & i \neq j, \\ s - a_i, & i = j \neq k, \\ a_k, & i = j = k. \end{cases}$$

Then $\det R_k = (-1)^{n-1-k} \det Q''_{n,k}$, since $R_k$ is the cofactor $Q''_{n,k}$ with $n-1-k$ column transpositions. So we have

$$\begin{aligned} \det Q'' &= (s - a_n) \det Q''_{n,n} + \sum_{k=1}^{n-1} (-1)^k (s - a_{n-k}) \det Q''_{n,n-k} \\ &= (s - a_n) \det Q''_{n,n} - \sum_{k=1}^{n-1} (s - a_k) \det R_k. \end{aligned}$$

Consider the matrix $Q''_{n,n}$. We have

$$Q''_{n,n} = \begin{bmatrix} s - a_1 & a_1 & a_1 & \cdots & a_1 \\ a_2 & s - a_2 & a_2 & \cdots & a_2 \\ \vdots & & \ddots & & \vdots \\ a_{n-1} & a_{n-1} & a_{n-1} & \cdots & s - a_{n-1} \end{bmatrix}.$$

Let $\sigma \in S_{n-1}$ have fixed point set $X$. Then

$$\prod_{i=1}^{n-1} a_{i\sigma(i)} = \prod_{i \in X} (s - a_i) \prod_{j \in \{1,\ldots,n-1\} \setminus X} a_j.$$

For a given fixed point set $X$, the permutations which have fixed point set $X$ are the derangements of $\{1, \ldots, n-1\} \setminus X$, and the signature is the signature of the derangement. We use the following Lemma 2.3.9.

**Lemma 2.3.9.** *Let $f(k)$ be the difference of the number of even derangements of $k$ and the number of odd derangements of $k$. Then $f(k) = (-1)^{k-1}(k-1)$.*

*Proof.* In fact, we have $f(k) = \det(J - I)$. Subtracting row 1 from each of the other rows, and then adding each of the other rows to row 1, we have

$$f(k) = \det(J - I) = \det \begin{bmatrix} (k-1) & 0 & 0 & \cdots & 0 \\ 1 & -1 & 0 & \cdots & 0 \\ 1 & 0 & -1 & \cdots & 0 \\ \vdots & & & \ddots & \vdots \\ 1 & 0 & 0 & \cdots & -1 \end{bmatrix} = (k-1)(-1)^{k-1}.$$

□

By Lemma 2.3.9, we have

$$\det Q''_{n,n} = \sum_{X \subseteq \{1,\ldots,n-1\}} (-1)^{|X|-1}(|X|-1) \prod_{i \in X} a_i \prod_{j \in \{1,\ldots,n-1\} \setminus X} (s - a_j).$$

Let $t = a_1 + \cdots + a_{n-1}$. Then the terms of $\det Q''_{n,n}$ which do not contain a factor of $a_n$ are obtained by replacing $s$ with $t$ in the above expression. The expression

$$\sum_{X \subseteq \{1,\ldots,n-1\}} (-1)^{|X|-1}(|X|-1) \prod_{i \in X} a_i \prod_{j \in \{1,\ldots,n-1\} \setminus X} (t - a_j)$$

is formally positive if

$$\prod_{i=1}^{n-1}(t-a_i) = \sum_{\emptyset \neq X \subseteq \{1,\ldots,n-1\}} (|X|-1) \prod_{i\in X} a_i \prod_{j\in\{1,\ldots,n-1\}\setminus X} (t-a_j).$$

Since

$$t^{n-1} = \prod_{i=1}^{n-1}((t-a_i)+a_i),$$

this is equivalent to the following identity, which we state as Lemma 2.3.10.

**Lemma 2.3.10.** *Let $t = a_1 + a_2 + \cdots + a_n$ and $N = \{1, 2, \ldots, n\}$. Then*

$$t^n = \sum_{X\subseteq N} |X| \prod_{i\in X} a_i \prod_{j\in N\setminus X} (t-a_j).$$

*Proof.* On the right hand side above, consider $t$ as a formal variable. Since $t^n$ occurs only when $X = \emptyset$, in which case $|X| = 0$, the highest degree term of $t$ is at most degree $n-1$. A term with factor $t^{n-1}$ occurs only for $|X| = 1$. In the case $X = \{i\}$, the product is

$$a_i \prod_{j\in N\setminus\{i\}} (t-a_j),$$

so the coefficient on $t^{n-1}$ is $a_1 + a_2 + \cdots + a_n$.

We claim that the coefficient on $t^k$ for each $k = 0, \ldots, n-2$ is 0. In fact, a term divisible by $t^k$ occurs in the product for $X$ only when $|N \setminus X| \geq k$. Suppose $|N \setminus X| = k + \ell$ for some $\ell \geq 0$. Then the coefficient on $t$ in the product for the set $X$ is

$$(-1)^\ell \prod_{i\in X} a_i \sum_{Y\subset N\setminus X, |Y|=\ell} \prod_{j\in Y} a_j.$$

In particular, each coefficient on $t^k$ is a squarefree homogeneous polynomial of degree $n-k$. Fix a set $Z \subseteq N$ with $|Z| = n-k$ for some $k \geq 2$. Then the coefficient on $t^k \prod_{i\in Z} a_i$ is

$$\sum_{X\subseteq Z} (-1)^{|Z|-|X|} = \sum_{i=0}^{n-k} \binom{n-k}{i} (-1)^{n-k+i} = (1-1)^{n-k} = 0.$$

So the identity reduces to $t^n = (a_1 + \cdots + a_n)t^{n-1}$, which is true. □

Therefore the minor determinant $\det Q''_{n,n}$ is formally positive (mod $a_n$). We give the exact expression as Lemma 2.3.11.

**Lemma 2.3.11.** *Let $M = \{1, \ldots, n-1\}$. Then*

$$\det Q''_{n,n} = 2s \sum_{\substack{\emptyset \neq X \subseteq M \\ |X| \text{ odd}}} (|X| - 1) \prod_{i \in X} a_i \prod_{j \in M \setminus X} (s - a_j) \pmod{a_n},$$

*and $Q''_{n,n}$ is formally positive* (mod $a_n$).

*Proof.* This follows immediately by canceling the negative terms in the above expression, and using the identity of Lemma 2.3.10. □

Now consider the matrix

$$R_k = \begin{bmatrix} s - a_1 & a_1 & a_1 & \cdots & a_1 \\ a_2 & s - a_2 & a_2 & \cdots & a_2 \\ \vdots & & \ddots & & \vdots \\ a_k & a_k & \cdots & a_k & a_k \\ \vdots & & & \ddots & \vdots \\ a_{n-1} & a_{n-1} & a_{n-1} & \cdots & s - a_{n-1} \end{bmatrix}.$$

Let $\sigma \in S_{n-1}$. Then

$$\prod_{i=1}^{n-1} (R_k)_{i\sigma(i)} = a_k \prod_{i \in X \setminus \{k\}} (s - a_i) \prod_{j \in \{1, \ldots, n-1\} \setminus (X \cup \{k\})} a_j.$$

Letting $M_k = \{1, \ldots, n-1\} \setminus \{k\}$, where $M$ is as above, we have

$$\begin{aligned}
\det R_k &= \sum_{\substack{\sigma \in S_{n-1} \\ \sigma(k)=k}} \prod_{i=1}^{n-1} (R_k)_{i\sigma(i)} + \sum_{\substack{\sigma \in S_{n-1} \\ \sigma(k)\neq k}} \prod_{i=1}^{n-1} (R_k)_{i\sigma(i)} \\
&= a_k \sum_{X \subseteq M_k} (|X|-1)(-1)^{|X|-1} \prod_{i \in X} a_i \prod_{j \in M_k \setminus X} (s - a_j) \\
&\quad + a_k \sum_{X \subseteq M_k} |X|(-1)^{|X|} \prod_{i \in X} a_i \prod_{j \in M_k \setminus X} (s - a_j) \\
&= a_k \sum_{X \subseteq M_k} (-1)^{|X|} (|X| - (|X|-1)) \prod_{i \in X} a_i \prod_{j \in M_k \setminus X} (s - a_j) \\
&= a_k \sum_{X \subseteq M_k} (-1)^{|X|} \prod_{i \in X} a_i \prod_{j \in M_k \setminus X} (s - a_j).
\end{aligned}$$

We now have an expression for $\det Q'' (\mathrm{mod}\ a_n)$ which we can easily reduce to a form where it can be seen to be formally positive. First we look at Lemma 2.3.12.

**Lemma 2.3.12.** *The determinant* $\det Q''$ *is formally positive* $(\mathrm{mod}\ a_n)$.

*Proof.* In this proof, everything is $(\mathrm{mod}\ a_n)$.

We have

$$\begin{aligned}
\det Q'' = 2s &\sum_{\substack{\emptyset \neq X \subseteq M \\ |X| \text{ odd}}} (|X|-1) \prod i \in X \prod_{j \in M \setminus X} (s - a_j) \\
&- \sum_{k=1}^{n-1} a_k (s - a_k) \sum_{X \subseteq M_k} (-1)^{|X|} \prod_{i \in X} a_i \prod_{j \in M_k \setminus X} (s - a_j).
\end{aligned}$$

Working with the second line, we have

$$\begin{aligned}
&-\sum_{k=1}^{n-1} a_k(s-a_k)\sum_{X\subseteq M_k}(-1)^{|X|}\prod_{i\in X}a_i\prod_{j\in M_k\setminus X}(s-a_j)\\
&=-\sum_{k=1}^{n-1} a_k\sum_{X\subseteq M_k}(-1)^{|X|}\prod_{i\in X}a_i\prod_{j\in M\setminus X}(s-a_j)\\
&=-\sum_{k=1}^{n-1} a_k\sum_{\substack{X\subseteq M_k\\ |X| \text{ even}}}\prod_{i\in X}a_i\prod_{j\in M\setminus X}(s-a_j)\\
&\quad+\sum_{k=1}^{n-1} a_k\sum_{\substack{X\subseteq M_k\\ |X| \text{ odd}}}\prod_{i\in X}a_i\prod_{j\in M\setminus X}(s-a_j)\\
&=-\sum_{\substack{X\subseteq M\\ |X| \text{ odd}}}\sum_{k\in M\setminus X} a_k\prod_{i\in X}a_i\prod_{j\in M\setminus X}(s-a_j)\\
&\quad+\sum_{k=1}^{n-1} a_k\sum_{\substack{X\subseteq M_k\\ |X| \text{ odd}}}\prod_{i\in X}a_i\prod_{j\in M\setminus X}(s-a_j)\\
&\quad-\sum_{k=1}^{n-1} a_k\prod_{j\in M}(s-a_j).
\end{aligned}$$

Then, combining the above two equations, we get

$$\begin{aligned}
\det Q'' = &\sum_{\substack{X\subseteq M\\ |X| \text{ odd}}}\left(2s(|X|-1)-\sum_{k\in M\setminus X}a_k\right)\prod_{i\in X}a_i\prod_{j\in M\setminus X}(s-a_j)\\
&+\sum_{k=1}^{n-1} a_k\sum_{\substack{X\subseteq M_k\\ |X| \text{ odd}}}\prod_{i\in X}a_i\prod_{j\in M\setminus X}(t-a_j)-\sum_{k=1}^{n-1} a_k\prod_{j\in M}(t-a_j),
\end{aligned}$$

where the first line is formally positive, and the second line can be seen to be formally positive by separating out the part where $|X|=1$ from the first summation. In fact, this part of the summation is

$$\sum_{k=1}^{n-1} a_k\sum_{i\in M_k}a_i\prod_{j\in M_i}(s-a_j),$$

and the second summation can be expanded as

$$\sum_{k=1}^{n-1} a_k \sum_{i \in M_k} a_i \prod_{j \in M_k} (s - a_j),$$

but these two expressions are equal by reversing the order of $i$ and $k$.

So we have

$$\det Q'' = \sum_{\substack{X \subseteq M \\ |X| \text{ odd}}} \left( 2s(|X| - 1) - \sum_{k \in M \setminus X} a_k \right) \prod_{i \in X} a_i \prod_{j \in M \setminus X} (s - a_j)$$
$$+ \sum_{k=1}^{n-1} a_k \sum_{\substack{X \subseteq M_k \\ |X| \geq 3 \text{ odd}}} \prod_{i \in X} a_i \prod_{j \in M \setminus X} (t - a_j),$$

which is clearly formally positive. □

Now we can give the proof of Theorem 2.3.3.

*Proof of* Theorem 2.3.3. By the remarks following Lemma 2.3.8 and by the statement of Lemma 2.3.12, it remains to show only that the coefficient on $a_1 \cdots a_n$ in $\det Q''$ is positive. So the Theorem follows from Proposition 2.3.7. □

# Chapter 3

# Weights of codewords in cyclic binary codes

## 3.1 Basic definitions

There are two equivalent definitions of cyclic binary codes, one from a vector space viewpoint and one from a ring theory viewpoint.

**Definition 3.1.1** (Vector space definition)**.** *A* cyclic code *of length $n$ is a vector subspace of $\mathbb{Z}_2^n$ which is closed under cyclic translations. Where $\{e_0, \ldots, e_{n-1}\}$ is the standard basis, a cyclic translation is a linear function $f : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ such that there exists some integer $j$ for which $f(e_i) = f(e_{i+j})$ for each $i = 1, \ldots, n$ (subscripts taken mod $n$).*

**Definition 3.1.2** (Ring theoretic definition)**.** *A* cyclic code *of* length *$n$, is an ideal in the principal ideal ring $\mathbb{Z}_2[x]/(x^n - 1)$.*

We identify the element

$$(a_0, \ldots, a_{n-1}) \in Z_2^n$$

with the element

$$a_0 + a_1 x + \ldots a_{n-1} x^{n-1} \in Z_2[x]/(x^n - 1).$$

Then cyclic shifts correspond to multiplication by powers of $x$, and the ideal condition corresponds to the subspace closed under cyclic shifts condition. Therefore these two definitions are equivalent.

In the ring theoretic viewpoint, the generating polynomial of a cyclic code $C$ is a polynomial $g(x)$ such that $C = (g(x))$, and $g(x)$ divides $x^n - 1$. In the vector space viewpoint, if $\deg g(x) = d$, then the dimension of $C$ is $n - d$.

For any two elements $\boldsymbol{v}, \boldsymbol{x}$ of a code $C$, the Hamming distance $d(v, x)$ is the number of coordinates in which they differ under the standard basis. The weight of an element $\boldsymbol{v} \in C$ is $w(\boldsymbol{v}) = d(\boldsymbol{v}, 0)$, and the minimum weight of $C$ is the minimum over all $\boldsymbol{v} \in C$ of $w(\boldsymbol{v})$.

Suppose the minimum weight $d$ of a code $C$ satisfies $d \geq 2e + 1$. In this case, let $\boldsymbol{v} \in C$ and let $\boldsymbol{e} \in Z_2^n$ be any vector such that $w(\boldsymbol{e}) \leq d$. Let $f(\boldsymbol{x}) = d(\boldsymbol{v} + \boldsymbol{e}, \boldsymbol{x})$. Then $\boldsymbol{v}$ is the unique element of $C$ that satisfies the inequality $f(\boldsymbol{v}) \leq d$. The code $C$ is said to be *e-error correcting*.

## 3.2 The Codes $C_r^t$ which are 2-error correcting

Let $\omega$ be a primitive $n$th root of unity over $GF(2)$. The minimal polynomial of $\omega^i$ over $GF(2)$ will be denoted as $m_i(x)$ for each integer $i$.

**Theorem 3.2.1** (BCH Bound)**.** *Let $f(x) \in GF(2)[x]$, and suppose for some $i$, each of*

$$\omega^i, \omega^{i+1}, \ldots, \omega^{i+t-1}$$

*are all roots of $f(x)$. Then the minimum weight of the code generated by $f(x)$ is $\geq t + 1$.*

The classic 2-error correcting BCH code is the code of length $n$ generated by $m_1(x)m_3(x)$. Considering the field automorphism of $GF(2^n)$ given by $x \mapsto x^2$, we have that in addition to $\omega$ and $\omega^3$, also $\omega^2$ and $(\omega^2)^2 = \omega^4$ are roots of $m_1(x)m_3(x)$. So the first 4 consecutive powers of $\omega$ are roots, and by the BCH bound this code has minimum distance $\geq 5$.

In general, the BCH code of designed minimum distance $d = 2s + 1$ is the code generated by $m_1(x)m_3(x) \cdots m_{2s-1}(x)$. Each consecutive even power of $\omega$ between $\omega^2$ and $\omega^{2s}$ is a root of this polynomial by applying the field automorphism $x \mapsto x^2$.

We now turn to a particular type of generalization of the 2-error correcting BCH code. Let $n = 2^r - 1$, and let $C_r^t$ be the cyclic code of length $n$ generated by $m_1(x)m_t(x)$. The codes $C_r^3$ are the 2-error correcting BCH codes.

Two families of $t$ values which give infinitely many 2-error correcting codes have been known since 1971. In 1968, Gold [7] showed that for $t = 2^s + 1$, the code $C_r^t$ is 2-error correcting if $(s, r) = 1$. The numbers $t = 2^s + 1$ are known as the *Gold numbers*. In 1971, Kasami [13] showed that for $t = 4^s - 2^s + 1$, the code $C_r^t$ is 2-error correcting if $(s, r) = 1$. The numbers $t = 4^s - 2^s + 1$ are known as the *Kasami-Welch numbers*. In this case, if $(s, r) > 1$ then the code has words of weight 3.

Recent results of Hernando and McGuire [8] state that the only values of $t$ for which the code $C_r^t$ is 2-error correcting for infinitely many values of $r$ are the Gold and Kasami-Welch numbers. That is, for any $t$ which is not of one of these two forms, there are only finitely many 2-error correcting codes $C_r^t$.

## 3.3 Codewords of weight 4 in $C_r^t$

We investigate the number of codewords of weight 4 in the codes $C_r^t$. In particular, we are interested in finding formulas for the number of codewords of weight 4 for families of these codes when $t$ is fixed and $r$ varies.

In some cases, the weights of all codewords for dual codes in some family are known. In these cases, the MacWilliams identity gives a relationship between the weights of codewords in a binary linear code $C$ and its dual code $C^\perp$.

**Theorem 3.3.1** (MacWilliams identity)**.** *If $C$ is a $k$-dimensional linear binary code of length $n$, and $A_i$ is the number of words of weight $i$ in $C$ and $A'_i$ is the number of words of weight $i$ in the dual $C^\perp$, then*

$$\sum_{k=0}^{n} A'_k x^{n-k} y^k = \frac{1}{|C|} \sum_{i=0}^{n} A_i (x+y)^{n-i} (x-y)^i.$$

The number of codewords for each different weight are known for the dual codes of $C_r^t$ for each of the Gold numbers. These are given in Tables 3.1 and 3.2. Applying

| $i$ | $A_i$ |
|---|---|
| $0$ | $1$ |
| $2^{m-1} - 2^{(m+s-2)/2}$ | $(2^m - 1)(2^{m-s-1} + 2^{(m-s-2)/2})$ |
| $2^{m-1}$ | $(2^m - 1)(2^m - 2^{m-s} + 1)$ |
| $2^{m-1} + 2^{(m+s-2)/2}$ | $(2^m - 1)(2^{m-s-1} - 2^{(m-s-2)/2})$ |

Table 3.1: Weight enumerator for the dual of $C_m^{2^j+1}$ with $m$ odd and $s = (j, m)$ (MacWilliams and Sloane).

| $i$ | $A_i$ |
|---|---|
| $0$ | $1$ |
| $2^{m-1}$ | $(2^m - 1)[(2^s - 1)2^{m-2s} + 1]$ |
| $2^{m-1} \pm 2^{(m+2s-2)/2}$ | $2^{(m-2s-2)/2}(2^m - 1)(2^{(m-2s)/2} \mp 1)/(2^s + 1)$ |
| $2^{m-1} \pm 2^{m/2-1}$ | $2^{(m+2s-2)/2}(2^m - 1)(2^{m/2} \mp 1)/(2^s + 1)$ |

Table 3.2: Weight enumerator for the dual of $C_m^{2^j+1}$, $1 < i < \frac{1}{2}m$, $(m, 2j) = 2(m, j) = 2s$ (MacWilliams and Sloane).

the MacWilliams identity, we can determine the number of codewords of weight 4 in these codes.

For other values of $t$ where explicit formulas for weights of the dual code are not as easily calculated, we use an approach from algebraic geometry to determine formulas for the number of words of weight 4.

Let

$$g_t(X, Y, Z) = \frac{X^t + Y^t + Z^t + (X + Y + Z)^t}{(X + Y)(X + Z)(Y + Z)}.$$

We establish a connection between certain zeroes of $g_t$ and words of weight 4 in the codes $C_r^t$.

Suppose a word of weight 4 in $C_r^t$ has 1's in positions $i, j, k, \ell$. Then $\omega^i + \omega^j + \omega^k + \omega^\ell = 0$ and $\omega^{it} + \omega^{jt} + \omega^{kt} + \omega^{\ell t} = 0$. Letting $X = \omega^i$, $Y = \omega^j$, $Z = \omega^k$, $W = \omega^\ell$ we have the system

$$\begin{aligned} X + Y + Z + W &= 0 \\ X^t + Y^t + Z^t + W^t &= 0. \end{aligned}$$

Since this is a system over a field of characteristic 2, we have $W = X + Y + Z$ and so

$$X^t + Y^t + Z^t + (X + Y + Z)^t = 0.$$

This is clearly divisible by $X + Y$, $X + Z$, and $Y + Z$.

We can also go in the other direction. If $(X, Y, Z)$ is a solution of $g_t(X, Y, Z) = 0$ where $X, Y, Z$ are distinct and nonzero, this gives a solution to the above system. Each solution of the above system has $4! = 24$ permutations corresponding to the same word of weight 4.

**Definition 3.3.2.** *Let $N_r$ be the number of projective points on a curve over $GF(q^r)$. Then the zeta function of the curve is*

$$\zeta(t) = \exp\left(\sum_{r=1}^{\infty} N_r \frac{t^r}{r}\right).$$

Hartshorne [9] gives the following formula for the zeta function, which is applicable to $g_t$.

If $X$ is a smooth variety of dimension $n$, then

$$\zeta(t) = \frac{P_1(t)P_3(t)\cdots P_{2n-1}(t)}{P_0(t)P_2(t)\cdots P_{2n}(t)},$$

where $P_0(t) = 1-t$, $P_{2n}(t) = 1-q^n t$, and for each $1 \leq i \leq 2n-1$, $P_i(t)$ is a polynomial with integer coefficients which can be written

$$P_i(t) = \prod(1 - \alpha_{ij}t),$$

where the $\alpha_{ij}$ are algebraic integers with $|\alpha_{ij}| = q^{i/2}$.

Further, in the case of $g_t$, the polynomial $P_1(t)$ has degree $2g$, where

$$g = (d-1)(d-2)/2,$$

and where $d$ is the degree of the polynomial $g_t$. This implies that the coefficients $a_i$

on $t^i$ satisfy

$$a_{2g-i} = q^{g-i} a_i.$$

For some values of $t$ where $g_t$ is absolutely irreducible, we can compute the zeta function of $g_t$.

### 3.3.1 The codes $C_s^7$ and $C_s^{11}$

For $t = 7$, Wilson and Janwa compute the zeta function of $g_t$. By computer or by hand, it is straightforward to find that $N_1 = 0$, $N_2 = 14$, and $N_3 = 24$, which is enough to determine the zeta function:

$$\begin{aligned}\zeta(x) &= \exp\left(\sum_{s=1}^{\infty} \frac{N_s}{s} x^s\right) \\ &= 1 + \left(\frac{14}{2}x^2 + \frac{24}{3}x^3 + \cdots\right) + \frac{1}{2}\left(\frac{14}{2}x^2 + \frac{24}{3}x^3 + \cdots\right)^2 \\ &= 1 + 0x + 7x^2 + 8x^3 + \cdots\end{aligned}$$

so we get

$$P_1(x) = (1-x)(1-2x)\zeta(x) = 1 - 3x + 9x^2 - 13x^3 + \cdots.$$

And this implies that

$$P_1(x) = 1 - 3x + 9x^2 - 13x^3 + 18x^4 - 12x^5 + 8x^6.$$

So we have

$$\zeta(x) = \exp\left(\sum_{s=1}^{\infty} \frac{N_s}{s} x^s\right) = \frac{P_1(x)}{(1-x)(1-2x)},$$

and we can recursively compute the coefficients $N_s$ using this formula.

In this case, when $s$ is even, we have exceptional solutions which do not correspond to codewords of weight 4 in $C_s^7$. These are solutions where two of $X, Y, Z$ are equal or one of $X$,$Y$,$Z$, or $X + Y + Z$ is zero. In fact for each even $s$, there are always 14

exceptional solutions. So we have the following formula for the number of words of weight 4:

$$w_4(C_s^7) = \begin{cases} nN_s/24 & if\ s\ is\ odd, \\ n(N_s - 14)/24 & if\ s\ is\ even. \end{cases}$$

Now we consider the case $t = 11$. The genus $g = 21$, so to compute the zeta function of $g_{11}$ using Hartshorne's formula, we must know the number of projective solutions of $g_{11}$ over $GF(2^s)$ for each $s = 1, \ldots, 21$.

Using a computer, we directly compute the number of projective solutions of $g_{11}$ over $GF(2^s)$ in these cases. The computations are listed in Figure 3.1. Here $N_s$ is the number of projective solutions of

$$g_{11}(X, Y, Z) = \frac{X^{11} + Y^{11} + Z^{11} + (X + Y + Z)^{11}}{(X + Y)(X + Z)(Y + Z)}$$

and $E_s$ is the number of exceptional solutions (note that the number of exceptional solutions is periodic in $s$ with period 12).

In general, we have

$$w_4(C_s^{(11)}) = (2^s - 1)(N_s - E_s)/24.$$

The zeta function is

$$\zeta(x) = \exp\left(\sum_{s=1}^{\infty} \frac{N_s}{s} x^s\right) = \frac{p(x)}{(1 - x)(1 - 2x)},$$

| $s$ | $N_s$ | $E_s$ | $w_4(C_s^{11})$ |
|---|---|---|---|
| 1 | 0 | 0 | 0 |
| 2 | 8 | 8 | 0 |
| 3 | 48 | 24 | 7 |
| 4 | 20 | 20 | 0 |
| 5 | 0 | 0 | 0 |
| 6 | 128 | 32 | 252 |
| 7 | 0 | 0 | 0 |
| 8 | 500 | 20 | 5100 |
| 9 | 480 | 24 | 9709 |
| 10 | 1568 | 8 | 66495 |
| 11 | 2112 | 0 | 180136 |
| 12 | 3956 | 44 | 667485 |
| 13 | 8736 | 0 | 2981524 |
| 14 | 15968 | 8 | 10894695 |
| 15 | 33408 | 24 | 45578897 |
| 16 | 58868 | 20 | 160691820 |
| 17 | 132192 | 0 | 721939068 |
| 18 | 261920 | 32 | 2860504416 |
| 19 | 521664 | 0 | 11395902232 |
| 20 | 1035380 | 20 | 45235525500 |
| 21 | 2089632 | 24 | 182592646117 |

Figure 3.1: Computations for the number of codewords of weight 4 in $C_s^{11}$ for small values of $s$.

where

$$\begin{aligned} p(x) &= 1 - 3x + 6x^2 + 4x^3 - 27x^4 + 57x^5 + 14x^6 - 204x^7 + 459x^8 - 185x^9 \\ &\quad - 798x^{10} + 2268x^{11} - 1545x^{12} - 2445x^{13} + 9594x^{14} - 10020x^{15} \\ &\quad - 1128x^{16} + 27504x^{17} - 39408x^{18} + 17616x^{19} + 64320x^{20} \\ &\quad - 133984x^{21} + 128640x^{22} + 70464x^{23} - 315264x^{24} + 440064x^{25} \\ &\quad - 36096x^{26} - 641280x^{27} + 1228032x^{28} - 625920x^{29} - 791040x^{30} \\ &\quad + 2322432x^{31} - 1634304x^{32} - 757760x^{33} + 3760128x^{34} \\ &\quad - 3342336x^{35} + 458752x^{36} + 3735552x^{37} - 3538944x^{38} \\ &\quad + 1048576x^{39} + 3145728x^{40} - 3145728x^{41} + 2097152x^{42}. \end{aligned}$$

This $\zeta$ function can be used to compute a recurrence relation to determine the number of codewords of weight 4 in $C_s^{11}$ for any value of $s$.

# Chapter 4

# Elliptic Semiplanes

## 4.1 Preliminaries

We begin by defining terms from design theory, as we will use them here. As defined in [24], an *incidence structure* is a triple $\mathbf{S} = (\mathcal{P}, \mathcal{B}, \mathbf{I})$, such that:

(1) $\mathcal{P}$ is a set, the elements of which are called *points*;

(2) $\mathcal{B}$ is a set, the elements of which are called *blocks*;

(3) $\mathbf{S}$ is an incidence relation between $\mathcal{P}$ and $\mathcal{B}$ (i.e., $\mathbf{I} \subseteq \mathcal{P} \times \mathcal{B}$). The elements of $\mathbf{I}$ are called *flags*.

The *incidence matrix* for an incidence structure is a 0-1 matrix with $|\mathcal{P}|$ columns corresponding to the elements of $\mathcal{P}$, $|\mathcal{B}|$ rows corresponding to the elements of $\mathcal{B}$, such that the entry in row $B \in \mathcal{B}$, column $p \in \mathcal{P}$ is a 1 if and only if $(p, B) \in \mathbf{I}$.

The blocks of an incidence structure are also often called *lines* in some contexts. We will use the terms interchangeably.

Given integers $v, k, t, \lambda$ with $v \geq k \geq t \geq 0$ and $\lambda \geq 1$, a $t$-$(v, k, \lambda)$ design is an incidence structure such that:

(i) $|\mathcal{P}| = v$,

(ii) $|B| = k$ for each $B \in \mathcal{B}$,

(iii) for any set $T$ of $t$ points, there are exactly $\lambda$ blocks incident with all points in $T$.

A *symmetric design* is a $t$-$(v, k, \lambda)$ design such that the number of points is equal to the number of blocks. More generally, an incidence structure is called *square* if the number of points is equal to the number of blocks.

For our purposes, we are interested only in the case where $t = 2$. For $\lambda \geq 1$ we will call an incidence structure a $\lambda$-design if it is a 2-$(v, k, \lambda)$ design for some integers $v, k$.

For any set $S$ of nonnegative integers, we will call an incidence structure a regular $S$-design if it satisfies conditions (i) and (ii) of the definition of a 2-$(v, k, \lambda)$ design, and also the modified condition (iii′):

(iii′) any two distinct points are incident in a number of blocks which is in the set $S$.

Let $p, q$ be two points in a $\{0, 1\}$-design. We call the points *parallel* if $p = q$ or if $p$ and $q$ are not incident with any common block. Similarly, let $B, C$ be two blocks in a $\{0, 1\}$-design. We call the blocks *parallel* if $B = C$ or if $B$ and $C$ are not incident with any common point. Clearly the relations of parallelism are symmetric and reflexive for both points and lines.

We are interested in a certain type of $\{0, 1\}$-design, where parallelism is transitive and therefore an equivalence relation. More specifically, we are interested in those designs where the quotient under the equivalence relation also is a design.

**Definition 4.1.1.** *An* elliptic semiplane *is a $\lambda$-fold cover of a symmetric $\lambda$-design. That is:*

1. *it is a square regular $\{0, 1\}$-design, with $n$ points, $n$ lines, $k + 1$ points per line, and $k + 1$ lines per point;*

2. *no two lines share two points;*

3. *parallelism is a transitive relation for lines and also for points;*

4. *the quotient under the equivalence relation of parallelism is a symmetric $\lambda$-design.*

Baker [1] gives an example of an elliptic semiplane with 45 points, 45 lines, and 7 points per line. We show directly that an elliptic semiplane with these parameters is unique up to isomorphism.

First we establish a way in which the incidence matrix for a $\lambda$-design can be made into an incidence matrix for an elliptic semiplane.

**Proposition 4.1.2.** *Let $A$ be the incidence matrix of a $\lambda$-cover of a symmetric design. Let $m_0, \ldots, m_{\lambda-1}$ be formal symbols such that $m_i \times m_j = m_k$ where $[k] = [i-j]$, where $[n]$ represents congruence class modulo $\lambda$. A $\lambda$-cover of $A$ exists if there is a way to replace each nonzero entry of $A$ with some $m_i$ in such a way that the resulting matrix $B$ satisfies*

$$BB^T = (m_0 + m_1 + \cdots + m_{\lambda-1})(J - I) + (k+1)I.$$

*Proof.* Let $A$ be the incidence matrix of a symmetric $\lambda$-design with $n$ points, $n$ lines, and block size $k+1$. Suppose there exists a matrix $B$ such that $B$ is $A$ with each 1 replaced by some $m_i$ in such a way that the condition on $BB^T$ is satisfied. Now let $M$ be the $\lambda \times \lambda$ permutation matrix of the cycle $(1, 2, \ldots, \lambda)$, and let $M_i = M^i$ for each $i = 0, \ldots, \lambda - 1$, and let $C$ be the $(\lambda n) \times (\lambda n)$ matrix formed by replacing $m_i$ by $M_i$ for each $i = 0, \ldots, \lambda - 1$ and 0 by the $\lambda \times \lambda$ zero matrix. We claim that $C$ is an incidence matrix for an elliptic semiplane.

Each of the matrices $M_i$ contains exactly one 1 in each row and column ($i = 1 \ldots, \lambda - 1$), and each row and column of $B$ contains $k+1$ nonzero entries, each of which is some $m_i$. Therefore each row and column of $C$, each of which contains $k+1$ rows or columns of matrices $M_i$, respectively, contains exactly $k+1$ 1s. The matrix $C$ is also square and $\lambda n \times \lambda n$, so has $\lambda n$ points and lines. This shows condition 1 of Definition 4.1.1.

Consider two distinct rows of $C$ which cover the same row of $B$. Since each of the matrices $M_i$ has only one 1 in each column, for each column at most one of these two rows has a 1. Therefore, the lines do not share any points in common; they are parallel.

Now consider two distinct rows of $C$ which cover distinct rows of $B$. More specif-

ically, consider the rows $\lambda(c_1 - 1) + d_1$ and $\lambda(c_2 - 1) + d_2$ where $1 \leq d_i \leq \lambda$ for $(i = 1, 2)$ and $c_1 \neq c_2$, $1 \leq c_i \leq n$ for $(i = 1, 2)$. Consider row $d$ of the matrix $M_j$ for $j = 0, \ldots, \lambda - 1$. Since $M_j = M^j$ and $M$ is a permutation sending $d$ to $d + 1$ (modulo $n$), the matrix $M^j$ has a 1 in position $(d, d + j)$ (modulo $lambda$). So row $d_1$ of matrix $M_{j_1}$ has a 1 in the same column as row $d_2$ of matrix $M_{j_2}$ if and only if $d_1 + j_1 = d_2 + j_2 (\text{mod } \lambda)$. That is, if and only if $d_2 - d_1 = j_1 - j_2 (\text{mod } \lambda)$. Since the standard coordinate wise product of rows $c_1 - 1$ and $c_2 - 1$ of $B$ is $m_0 + m_1 + \cdots m_{\lambda-1}$, and the value of the product $m_{j_1} m_{j_2}$ is $m_k$ such that $[k] = [j_1 - j_2]$, there is exactly one column of $B$ such that the product of the entry in row $c_1 - 1$ and the entry in row $c_2 - 1$ is $m_k$ with $[k] = [d_2 - d_1]$. Therefore two rows of $C$ which cover distinct rows of $B$ have intersection size 1.

Combining these results, we see that two rows of $C$ are parallel if and only if they cover the same row of $B$, and two intersecting rows intersect in a set of size 1. Therefore conditions 2 and 3 hold. Modulo the equivalence relation of parallelism, the incidence matrix $C$ becomes the incidence matrix $A$ of a symmetric $\lambda$-design, so condition 4 also holds. □

**Corollary 4.1.3.** *Let $\lambda$ be a prime number. A $\lambda$-cover of a symmetric design with block size $k + 1$ exists if there is a way to take the incidence matrix $A$ of the design and replace each 1 of the matrix with a $\lambda$ root of unity in such a way that the resulting matrix $B$ satisfies $BB^* = (k + 1)I$.*

*Proof.* Let $A$ be an incidence matrix of a symmetric $\lambda$-design for some prime $\lambda$. Let $\omega$ be a primitive $\lambda$ root of unity, and suppose it is possible to replace each 1 in $A$ with a power of $\omega$ such that the resulting matrix $B$ satisfies $BB^* = (k + 1)I$.

Any two distinct rows of $A$ intersect in exactly $\lambda$ columns. So the $(i, j)$ entry of $BB^*$ for $i \neq j$ is a sum of $\lambda$ powers of $\omega$. That is, it is a polynomial in $\omega$ with nonnegative integer coefficients which sum to $\lambda$. But since $\lambda$ is a prime, the minimal polynomial of $\omega$ is $1 + x + x^2 + \cdots + x^{\lambda-1}$, and any nonnegative linear combination of powers of $\omega$ which is zero must be a multiple of this polynomial.

Therefore, for any two distinct rows $i_1$ and $i_2$ of $B$ and for each $\ell = 0, \ldots, \lambda - 1$

there is exactly one column $j$ such that $B_{i_1,j}\overline{B_{i_2,j}} = \omega^\ell$. That is, letting $m_\ell = \omega^\ell$ for each $\ell = 0, \ldots, \lambda - 1$, we have the condition in Proposition 4.1.2. □

We will be concerned primarily with $\lambda$-covers of symmetric designs with $\lambda = 2, 3$. We show that these covers can be built from incidence matrices of the base design in a certain way, and that all covers can be realized this way, by proving the converse of Corollary 4.1.3 in these cases.

**Proposition 4.1.4.** *A 2-cover of a symmetric design with block size $k+1$ and $\lambda = 2$ is equivalent to taking the incidence matrix $A$ of the design and replacing each 1 of the matrix with a $+1$ or $-1$ in such a way that the resulting matrix has $BB^T = (k+1)I$.*

*Proof.* Let $C$ be the $2n \times 2n$ incidence matrix of a 2-cover of a 2-design with block size $k + 1$, and the rows and columns ordered so that for any $m = 1, \ldots, n$, rows $2m - 1$ and $2m$ are parallel and columns $2m - 1$ and $2m$ are parallel. Let $A$ be the incidence matrix of the 2-design which is the quotient of $C$ by parallelism, and let $B$ be the matrix $A$ with 1 replaced by $+1$ if the corresponding $2 \times 2$ submatrix of $C$ is the identity, and $-1$ if the corresponding submatrix of $C$ is not the identity. That is, if it is the permutation matrix of the cycle $(1, 2)$, call it $I'$.

Consider a pair of distinct rows $i_1$ and $i_2$ in $A$. We say that rows $i_1$ and $i_2$ have intersection of type $M$ in column $j$ if $M$ is a $2\times2$ 0-1 matrix such that the $(x, y)$ entry of $M$ is 1 if and only if the $x$th row corresponding to row $i_1$ in $C$ (row $2(i_1 - 1) + x$ in $C$) and the $y$th row corresponding to row $i_2$ in $C$ (row $2(i_2 - 1) + y$ in $C$) intersect within the columns of $C$ corresponding to column $j$ of $A$. Let $M(i_1, i_2; j)$ be the intersection type of rows $i_1$ and $i_2$ in column $j$. For any distinct rows $i_1$ and $i_2$, we define

$$N(i_1, i_2) = \sum_{j=1}^{n} M(i_1, i_2; j) = J,$$

because none of the lines corresponding to $i_1$ are parallel to lines corresponding to $i_2$, and each pair of lines intersects in, at most, one point.

Now for each $i, j \in \{1, 2, \ldots, n\}$, let $C_{ij}$ be the $2\times2$ submatrix of $C$ corresponding

to position $(i, j)$ of $A$. Then

$$M(i_1, i_2; j) = C_{i_1,j}(C_{i_2,j})^T = C_{i_1,j}C_{i_2,j}^{-1},$$

since the matrices $C_{ij}$ are orthonormal. Now $N(i_1, i_2)$ is the sum of exactly two nonzero orthonormal 0-1 matrices, so it must be the sum of $I$ and $I'$. So any two distinct rows of $B$ intersect in two columns, one of which has the same entry in the two rows, and one of which has the opposite entry in the two rows. So the for $i_1$ and $i_2$ distinct, we have $(BB^T)_{i_1,i_2} = 1 + (-1) = 0$.

Clearly since $A$ is a design with block size $k+1$, we have $(BB^T)_{ii} = k+1$ for any $i$. Therefore we have $BB^T = (k+1)I$. □

In what follows we will let $\omega$ be a primitive cube root of unity. There are 6 different $3 \times 3$ permutation matrices, which we will denote as

$$1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \omega = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \omega^2 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

$$\alpha = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \beta = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \gamma = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}.$$

As permutations these are

$$I = e, \omega = (1,2,3), \omega^2 = (1,3,2), \alpha = (1,2), \beta = (2,3), \gamma = (1,3).$$

So in particular, $\omega^{-1} = \omega^2$ and the other four matrices are self-inverse.

When considering 3-covers of symmetric designs, we will be most interested in covers of $(15, 7, 3)$ designs, because these are the only ones known to exist. We prove the following Lemma, which applies to this case, but the conclusions of which may not apply to 3-designs on a larger number of points.

**Lemma 4.1.5.** *Suppose $M$ is a $4 \times n$ 0-1 matrix such that*

(1) *the $4 \times 4$ left submatrix of $M$ is*

$$\begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix},$$

(2) *all rows of $M$ have exactly 7 ones, and*

(3) *any two rows of $M$ have common ones in exactly 3 columns.*

*Then $n \geq 17$.*

*Proof.* Let $N$ be the right $4 \times (n-4)$ submatrix of $M$, and for each $i = 1, 2, 3, 4$, let $A_i$ be the set of column numbers of $N$ such that row $i$ of $N$ has a 1. Without loss of generality, assume that $A_1 = \{1, 2, 3, 4\}$ by (1) and (2). We also have $|A_2| = |A_3| = |A_4| = 6$ by (1) and (2). For each $i = 2, 3, 4$, let $A_i' = A_1 \cap A_i$. Then we have $|A_i'| = 3$ for $i = 2, 3, 4$ and for $i, j \in \{2, 3, 4\}$ with $i \neq j$, we have $|A_i' \cap A_j'| \leq 2$ by (1) and (3). But any distinct 3 element subsets of a set of size 4 intersect in 2 points, so we have equality.

Let $A_i'' = A_i \cap \{5, 6, 7, \ldots, n-4\}$ for each $i = 1, 2, 3, 4$. Then $|A_1''| = 0$, and $|A_i''| = 3$ for each $i = 2, 3, 4$. Also for any distinct $i, j \in \{1, 2, 3, 4\}$, rows $i$ and $j$ of $M$ have common ones in 3 of the leftmost 8 columns, so $|A_i'' \cap A_j''| = 0$. So we have $|A_2'' \cup A_3'' \cup A_4''| = 9$, and therefore $N$ has at least $4 + 9 = 13$ columns, so $n - 4 \geq 13$ and $n \geq 17$. □

We use this to prove Proposition 4.1.6, which will enable us to enumerate the 3-covers of $(15, 7, 3)$ designs, ultimately showing that such a cover is unique.

**Proposition 4.1.6.** *A 3-cover of a symmetric design with $n$ points, $n$ lines, block size $k+1$, and $\lambda = 3$, with $n < 17$ is equivalent to taking the incidence matrix $A$ of the design and replacing each 1 of the matrix with a 1 or $\omega$ or $\omega^2$ in such a way that the resulting matrix has $BB^* = (k+1)I$.*

*Proof.* Let $C$ be the $3n \times 3n$ incidence matrix of a 3-cover of a 3-design with block size $k+1$, and the rows and columns ordered so that for any $m = 1, \ldots, n$, rows $2m-2$,$2m-1$,$2m$ form a parallel class, and columns $2m-2$,$2m-1$,$2m$ form a parallel class. Let $A$ be the incidence matrix of the 3-design which is the quotient of $C$ by parallelism, and let $B$ be the $n \times n$ matrix $A$ with each 1 replaced by the symbol of the corresponding $3 \times 3$ submatrix of $C$, that is, by one of the six symbols $1, \omega, \omega^2, \alpha, \beta, \gamma$.

Analogous with the proof of Proposition 4.1.4, for any two distinct rows $i_1$ and $i_2$ of $A$, and a column $j$ of $A$, we let $M(i_1, i_2; j)$ be the $3 \times 3$ matrix with a 1 in position $(x, y)$ if the $x$th row of $C$ corresponding with row $i_1$ and the $y$th row of $C$ corresponding with row $i_2$ intersect in a column corresponding to column $j$. We again define

$$N(i_1, i_2) = \sum_{j=1}^{n} M(i_1, i_2),$$

and note that for any distinct $i_1$ and $i_2$ we always have $N(i_1, i_2) = J$, since none of the lines of $C$ corresponding to $i_1$ are parallel to any of the lines corresponding to $i_2$, and each pair of distinct lines intersects in, at most, one point.

For each $i, j \in \{1, 2, \ldots, n\}$, let $C_{ij}$ be the $3 \times 3$ submatrix of $C$ corresponding to position $(i, j)$ of $A$. We again have

$$M(i_1, i_2; j) = C_{i_1,j} C_{i_2,j}^T.$$

Also $N(i_1, i_2) = J$ is a sum of 3 of the six matrices $I, \omega, \omega^2, A, B, C$. The matrices $I, \omega, \omega^2$ are pairwise orthogonal, as are $\alpha, \beta, \gamma$, and of any two matrices, one from each of the two groupings, none are orthogonal. So the only sums of three nonzero permutation matrices which sum to $J$ are $I + \omega + \omega^2$ and $\alpha + \beta + \gamma$.

We will show that by reordering the rows and columns of $C$, and still preserving the condition that parallel classes of rows and columns are adjacent, we can ensure that $B$ contains only the symbols 0, 1, $\omega$, $\omega^2$. First we choose a row $i_0$ and a column $j_0$ of $A$ such that $A_{ij} = 0$, and perform row permutations and column permutations

on $A$ so that row $i_0$ is moved to row 1 and column $j_0$ is moved to column 1. Then we perform column permutations on $A$ so that the 1s in row 1 are in positions 2 through $k+2$ and row permutations on $A$ so that the 1s in column 1 are in positions 2 through $k+2$.

By performing row permutations on a $3\times 3$ permutation matrix, we can transform any matrix into 1 (or any other permutation matrix). The same is true for column operations. So considering each of the nonzero entries in the first row of $B$, we perform column permutations in the 3 corresponding columns of $C$ to make the entry 1. And we perform row permutations within each set of 3 rows of $C$ corresponding to nonzero entries of the first column of $B$ to make all of these entries also 1. Now the upper left $(k+2)\times(k+2)$ submatrix of $B$ looks like

$$\left[\begin{array}{c|ccc} 0 & 1 & \cdots & 1 \\ \hline 1 & & & \\ \vdots & & D & \\ 1 & & & \end{array}\right],$$

where each row and column of $D$ contains 3 nonzero entries. Consider the first row of $D$. Since $N(1,2)=J$, and all the first row entries are 1, we must have the nonzero entries of the first row of $D$ be either $1,\omega,\omega^2$ or $\alpha,\beta,\gamma$. Suppose they are $\alpha,\beta,\gamma$. Within each set of 3 columns of $C$ corresponding to a column of $B$ numbered from 2 through $k+2$, swap the first and second columns. This transformation exchanges

$$1\leftrightarrow\alpha,\omega\leftrightarrow\beta,\omega^2\leftrightarrow\gamma.$$

Then in the rows of $C$ corresponding to the first row of $B$, swap the first and second rows. This transformation exchanges

$$1\leftrightarrow\alpha,\omega\leftrightarrow\gamma,\omega^2\leftrightarrow\beta.$$

After these two transformations, the first row of $D$ contains nonzero entries 1, $\omega$, $\omega^2$

and row 1 of $B$ still contains 1s in positions 2 through $k+2$.

Consider the column variant of the function $M$, which given two distinct columns $j_1$ and $j_2$ and a row $i$ gives a matrix showing the positions where corresponding columns of $C$ intersect, just as $M$ does for rows. Then call this function $M'(i; j_1, j_2)$, and let

$$N'(j_1, j_2) = \sum_{i=1}^{n} M'(i; j_1, j_2).$$

By duality we have $N'(j_1, j_2) = J$, so the sum must be of $1, \omega, \omega^2$ or $\alpha, \beta, \gamma$.

Therefore, if $B_{ij} \in \{1, \omega, \omega^2\}$ for some $i, j \in \{2, 3, \ldots, k+2\}$, it follows that $B_{ij} \in \{0, 1, \omega, \omega^2\}$ for each entry in the same row or column in that submatrix. Suppose there are proper nonempty subsets $X, Y \subset \{2, 3, \ldots, k+2\}$ such that for each $x \in X$, row $x$ of $A$ contains 3 nonzero entries in columns from $Y$, and for each $y \in Y$, row $y$ of $A$ contains 3 nonzero entries in columns from $X$. Clearly we must have $|X| = |Y|$, and $|X| \geq 3$. Also, letting

$$X' = \{2, 3, \ldots, k+2\} \setminus X,$$

$$Y' = \{2, 3, \ldots, k+2\} \setminus Y,$$

we see that $X'$ and $Y'$ must satisfy the same conditions as $X$ and $Y$. We claim that $|X| > 3$. In fact, if $|X| = 3$, then the submatrix with rows $X$ and columns $Y'$ is a $3 \times 4$ zero matrix, and the matrix with rows $1 \cup X$ and columns $1 \cup Y'$ gives a contradiction to Lemma 4.1.5. Therefore $|X| > 3$, and since $X'$ satisfies the same conditions, $|X'| > 3$. But $X$ and $X'$ are disjoint subsets of a set of size at most 7, since $n < 17$ implies $k \leq 7$. This is a contradiction, so $X$ and $Y$ do not exist. So the nonzero entries in the matrix $D$ are all $1, \omega, \omega^2$.

Consider now the upper right $(k+2) \times (n-k-2)$ submatrix. Each column has three nonzero entries, which are either $1, \omega$, and $\omega^2$ or $\alpha, \beta$, and $\gamma$. If a column has entries $\alpha, \beta$, and $\gamma$, then a swap of the first and second corresponding column of $C$ makes these $1, \omega$, and $\omega^2$, without altering the upper left submatrix of $B$. Similarly the lower left $(n-k-2) \times (k+2)$ submatrix of $B$ can be changed by row operations

to contain only entries from $1, \omega$, and $\omega^2$ without altering the first $k+2$ rows of $B$.

It remains to show that the lower right $(n-k-2) \times (n-k-2)$ submatrix of $B$ contains only entries from $0, 1, \omega$, and $\omega^2$. Consider a nonzero entry in the lower right submatrix of $B$, with coordinates $(x, y)$ in $B$. Since every line of $A$ intersects every other line of $A$ in 3 points, there are 3 columns among 2 through $k+2$ which contain a nonzero entry in row $x$ by considering the intersection of column $y$ with column 1. Call these columns $y_1, y_2$, and $y_3$. Also since every pair of distinct points of $A$ have 3 lines in common, there are 3 rows among 2 through $k+2$ which contain a nonzero entry in column $y$ by considering the intersection of row $x$ with row 1. Call these rows $x_1, x_2$, and $x_3$. Now consider the $4 \times 4$ matrix formed by rows 1, $x_1$, $x_2$, and $x_3$, and columns 1, $y_1$, $y_2$, and $y_3$, of matrix $A$. Suppose the entry in position $(x_i, y_j)$ is zero for each $i, j \in \{1, 2, 3\}$. Then the $4 \times n$ matrix formed from rows 1, $x_1$, $x_2$, and $x_3$, contradicts Lemma 4.1.5. Therefore there must be some $i, j$ such that $A_{x_i, y_j} = 1$.

Now $B_{x_i, y_j}$, $B_{x, y_j}$ and $B_{x_i, y}$ are all nonzero and contained in the set $\{1, \omega, \omega^2\}$. Therefore, so is $B_{x,y}$. This completes the proof. □

The proof of Proposition 4.1.6 depends on Lemma 4.1.5, and therefore on the condition $n < 17$. No counterexamples are known for any value of $n$, and we conjecture that this result is true in general. This could be true if a type of connectivity result can be proven for 3-covers, or perhaps if no more such covers exist with $n > 17$. This appears to be an open question.

**Conjecture 4.1.7.** *A 3-cover of a symmetric design with block size $k+1$ and $\lambda = 3$ is equivalent to taking the incidence matrix $A$ of the design and replacing each 1 of the matrix with a 1, $\omega$, or $\omega^2$ in such a way that the resulting matrix has $BB^* = (k+1)I$.*

This conjecture appears as Theorem 4 in Biggs and Ito [3], but the proof is lacking. At the crucial step it appeals to "similar arguments." The similar arguments would suffer from the same sort of deficiency addressed by Lemma 4.1.5, and so would only work for small values of $k$.

$D_1 =$

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 |
| 2 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 0 |
| 3 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 1 |
| 4 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 1 |
| 5 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 |
| 6 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 |
| 7 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 |
| 8 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 1 |
| 9 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 |
| 10 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 |
| 11 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 0 |
| 12 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1 |
| 13 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 |
| 14 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 |
| 15 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |

Figure 4.1: The first of five nonisomorphic $(15, 7, 3)$ designs given by Nandi [17].

## 4.2 Existence and uniqueness of an elliptic semiplane with 45 points

In this section, we will show that there is a unique elliptic semiplane on 45 points, realized as the 3-fold cover of a $(15, 7, 3)$ design. Nandi [17] classifies all $(15, 7, 3)$ designs up to isomorphism. There are five isomorphism classes, which we will call $D_1, D_2, \ldots, D_5$. The incidence matrices of a representative of each isomorphism class are given in Figures 4.1–4.5 both for completeness, and because they are used extensively in the uniqueness proof for the covering design.

To prove uniqueness, we will use the following technical lemma in several places.

**Lemma 4.2.1.** *Suppose*

$$M = \begin{bmatrix} 0 & 1 & 1 \\ 1 & a & b \\ 1 & c & d \end{bmatrix}$$

*is a submatrix in an incidence matrix of a* 3*-design, where the* 1*s have been replaced by cube roots of unity as described in Proposition 4.1.6, and each of* $a, b, c$*, and* $d$ *is*

$D_2 =$

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 |
| 2 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 0 |
| 3 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 1 |
| 4 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 1 |
| 5 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 |
| 6 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 |
| 7 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 0 |
| 8 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 1 |
| 9 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 |
| 10 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 |
| 11 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 |
| 12 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1 |
| 13 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 |
| 14 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 |
| 15 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |

Figure 4.2: The second of five nonisomorphic $(15, 7, 3)$ designs given by Nandi [17].

$D_3 =$

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 |
| 2 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 0 |
| 3 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 |
| 4 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 1 |
| 5 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 |
| 6 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 |
| 7 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 0 |
| 8 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 1 |
| 9 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 |
| 10 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 |
| 11 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 |
| 12 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 1 |
| 13 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 0 |
| 14 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 0 |
| 15 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |

Figure 4.3: The third of five nonisomorphic $(15, 7, 3)$ designs given by Nandi [17].

$D_4 =$

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 |
| 2 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 0 |
| 3 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 1 |
| 4 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 |
| 5 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 |
| 6 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 |
| 7 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 |
| 8 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 |
| 9 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 |
| 10 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 0 |
| 11 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 0 |
| 12 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1 |
| 13 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 |
| 14 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 |
| 15 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |

Figure 4.4: The fourth of five nonisomorphic $(15, 7, 3)$ designs given by Nandi [17].

$D_5 =$

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 |
| 2 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 |
| 3 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 |
| 4 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 |
| 5 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 1 |
| 6 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 |
| 7 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 |
| 8 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 0 |
| 9 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 |
| 10 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 1 |
| 11 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 |
| 12 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 |
| 13 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 |
| 14 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 |
| 15 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |

Figure 4.5: The fifth of five nonisomorphic $(15, 7, 3)$ designs given by Nandi [17].

*nonzero. Then $a = d$, $b = c$, and $a \neq b$.*

*Proof.* Considering the second and third rows, we must have

$$\{1, a\overline{b}, c\overline{d}\} = \{1, \omega, \omega^2\}.$$

In particular, $a\overline{b} \neq 1$, so $a \neq b$, and $c\overline{d} \neq 1$, so $c \neq d$.

Suppose $b \neq c$. Then

$$\{a, b, c\} = \{d, b, c\} = \{1, \omega, \omega^2\}.$$

So $a = d$. We have $\overline{a\overline{b}} = c\overline{a}$, so $b\overline{a} = c\overline{a}$, and $b = c$, a contradiction.

So we have $b = c$, and $\overline{a\overline{b}} = b\overline{d}$, so $b\overline{a} = b\overline{d}$, and $a = d$. □

**Theorem 4.2.2.** *There is a unique elliptic semiplane on* 45 *points and lines with* 7 *points on a line.*

*Proof.* Suppose that such an elliptic semiplane exists. Then it must be a 3-fold cover of a $(15, 7, 3)$ design. Nandi [17] gives a classification of $(15, 7, 3)$ designs up to isomorphism, of which there are five, given in Figures 4.1–4.5. We will show that each of the designs $D_1, D_2, D_3$, and $D_4$ do not admit a 3-cover.

Suppose that a 3-fold cover of the design $D_1$ in Figure 4.1 exists. Consider the line given by row 1 and the non-incident point given by column 5. We isolate the

rows and columns corresponding to this line and point as

| | 5 | 1 | 2 | 3 | 4 | 9 | 10 | 11 |
|---|---|---|---|---|---|---|---|---|
| 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 2 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 |
| 5 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 1 |
| 7 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 |
| 9 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 0 |
| 11 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 |
| 12 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 |
| 14 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 1 |

We proceed using Proposition 4.1.6 to replace each 1 with 1, $\omega$, or $\omega^2$. We may assume that the first row and column here have 1s. Then each other row and column must contain one each of 1, $\omega$, and $\omega^2$. Without loss of generality, assume that those entries in row 2 are 1, $\omega$, and $\omega^2$, in that order. Let $A, B, C$, and $D$ be the entries in positions $(9,2), (9,9), (11,2)$, and $(11,9)$ respectively. We must have $C = B$ and $D = A$, by Lemma 4.2.1. Also, neither of $A$ and$B$ can be $\omega$ because $\omega$ is in position $(1,2)$. Therefore, any row or column that contains $A$ and $B$ must contain $\omega$ as the third entry. This implies that $(9,4), (11,10)$, and $(14,9)$ all contain $\omega$. Columns 4 and 10 both contain an $\omega$, so the third entry in row 12, $(12,3)$ must be $\omega$. Now $(14,3)$ must be 1, and $(14,11)$ must be $\omega^2$.

But now consider the $2 \times 2$ submatrix given by $(5,1), (5,11), (7,1)$, and $(7,11)$. Column 1 contains a 1 and column 11 contains an $\omega^2$, which means there is no way to fill in this $2 \times 2$ matrix consistent with Lemma 4.2.1. We have the following, with undetermined entries blank, and the $2 \times 2$ matrix which leads to a contradiction

marked by $X$

| | 5 | 1 | 2 | 3 | 4 | 9 | 10 | 11 |
|---|---|---|---|---|---|---|---|---|
| 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 2 | 1 | 1 | $\omega$ | $\omega^2$ | 0 | 0 | 0 | 0 |
| 5 | 1 | X | 0 | 0 | | 0 | 0 | X |
| 7 | 1 | X | 0 | 0 | 0 | 0 | | X |
| 9 | 1 | 0 | A | 0 | $\omega$ | B | 0 | 0 |
| 11 | 1 | 0 | B | 0 | 0 | A | $\omega$ | 0 |
| 12 | 1 | 0 | 0 | $\omega$ | | 0 | | 0 |
| 14 | 1 | 0 | 0 | 1 | 0 | $\omega$ | 0 | $\omega^2$ |

Suppose that a 3-fold cover of the design $D_2$ in Figure 4.2 exists. Consider the line given by row 1 and the non-incident point given by column 7. We isolate the rows and columns corresponding to this line and point as

| | 7 | 1 | 2 | 3 | 4 | 9 | 10 | 11 |
|---|---|---|---|---|---|---|---|---|
| 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 3 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 0 |
| 4 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 |
| 7 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 |
| 9 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 0 |
| 10 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 1 |
| 13 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 |
| 14 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 1 |

We proceed using Proposition 4.1.6 to replace each 1 with 1, $\omega$, or $\omega^2$. We may assume that the first row and column here have 1s. Then each other row and column must contain one each of 1, $\omega$, and $\omega^2$. Without loss of generality, assume that those entries in row 3 are 1, $\omega$, and $\omega^2$, in that order. Consider the $2 \times 2$ nonzero matrix formed by entries $(3,1), (3,10), (7,1)$, and $(7,10)$. By Lemma 4.2.1 we have that $(7,1)$ is $\omega^2$ and $(7,10)$ is 1.

Now consider the $2 \times 2$ submatrix given by $(9,2), (9,4), (10,2)$, and $(10,4)$. Following Lemma 4.2.1, label these entries as $A, B, B$, and $A$ respectively. Column 2 contains an $\omega$ outside of this $2 \times 2$ submatrix, so $\{A, B, \omega\} = \{1, \omega, \omega^2\}$. This means that $(13,4)$ must be $\omega$, yet this makes $(13,10)$ have no possible entry, a contradiction, which we mark by X in the table shown here for clarity.

| | 7 | 1 | 2 | 3 | 4 | 9 | 10 | 11 |
|---|---|---|---|---|---|---|---|---|
| 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 3 | 1 | 1 | $\omega$ | 0 | 0 | 0 | $\omega^2$ | 0 |
| 4 | 1 | $\omega$ | 0 | | 0 | 0 | 0 | |
| 7 | 1 | $\omega^2$ | 0 | 0 | 0 | | 1 | 0 |
| 9 | 1 | 0 | A | 0 | B | | 0 | 0 |
| 10 | 1 | 0 | B | 0 | A | 0 | 0 | |
| 13 | 1 | 0 | 0 | | $\omega$ | 0 | X | 0 |
| 14 | 1 | 0 | 0 | | 0 | | 0 | |

Suppose that a 3-fold cover of the design $D_3$ in Figure 4.3 exists. Consider the line given by row 1 and the non-incident point given by column 6. We isolate the rows and columns corresponding to this line and point as

| | 6 | 1 | 2 | 3 | 4 | 9 | 10 | 11 |
|---|---|---|---|---|---|---|---|---|
| 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 3 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 |
| 5 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 1 |
| 6 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 |
| 8 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 |
| 11 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 |
| 13 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 |
| 14 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 1 |

We proceed using Proposition 4.1.6 to replace each 1 with 1, $\omega$, or $\omega^2$. We may

assume that the first row and column here have 1s. Then each other row and column must contain one each of 1, $\omega$, and $\omega^2$. Without loss of generality, assume that those entries in row 3 are 1, $\omega$, $\omega^2$, in that order. Now the entries $(5,1),(5,4),(6,1)$, and $(6,4)$ form a $2 \times 2$ nonzero submatrix. By Lemma 4.2.1, label these as $A, B, B$, and $A$ respectively. We have $\{A, B\} = \{\omega, \omega^2\}$, so entry $(6,10)$ must be 1. Consider now the nonzero $2 \times 2$ matrix given by $(8,2),(8,10),(11,2)$, and $(11,10)$. There is no consistent way to fill in this matrix according to Lemma 4.2.1, since column 2 already contains $\omega$ and column 10 already contains 1.

So this gives a contradiction. For clarity, here is the partially completed matrix, with incomplete entries blank and the contradiction marked by $X$.

| | 6 | 1 | 2 | 3 | 4 | 9 | 10 | 11 |
|---|---|---|---|---|---|---|---|---|
| 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 3 | 1 | 1 | $\omega$ | 0 | 0 | $\omega^2$ | 0 | 0 |
| 5 | 1 | A | 0 | 0 | B | 0 | 0 | |
| 6 | 1 | B | 0 | 0 | A | 0 | 1 | 0 |
| 8 | 1 | 0 | X | | 0 | 0 | X | 0 |
| 11 | 1 | 0 | X | 0 | 0 | 0 | X | |
| 13 | 1 | 0 | 0 | | | | 0 | 0 |
| 14 | 1 | 0 | 0 | | 0 | | 0 | |

Suppose that a 3-fold cover of the design $D_4$ in Figure 4.4 exists. Consider the line given by row 2 and the non-incident point given by column 6. We isolate the

rows and columns corresponding to this line and point as

| | 6 | 1 | 2 | 3 | 5 | 12 | 13 | 14 |
|---|---|---|---|---|---|---|---|---|
| 2 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 3 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 0 |
| 4 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 0 |
| 5 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 1 |
| 10 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 |
| 11 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 0 |
| 13 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 1 |
| 14 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 |

We proceed using Proposition 4.1.6 to replace each 1 with 1, $\omega$, or $\omega^2$. We may assume that the first row and column here have 1s. Then each other row and column must contain one each of 1, $\omega$, and $\omega^2$. Without loss of generality, assume that those entries in column 1 are 1, $\omega$, and $\omega^2$, in that order. There is a nonzero $2 \times 2$ matrix formed by $(4,3),(4,12),(13,3)$, and $(13,12)$. By Lemma 4.2.1 label these entries as $A, B, B$, and $A$ respectively. Then since row 4 also contains $\omega$, we have that $\{A, B\} = \{1, \omega^2\}$, and any row or column with $A$ and $B$ must contain $\omega$ as the third nonzero entry. This implies that $(13,14),(14,3)$, and $(11,12)$ are all $\omega$.

There is also another $2 \times 2$ nonzero submatrix, formed by $(3,2),(3,13),(10,2)$, and $(10,13)$. Label these entries as $C, D, D$, and $C$ respectively. Since row 3 already contains a 1, we must have $\{C, D\} = \{\omega, \omega^2\}$, and any row or column which contains $C$ and $D$ must contain 1 as its third nonzero entry. This implies that $(10,14),(11,2)$, and $(14,13)$ are all 1. Entry $(5,14)$ now gives a contradiction, because row 5 contains an $\omega^2$, but column 14 contains 1 and $\omega$. For clarity, we show the partially completed

matrix below, with incomplete entries blank and the contradiction shown as $X$.

| | 6 | 1 | 2 | 3 | 5 | 12 | 13 | 14 |
|---|---|---|---|---|---|---|---|---|
| 2 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 3 | 1 | 1 | C | 0 | 0 | 0 | D | 0 |
| 4 | 1 | $\omega$ | 0 | A | 0 | B | 0 | 0 |
| 5 | 1 | $\omega^2$ | 0 | 0 | | 0 | 0 | X |
| 10 | 1 | 0 | D | 0 | 0 | 0 | C | 1 |
| 11 | 1 | 0 | 1 | 0 | | $\omega$ | 0 | 0 |
| 13 | 1 | 0 | 0 | B | 0 | A | 0 | $\omega$ |
| 14 | 1 | 0 | 0 | $\omega$ | | 0 | 1 | 0 |

So far we have shown that there are no 3-covers of the designs $D_1$ through $D_4$. It remains to show that there is a unique 3-cover of the design $D_5$. We also proceed here by using Proposition 4.1.6.

So if there is a 3-cover of a $(15, 7, 3)$-design, then it is a cover of Nandi's design $D_5$, from Figure 4.5. This design is isomorphic to the incidence matrix for lines of the 3-dimensional projective geometry over $GF(2)$, $PG(3, 2)$. By Proposition 4.1.6, if there is a 3-cover then it is possible to replace each 1 in $D_5$ with a cube root of unity, such that the resulting matrix $B$ satisfies $BB^* = 7I$.

Consider a line and a point not incident with the line. There are 7 points on the line and 7 lines incident with the point. Consider the $7 \times 7$ incidence matrix formed by these lines and points. Since the full design is $PG(3, 2)$, this is the incidence matrix of a $PG(2, 2)$. The projective plane $PG(3, 2)$ is unique up to isomorphism, and is isomorphic to the cyclic design generated by $\{1, 2, 4\}$ over $\mathbb{Z}_7$. For example, in our

case, we choose the row 1 and the column 6 from $D_5$, and obtain

| | 6 | 1 | 2 | 10 | 9 | 4 | 11 | 3 |
|---|---|---|---|---|---|---|---|---|
| 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 2 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 0 |
| 11 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| 14 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 |
| 12 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 1 |
| 7 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 |
| 9 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 |
| 5 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 |

Let the lower right $7 \times 7$ submatrix of this $8 \times 8$ matrix be $R$. Then we can permute the columns and rows of the matrix $D_5$ to make the matrix be of the form

$$\left[\begin{array}{c|ccc|ccc} 0 & 1 & \cdots & 1 & 0 & \cdots & 0 \\ \hline 1 & & & & & & \\ \vdots & & \mathrm{R} & & & \mathrm{R} & \\ 1 & & & & & & \\ \hline 0 & & & & & & \\ \vdots & & \mathrm{R} & & & \mathrm{X} & \\ 0 & & & & & & \end{array}\right],$$

where $X$ is a cyclic $7 \times 7$ matrix. The row ordering is

$$\{1, 2, 11, 14, 12, 7, 9, 5, 3, 10, 15, 13, 6, 8, 4\},$$

and the column ordering is

$$\{6, 1, 2, 10, 9, 4, 11, 3, 13, 12, 8, 5, 14, 7, 15\}.$$

The matrix $X$ is

$$X = \begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \end{bmatrix},$$

which is a cyclic matrix.

Suppose that there is a 3-cover, and the matrix $B$ is the matrix $D_5$ with each 1 replaced by a root of unity, 1, $\omega$ or $\omega^2$. Without loss of generality, we may assume that each 1 in row 1 or column 6 is replaced by 1 (multiply each row $i$ with a nonzero entry in column 6 by $\overline{B_{i6}}$ and each column $j$ with a nonzero entry in row 1 by $\overline{B_{1j}}$). Each row and each column of the $7 \times 7$ submatrix above, bordered by column 6 and row 1, must contain a 1, a $\omega$ and a $\omega^2$ to satisfy the condition $BB^* = 7I$, specifically that the off diagonal entries are 0.

Now consider the upper left $R$. Without loss of generality, we may assume that the nonzero entries in the first row are 1, $\omega$ and $\omega^2$ in that order. When we perform a row permutation operation between columns in this matrix $R$, we simultaneously perform the corresponding column operation on the upper right matrix $R$, so that at every step, all 3 matrices $R$ have corresponding nonnegative entries. That is, at any step, $(i, j)$ is nonzero for $i, j \in \{2, \ldots, 8\}$ if and only if $(i + 7, j)$ and $(i, j + 7)$ are nonzero. Also, since $X_{ij}$ is nonzero if and only if $R_{ij}$ is zero, at every step it remains the case that $(i + 7, j + 7)$ is nonzero if and only if $(i, j)$ is nonzero. We do the same for column permutation operations.

If the second row of the upper right matrix $R$ now does not contain first nonzero entry 1, then the sixth row does (rows 1, 2, and 6 being the rows of $R$ with nonzero entries in column 2, and $R_{12} = \omega$, $R_{22} = \omega^2$). In that case, perform the row and column operations swapping rows 2 and 6, and making the nonzero entries of the matrix be those of $R$ once again, without moving the the nonzero entries in row 1 or

the entry in position $(2,2)$ at any step.

Now suppose the entry in position $(2,3)$ is not $\omega$. Then it must be $\omega^2$ and position $(2,5)$ is $\omega$. Swap columns 3 and 5, and then perform more row and column operations without moving columns $1,2,3$, and 5 and without moving rows 1 and 2 so that the nonzero entries of the matrix are again those of $R$.

Suppose that the entry in position $(3,3)$ is not 1. Then it must be $\omega^2$, since $(2,3)$ is already $\omega$. We now make a sequence of simple deductions which lead to a unique matrix.

Column 2 contains 1 and $\omega$, so the last unknown entry, in positions $(2,6)$ must be $\omega^2$. Columns 4 and 5 both contain $\omega^2$, and row 4 has nonzero positions in columns $4,5$, and 7, so $(5,7)$ is $\omega^2$. Column 3 contains $\omega$ and $\omega^2$, so $(7,3)$ is 1. Row 7 contains 1 and column 7 contains $\omega^2$, so $(7,7)$ is $\omega$, and the final nonzero entry in row 7, $(7,1)$ is $\omega^2$. This makes the final nonzero entry in column 1, $(1,5)$ a $\omega$, the final entry in column 7, $(7,6)$ is 1, the final entry in row 6, $(6,6)$ is $\omega$. Then column 5 contains $\omega^2$ and row 5 contains $\omega$, so $(5,5)$ is 1. Now the rest of the deductions are rows which contain only one unresolved nonzero entry. Finally, we obtain the matrix

$$R_1 = \begin{bmatrix} 1 & \omega & 0 & \omega^2 & 0 & 0 & 0 \\ 0 & 1 & \omega & 0 & \omega^2 & 0 & 0 \\ 0 & 0 & \omega^2 & \omega & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & \omega & 0 & \omega^2 \\ \omega & 0 & 0 & 0 & 1 & \omega^2 & 0 \\ 0 & \omega^2 & 0 & 0 & 0 & \omega & 1 \\ \omega^2 & 0 & 1 & 0 & 0 & 0 & \omega \end{bmatrix}.$$

If instead we suppose position $(3,3)$ contains 1, then row 3 and column 4 contain 1 and $\omega^2$ respectively, so $(3,4)$ contains $\omega$. Then $(3,6)$ must be $\omega^2$, since row 3 contains

1 and $\omega$. The same deductions follow until we get the matrix

$$R_2 = \begin{bmatrix} 1 & \omega & 0 & \omega^2 & 0 & 0 & 0 \\ 0 & 1 & \omega & 0 & \omega^2 & 0 & 0 \\ 0 & 0 & 1 & \omega & 0 & \omega^2 & 0 \\ 0 & 0 & 0 & 1 & \omega & 0 & \omega^2 \\ \omega^2 & 0 & 0 & 0 & 1 & \omega & 0 \\ 0 & \omega^2 & 0 & 0 & 0 & 1 & \omega \\ \omega & 0 & \omega^2 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

The matrix $R_1$ can be obtained from $R_2$ by performing the operation $\omega \leftrightarrow \omega^2$ and performing column and row permutations. So these two types of covers are isomorphic.

So up to isomorphism there is a unique way to fill in the upper left $8 \times 8$ submatrix. Assume that the upper left $R$ is filled in as $R_2$, and consider a column numbered between $j+8$ for some $j \in \{1, \ldots, 7\}$. This column shares 3 nonzero entries with columns 1 and $j+1$. These 3 corresponding rows of column $j+8$ must therefore contain $1, \omega$, and $\omega^2$ in some order, so that columns 1 and $j+8$ satisfy the requirement in $BB^* = 7I$. Multiply column $j+8$ by a cube root of unity, so that the 1 from column $j+1$ is in the same row as the 1 from column $j+8$. This multiplication is an isomorphism, so we now must have the $\omega$ from column $j+1$ in the same row as the $\omega^2$ from column $j+8$, and the $\omega^2$ from column $j+1$ in the same row as the $\omega$ from column $j+1$. The same can be done for rows 9–15, so that the cover is isomorphic

to one with matrix

$$\begin{bmatrix}
0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & \omega & 0 & \omega^2 & 0 & 0 & 0 & 1 & \omega^2 & 0 & \omega & 0 & 0 & 0 \\
1 & 0 & 1 & \omega & 0 & \omega^2 & 0 & 0 & 0 & 1 & \omega^2 & 0 & \omega & 0 & 0 \\
1 & 0 & 0 & 1 & \omega & 0 & \omega^2 & 0 & 0 & 0 & 1 & \omega^2 & 0 & \omega & 0 \\
1 & 0 & 0 & 0 & 1 & \omega & 0 & \omega^2 & 0 & 0 & 0 & 1 & \omega^2 & 0 & \omega \\
1 & \omega^2 & 0 & 0 & 0 & 1 & \omega & 0 & \omega & 0 & 0 & 0 & 1 & \omega^2 & 0 \\
1 & 0 & \omega^2 & 0 & 0 & 0 & 1 & \omega & 0 & \omega & 0 & 0 & 0 & 1 & \omega^2 \\
1 & \omega & 0 & \omega^2 & 0 & 0 & 0 & 1 & \omega^2 & 0 & \omega & 0 & 0 & 0 & 1 \\
0 & 1 & \omega^2 & 0 & \omega & 0 & 0 & 0 & 0 & 0 & & 0 & & & \\
0 & 0 & 1 & \omega^2 & 0 & \omega & 0 & 0 & & 0 & 0 & & 0 & & \\
0 & 0 & 0 & 1 & \omega^2 & 0 & \omega & 0 & & & 0 & 0 & & 0 & \\
0 & 0 & 0 & 0 & 1 & \omega^2 & 0 & \omega & & & & 0 & 0 & & 0 \\
0 & \omega & 0 & 0 & 0 & 1 & \omega^2 & 0 & 0 & & & & 0 & 0 & \\
0 & 0 & \omega & 0 & 0 & 0 & 1 & \omega^2 & & 0 & & & & 0 & 0 \\
0 & \omega^2 & 0 & \omega & 0 & 0 & 0 & 1 & 0 & & 0 & & & & 0
\end{bmatrix}.$$

Consider the blank entry in position $(9, 11)$. Call this entry $x$. Consider the product of row 3 with the conjugate of row 9. In column 3, the product is $1\overline{\omega^2} = \omega$. In column 11, this product is $\omega^2\overline{x}$. So $\overline{x} \neq \omega^2$, which means $x \neq \omega$. Consider the product of row 8 with the conjugate of row 9. In column 2, the product is $\omega\overline{1} = \omega$, and in column 11, this product is $\omega\overline{x}$, so $x \neq 1$. This means $x = \omega^2$.

Now consider the blank entry in position $(9, 13)$, and call this entry $x$. The product of row 3 with the conjugate of row 9 shows that the product in column 2, $\omega^2\overline{1} = \omega^2$, is distinct from the product in column 13, $1\overline{x} = \overline{x}$, so $x \neq \omega$. The product of row 3 with the conjugate of row 9 shows that the product in column 3, $1\overline{\omega^2} = \omega$, is distinct from the product in column 13, $\omega\overline{x}$, so $x \neq 1$. This means $x = \omega^2$.

Similarly, consider the blank entry in position $(9, 14)$, and call this entry $x$. We look at the product of row 7 with the conjugate of row 9 to see that the product in column 3, $\omega^2\overline{\omega^2} = 1$, is distinct from the product in column 14, $1\overline{x}$. So $x \neq 1$. We

look at the product of row 4 with the conjugate of row 9 to see that the product in column 5, $\omega\overline{\omega} = 1$, is distinct from the product in column 14, $\omega\overline{x}$. So $x \neq \omega$ and $x = \omega^2$.

Now consider the blank entry in position $(9, 15)$. Call it $x$. Look at the product of row 7 with row 9. From column 3 we have $\omega^2\overline{\omega^2} = 1$, from column 14 we have $1\overline{\omega^2} = \omega$, and from column 15 we have $\omega^2\overline{x}$. So we have

$$\{1, \omega, \omega^2\} = \{1, \omega, \omega^2\overline{x}\}.$$

So $\omega^2\overline{x} = \omega^2$ and $x = 1$.

Altogether, the first row of the lower right $7 \times 7$ submatrix is

$$(0, 0, \omega^2, 0, \omega^2, \omega^2, 1).$$

Now consider a cyclic rotation of each of the four major $7 \times 7$ submatrices, by rotating the rows one position to the right, and then the columns one position to the bottom, within each of the four $7 \times 7$ submatrices. That is, the product of the row permutation

$$(2, 3, 4, 5, 6, 7, 8)(9, 10, 11, 12, 13, 14, 15)$$

and the same column permutation. The three major $7 \times 7$ submatrices (other than the lower right one) are invariant under this operation, since they are cyclic. The arguments above now apply to the new lower right matrix, showing that the first row is again

$$(0, 0, \omega^2, 0, \omega^2, \omega^2, 1).$$

Applying this operation repeatedly, we see that the lower right $7 \times 7$ submatrix must also be cyclic. So the cover is unique up to isomorphism, if it exists. Checking

that $BB^* = 7I$ is now straightforward. We have

$$B = \begin{bmatrix}
0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & \omega & 0 & \omega^2 & 0 & 0 & 0 & 1 & \omega^2 & 0 & \omega & 0 & 0 & 0 \\
1 & 0 & 1 & \omega & 0 & \omega^2 & 0 & 0 & 0 & 1 & \omega^2 & 0 & \omega & 0 & 0 \\
1 & 0 & 0 & 1 & \omega & 0 & \omega^2 & 0 & 0 & 0 & 1 & \omega^2 & 0 & \omega & 0 \\
1 & 0 & 0 & 0 & 1 & \omega & 0 & \omega^2 & 0 & 0 & 0 & 1 & \omega^2 & 0 & \omega \\
1 & \omega^2 & 0 & 0 & 0 & 1 & \omega & 0 & \omega & 0 & 0 & 0 & 1 & \omega^2 & 0 \\
1 & 0 & \omega^2 & 0 & 0 & 0 & 1 & \omega & 0 & \omega & 0 & 0 & 0 & 1 & \omega^2 \\
1 & \omega & 0 & \omega^2 & 0 & 0 & 0 & 1 & \omega^2 & 0 & \omega & 0 & 0 & 0 & 1 \\
0 & 1 & \omega^2 & 0 & \omega & 0 & 0 & 0 & 0 & 0 & \omega^2 & 0 & \omega^2 & \omega^2 & 1 \\
0 & 0 & 1 & \omega^2 & 0 & \omega & 0 & 0 & 1 & 0 & 0 & \omega^2 & 0 & \omega^2 & \omega^2 \\
0 & 0 & 0 & 1 & \omega^2 & 0 & \omega & 0 & \omega^2 & 1 & 0 & 0 & \omega^2 & 0 & \omega^2 \\
0 & 0 & 0 & 0 & 1 & \omega^2 & 0 & \omega & \omega^2 & \omega^2 & 1 & 0 & 0 & \omega^2 & 0 \\
0 & \omega & 0 & 0 & 0 & 1 & \omega^2 & 0 & 0 & \omega^2 & \omega^2 & 1 & 0 & 0 & \omega^2 \\
0 & 0 & \omega & 0 & 0 & 0 & 1 & \omega^2 & \omega^2 & 0 & \omega^2 & \omega^2 & 1 & 0 & 0 \\
0 & \omega^2 & 0 & \omega & 0 & 0 & 0 & 1 & 0 & \omega^2 & 0 & \omega^2 & \omega^2 & 1 & 0
\end{bmatrix}.$$

□

The original construction of this elliptic semiplane is due to Baker [1]. In Baker's construction, there are four types of $3 \times 3$ submatrices, corresponding to our 1, $\alpha$, $\beta$, and $\gamma$. By uniqueness, Baker's elliptic semiplane is isomorphic to $B$.

Ito [10] states this same uniqueness result in the context of the corresponding bipartite graph, but only gives the proof beginning with the $PG(3, 2)$, Nandi's design $D_5$.

We now give an alternative construction of the elliptic semiplane in terms of the Petersen graph.

For each $i = 1, 2, 3$, let $A_i$ be the set of elements of the form $(S, i)_A$, where $S$ is a set of two disjoint pairs in $\{1, 2, 3, 4, 5\}$, that is, an edge in the Petersen graph, and let $B_i$ be the set of elements of the form $(S, i)_B$ with the same condition on $S$.

Let $G$ be a bipartite graph with vertex set

$$(A_1 \cup A_2 \cup A_3) \cup (B_1 \cup B_2 \cup B_3).$$

Let $d(x, y)$ denote the distance between $x$ and $y$ in the line graph of the Petersen graph. Then in $G$, $(S, i)_A$ is adjacent to $(T, j)_B$ if and only if one of the following conditions is true

(i) $i \equiv j (\text{mod } 3)$ and $d(S, T) = 0$,

(ii) $i \equiv j - 1 (\text{mod } 3)$ and $d(S, T) = 3$, or

(iii) $i \equiv j - 2 (\text{mod } 3)$ and $d(S, T) = 1$.

The following proposition shows that the configuration represented by the bipartite graph $G$ with blocks $A_1 \cup A_2 \cup A_3$ and points $B_1 \cup B_2 \cup B_3$ satisfies conditions 1 and 2 of Definition 4.1.1.

**Proposition 4.2.3.** *The graph $G$ has valency 7 and girth 6.*

*Proof.* Considering the line graph of the Petersen graph, because Sym(5) acts as graph automorphisms, we need only consider the vertex $\{\{1, 2\}, \{3, 4\}\}$. For simplified notation, we will write $(ij)(k\ell)$ for $\{\{i, j\}, \{k, \ell\}\}$. The vertices at distance 1 are

$$(12)(35), (12)(45), (15)(34), (25)(34).$$

The vertices at distance 2 are

$$(14)(35), (24)(35), (13)(45), (23)(45), (15)(23), (15)(24), (13)(25), (14)(25).$$

The vertices at distance 3 are

$$(13)(24), (14)(23).$$

In particular, there are 2 vertices at distance 3 and 4 vertices at distance 1, so the

degree of the vertex $((12)(34), 1)_A$ is $1 + 2 + 4 = 7$, and by symmetry $G$ is regular of valency 7.

Now to see $G$ has girth 6 we must show that there are no 4 cycles in $G$. Suppose there is a 4 cycle. Then without loss of generality, it contains $((12)(34), 1)_A$. In fact, suppose the cycle is

$$((12)(34), 1)_A, (S_x, x)_B, (S_y, y)_A, (S_z, z)_B, ((12)(34), 1)_A.$$

Consider the possible triples $(x, y, z)$. Let $q$ be the sum of the distances

$$q = d((12)(34), S_x) + d(S_x, S_y) + d(S_y, S_z) + d(S_z, (12)(34)).$$

In order for this to be a cycle, $q$ must be even. Each of the terms in the sum is $1, 3$, or 0, so each term is even if and only if it is 0. So in the sequence $(1, x, y, z, 1)$ the number of elements which are equal to the next element must be even. We will call this the $q$ even rule.

Clearly $(x, y, z)$ is equivalent to $(z, y, x)$ by reversing the order of the cycle. We break down the cases as follows, where for those cases with $x \neq z$, we always consider the case where $z < x$. There are 18 possible triples $(x, y, z)$ with $z \leq x$.

Case $(x, y, z) = (1, 1, 1), (2, 1, 1), (3, 1, 1), (2, 2, 2)$ or $(3, 3, 3)$. Since there is only one edge between $A_i$ and $B_i$ for each $i$, these cases each contain a backtrack, so they do not exist.

Case $(x, y, z) = (1, 2, 1)$ or $(1, 3, 1)$. In this case $S_x = (12)(34)$ and $S_z \neq (12)(34)$, because otherwise this would be a backtrack, so this case also does not exist.

Case $(x, y, z) = (2, 2, 1)$ or $(3, 3, 1)$. In either case, we have $S_x = S_y$ and $S_z = (12)(34)$, but $d((12)(34), S_x) \neq d(S_y, S_z)$, a contradiction.

Case $(x, y, z) = (3, 3, 2), (3, 2, 1), (2, 3, 1)$, or $(3, 2, 2)$. These cases violate the $q$ even rule.

Case $(x, y, z) = (2, 1, 2)$. Each step is a step of distance 3 in the projection onto the line graph of the Petersen graph. But the set of vertices at distance 0 or 3 from

(12)(34) has size 3. Considering this set of 3 vertices as a triangle, any path of length 4 must contain backtracks (which correspond to backtracks in the path on the full graph $G$, since we are alternating between $A_1$ and $B_2$), or not end at the same vertex it began. Either way, this is a contradiction.

Case $(x, y, z) = (3, 1, 3)$. Similar to the previous case, we consider the projection onto the underlying line graph of the Petersen graph. Each step is a step of distance 1. The line graph of the Petersen graph contains triangles, but no cycles of length 4, so this case also cannot happen.

Case $(x, y, z) = (3, 1, 2), (3, 2, 3)$, or $(2, 3, 2)$. Each of these cases corresponds to two steps of distance 1 followed by two steps of distance 3, by symmetry and rotating the cycles. So, in the projection onto the line graph of the Petersen graph, these cycles correspond to successive steps of distance $1, 1, 3, 3$. After the first two steps of length 1, we end up at vertex $S_y \neq (12)(34)$, and $d((12)(34), S_y) < 3$. This is a contradiction, since $S_y, S_z, (12)(34)$ form a triangle with steps of distance 3. □

We claim that this is isomorphic to our construction $G$, and we complete the argument by showing that the Petersen construction represents an elliptic semiplane and then applying our uniqueness result, Theorem 4.2.2.

**Proposition 4.2.4.** *The graph $G$ corresponds to an elliptic semiplane on 45 points.*

*Proof.* To see that conditions 3 and 4 of Definition 4.1.1 apply, let $S$ be an edge of the Petersen graph and consider the three blocks corresponding to $(S, 1)_A$, $(S, 2)_A$, and $(S, 3)_A$. The union of the points contained in these lines are all those points of the form $(T, j)_B$, where $d(S, T) \in \{0, 1, 3\}$ and $j \in \{1, 2, 3\}$. So the union of these three blocks contains 21 distinct points. Therefore these three blocks are parallel. Since each block is parallel to exactly two other blocks, parallelism is transitive.

The parallelism quotient graph of $G$ is the bipartite graph with vertex set consisting of all vertices of the form $S_A$ or $S_B$, where $S$ is a union of two disjoint pairs from $\{1, 2, 3, 4, 5\}$. In other words, a vertex of $G$ with projection onto the first coordinate. A vertex $S_A$ is adjacent to a vertex $T_B$ if and only if $d(S, T) \in \{0, 1, 3\}$, where $d$

represents distance in the Petersen line graph. We need to show that in the block design corresponding to this quotient graph, each pair of blocks intersects in 3 points.

Let $(S_1)_A$ and $(S_2)_A$ be vertices in the quotient graph, with $S_1 \neq S_2$. Let $\Gamma_i = \{T : d(S_i, T) \in \{0, 1, 3\}\}$ for $i = 1, 2$. We must show that $|\Gamma_1 \cap \Gamma_2| = 3$. There are three cases.

Suppose $d(S_1, S_2) = 1$. Then $S_1, S_2 \in \Gamma_1 \cap \Gamma_2$. Distance 3 or 0 is an equivalence relation on vertices in the Petersen line graph, so

$$S \in (\Gamma_1 \cap \Gamma_2) \setminus \{S_1, S_2\}$$

is true if and only if $d(S_1, S) = 1$ and $d(S_2, S) = 1$. The Petersen graph has valency 3, so there is exactly one such $S$, and $|\Gamma_1 \cap \Gamma_2| = 3$.

Now suppose $d(S_1, S_2) = 2$. Without loss of generality, suppose $S_1 = \{12, 34\}$. Then the vertices at distance 3 from $S_1$ are $\{13, 24\}$ and $\{14, 23\}$. Each has valency 4, and the distance between them is 3, so there are at least 8 vertices $Y$ at distance 2 from $S_1$ such that there is a vertex $Z$ with $d(Y, Z) = 1$ and $d(S_1, Z) = 3$. One of these vertices $Y$ must be $S_2$, so there is exactly one vertex in $\Gamma_1 \cap \Gamma_2$ at distance 3 from $S_1$. Similarly, there is exactly one vertex in $\Gamma_1 \cap \Gamma_2$ at distance 3 from $S_2$. Also for any pair of vertices at distance 2 in the Petersen line graph, there is a unique vertex at distance 1 from both of them (since the Petersen graph has no triangles or 4-cycles). So $|\Gamma_1 \cap \Gamma_2| = 3$.

Now suppose $d(S_1, S_2) = 3$. Then the equivalence class of vertices at distance 3 is exactly $\Gamma_1 \cap \Gamma_2$. □

This completes the proof of our isomorphism result. We also state the following Proposition, for which the proof is a direct consequence of the uniqueness result.

**Proposition 4.2.5.** *As block designs, the graph $G$ constructed from the Petersen line graphs is isomorphic to the incidence matrix given by $B$ in the proof of Theorem 4.2.2.*

*Proof.* This follows immediately from Theorem 4.2.2. □

## 4.3 Automorphisms and dualities

Let $(P, L)$ be the Baker elliptic semiplane with point set $P$ and line set $L$. As proven in the previous section, the Baker semiplane is the unique 3-cover of a $(15, 7, 3)$ design, up to isomorphism.

An *automorphism* is a pair of permutations $\sigma \in Sym_P$ and $\tau \in Sym_L$ such that any $p \in P$ is incident to $l \in L$ if and only if $\sigma(p)$ is incident to $\tau(l)$. Let $A$ be the set of automorphisms of the Baker semiplane. The set $A$ forms a group.

A *duality* is a pair of bijections $\alpha : P \to L$ and $\beta : L \to P$ such that each $p \in P$ is incident to $l \in L$ if and only if $\beta(l)$ is incident to $\alpha(p)$.

The product of two dualities is an automorphism. Let $A^+$ be the set of all dualities and automorphisms. Then $A^+$ is a group with $[A^+ : A]$ either 1 or 2.

Let $F$ be the subgroup of $A$ which takes points to parallel points and lines to parallel lines. We call $F$ the *fiber stabilizer* of $A$, and we let $\bar{A} = A/F$, $\bar{A}^+ = A^+/F$.

Our main theorem is the following:

**Theorem 4.3.1.**

(a) *$F$ is isomorphic to $Z_3$,*

(b) *$A$ is isomorphic to $3 \cdot Alt_7$, and*

(c) *$A^+$ is isomorphic to $3 \cdot Sym_7$.*

A result given by Ito [10] states that $A^+ = A$. There seems to be a subtle mistake in the proof, as it contradicts Theorem 4.3.1.

First, we prove Theorem 4.3.1(a) directly by considering row and column operations on $3 \times 3$ submatrices of the $45 \times 45$ incidence matrix given in Theorem 4.2.2.

*Proof of* Theorem 4.3.1(a). As in the previous section, we label the different $3 \times 3$ permutation matrices as 1, $\omega$, $\omega^2$, $\alpha$, $\beta$, and $\gamma$. Row and column permutations act on the set of six permutation matrices according to Figures 4.6 and 4.7.

An element of $f \in F$ acts by permuting the rows and columns of the $45 \times 45$ incidence matrix such that parallel lines are sent to parallel lines and parallel columns

are sent to parallel columns. This means that the set of columns or rows numbered $\{1+3n, 2+3n, 3+3n\}$ is fixed globally for each $n = 0, 1, \ldots, 14$. Let $r_n$ be the row operation on rows $1+3n, 2+3n, 3+3n$, and $c_n$ be the column operation on columns $1+3n, 2+3n, 3+3n$ for each $n = 0, \ldots, 14$. Then $f$ is determined by choices of each $r_n$ and $c_n$. We will show that

$$r_0 = r_1 = \cdots = r_{14} = c_0 = c_1 = \cdots = c_{14},$$

and that $r_0 \in Alt_3 \cong Z_3$. Further, each of the three choices of permutation is an automorphism, so $F \cong Z_3$.

Suppose that $r_0 = 1 \in Sym(3)$. Then in order to preserve the entries in the first row of the matrix $B$, we must have $c_1 = c_2 = \cdots = c_7 = 1$. Each row has a nonzero entry in one of these 7 columns, and that entry is unchanged, so we have $r_0 = r_1 = \cdots = r_{14} = 1$. Each column has a nonzero entry, so we have $c_0 = c_1 = \cdots = c_{14} = 1$. Clearly this gives the identity automorphism.

Now suppose $r_0 \in Alt(3) \setminus \{1\}$. Then, according to Figures 4.6 and 4.7, in order to preserve the nonzero entries in the first row of $B$, we must have $c_1 = c_2 = \cdots = c_7 = r_0$. Each row has a nonzero entry in one of these 7 columns, which has been acted upon by the column operation $r_0$. The row operation $r_0$ acting on the set $\{1, \omega, \omega^2\}$ is the inverse to the column operation $r_0$. Therefore $r_0 = r_1 = r_2 = \cdots = r_{14}$. Similarly $c_0 = c_1 = \cdots = c_14 = r_0$, since every column has a nonzero entry in some row. This gives an automorphism of the incidence matrix of order 3.

Finally suppose $r_0 \in Sym(3) \setminus Alt(3)$. Then in order to preserve the entries in the first row of $B$, we must have $c_1 = c_2 = \cdots = c_7 = r_0$. Now consider the entries in positions $(2,2)$ and $(2,3)$ in the matrix $B$. These are both acted on by the column permutation $r_0$. But considering the odd permutations in Figures 4.6 and 4.7, there is no row permutation $r_1$ such that the row operation $r_1$ composed with the column operation $r_0$ would fix both 1 and $\omega$. This is a contradiction.

Therefore $r_0 \in Alt(3)$, each such choice giving exactly one automorphism. So $F$ is isomorphic to $Alt(3) = Z_3$. $\square$

| Row operation | Permutation on the set of $3 \times 3$ permutation matrices |
|---|---|
| 1 | 1 |
| (1,2) | $(1,\alpha)(\omega,\gamma)(\omega^2,\beta)$ |
| (1,3) | $(1,\gamma)(\omega,\beta)(\omega^2,\alpha)$ |
| (2,3) | $(1,\beta)(\omega,\alpha)(\omega^2,\gamma)$ |
| (1,2,3) | $(1,\omega^2,\omega)(\alpha,\gamma,\beta)$ |
| (1,3,2) | $(1,\omega,\omega^2)(\alpha,\beta,\gamma)$ |

Figure 4.6: Action of row permutations on the six $3 \times 3$ permutation matrices.

| Column operation | Permutation on the set of $3 \times 3$ permutation matrices |
|---|---|
| 1 | 1 |
| (1,2) | $(1,\alpha)(\omega,\beta)(\omega^2,\gamma)$ |
| (1,3) | $(1,\gamma)(\omega,\alpha)(\omega^2,\beta)$ |
| (2,3) | $(1,\beta)(\omega,\gamma)(\omega^2,\alpha)$ |
| (1,2,3) | $(1,\omega,\omega^2)(\alpha,\gamma,\beta)$ |
| (1,3,2) | $(1,\omega^2,\omega)(\alpha,\beta,\gamma)$ |

Figure 4.7: Action of column permutations on the six $3 \times 3$ permutation matrices.

In order to prove the rest of Theorem 4.3.1, we set aside some intermediate results as Lemmas.

First, we use a group construction of the graph $G$ from Proposition 4.2.3. In fact, let $S$ be the elements of $Sym_3$ and let $H$ be the conjugacy class in $Alt_5$ of elements of order 2 (of which there are 15, corresponding to the vertices of the Petersen line graph). Let $G'$ be the graph with vertices $S \times H$ and $(s,g),(t,h) \in G'$ adjacent if and only if one of the following is true:

(i) $st^{-1} = (1,2)$ and $|gh| = 1$,

(ii) $st^{-1} = (1,3)$ and $|gh| = 2$, or

(iii) $st^{-1} = (2,3)$ and $|gh| = 3$

This adjacency condition is symmetric, since whenever

$$st^{-1} \in \{(1,2),(1,3),(2,3)\},$$

we have $|st^{-1}| = 2$, so that $st^{-1} = ts^{-1}$.

**Proposition 4.3.2.** *The graph $G$ is isomorphic to the graph $G'$.*

*Proof.* Identify the elements in the 6 copies of the Petersen line graphs of $G$ and $G'$ by identifying each of the copies of the Petersen line graph in $G$ with one in $G'$ in the following way:

$$A_1 \sim 1, A_2 \sim (1,2,3), A_3 \sim (1,3,2), B_1 \sim (1,2), B_2 \sim (1,3), B_3 \sim (2,3).$$

Now, suppose $(s, g)$ and $(t, h)$ are adjacent. Then $st^{-1} \notin Alt_3$, so one of $s, t$ corresponds to an $A_i$ and the other to a $B_j$ for some $i, j \in \{1, 2, 3\}$. It is now easy to check given the correspondence above, that

(i) $st^{-1} = (1, 2)$ if and only if $i \equiv j (\text{mod } 3)$, $i \equiv j (\text{mod } 3)$ and $d(S, T) = 0$,

(ii) $st^{-1} = (1, 3)$ if and only if $i \equiv j - 1 (\text{mod } 3)$, and

(iii) $st^{-1} = (2, 3)$ if and only if $i \equiv j - 2 (\text{mod } 3)$.

It remains to show that $|gh|$ determines the distance between $g$ and $h$ in the Petersen line graph. In fact, it suffices to consider $g = (1, 2)(3, 4)$, and to consider Table 4.1. □

This group theoretic construction can be immediately used to establish a few properties of the automorphism group of the Baker elliptic semiplane, which we set aside as Lemma 4.3.3. These properties will combine with observations about the incidence matrix given in Theorem 4.2.2 to give more information about the automorphism group $A^+$, since Theorem 4.2.2 proves that these two objects are isomorphic as graphs.

**Lemma 4.3.3.**

(a) *The fiber stabilizer $F \cong Z_3$ is inverted by $A^+/A$ of order 2.*

(b) *$A^+$ has a subgroup $B^+$ isomorphic to $Sym_3 \times Sym_5$ whose image in $\bar{A}^+ \leq Sym_8$ is isomorphic to $Z_3 \times Sym_5$.*

| $h$ | $gh$ | $\lvert gh\rvert$ | $d(g,h)$ |
|---|---|---|---|
| (12)(34) | 1 | 1 | 0 |
| (12)(35) | (345) | 3 | 1 |
| (12)(45) | (354) | 3 | 1 |
| (13)(24) | (14)(23) | 2 | 3 |
| (13)(25) | (15234) | 5 | 2 |
| (13)(45) | (12354) | 5 | 2 |
| (14)(23) | (13)(24) | 2 | 3 |
| (14)(25) | (15243) | 5 | 2 |
| (14)(35) | (12453) | 5 | 2 |
| (15)(23) | (13425) | 5 | 2 |
| (15)(24) | (14325) | 5 | 2 |
| (15)(34) | (125) | 3 | 1 |
| (23)(45) | (13542) | 5 | 2 |
| (24)(35) | (14532) | 5 | 2 |
| (25)(34) | (152) | 3 | 1 |

Table 4.1: Correspondence between distance from $g$ and order of $|gh|$ in the Petersen line graph, where $g = (12)(34)$.

(c) *$B = B^+ \cap A$ has index 2 in $B^+$.*

*Proof.* The group $Sym_3 \times Sym_5$ acts faithfully as a group of automorphisms on the vertices of $G'$ by

$$(z, a) : (s, g) \mapsto (sz, a^{-1}ga).$$

Let $B^+$ be this subgroup of $A^+$. The subgroup $Alt_3 \times 1 \leq B^+$ is a subgroup of the fiber stabilizer $F$. By Theorem 4.3.1(a), we have $Alt_3 \times 1 = F$.

Consider the element $h = ((12), 1) \in B^+$. This element $h$ swaps the two parts of the bipartite graph $G'$, so is a duality. Let $B = B^+ \cap A$. Then we have $[A : B] = [A^+ : B^+]$, and $[A^+ : A] = 2$, so $[B^+ : B] = 2$. Let $k \in F$ be the element $((123), 1)$ in $B^+$. Then $hkh^{-1} = ((132), 1) = k^{-1}$. So $F$ is inverted by $B^+/B$, and therefore by $A^+/A$. □

**Lemma 4.3.4.**

(a) *$\bar{A}$ is isomorphic to a subgroup of $GL_4(2) \cong Alt_8$.*

(b) *$\bar{A}^+$ is isomorphic to a subgroup of $GL_4(2).2 \cong Sym_8$.*

(c) *$A$ contains an element of order 7.*

*Proof.* By Theorem 4.2.2, we know that the elliptic semiplane is unique and that its quotient by parallelism is isomorphic to $PG(3,2)$. The automorphism group of $PG(3,2)$ is $GL_4(2)$, because $PG(3,2)$ can be considered as $GL(2)^4$, where each 1-dimensional subspace is a point and each 3-dimensional subspace is a line. It is well known that $GL_4(2) \cong Alt_8$. This proves (a).

Since $[A^+ : A] \leq 2$, we know that $A$ is a normal subgroup of $A^+$. A duality of order 2 necessarily generates a subgroup $Z_2$, such that $Z_2 \cap A = 1$. By Lemma 4.3.3(a), such a duality exists, and it does not commute with $A$. This shows that $A^+ \neq A \times Z_2$, and therefore $A^+$ is a subgroup of an indirect extension of $Alt_8$ of degree 2, which must be $Sym_8$.

Part (c) follows because the product of the row permutation

$$(2,3,4,5,6,7,8)(9,10,11,12,13,14,15)$$

and the same column permutation on the matrix representing the elliptic semiplane in the proof of Theorem 4.2.2, leaves the matrix invariant. These permutations have order 7. □

**Lemma 4.3.5.**

(a) *$\bar{A}^+$ is isomorphic to $Sym_7$ or $Sym_8$.*

(b) *$\bar{A}$ is isomorphic to $Alt_7$ or $Alt_8$.*

*Proof.* By Lemma 4.3.3(b), $\bar{A}^+$ contains an element of order 2 which commutes with a subgroup isomorphic to $Sym_5$. In particular, $\bar{A}^+ \leq Sym_8$ contains commuting elements of order 2 and 5. Let $g \in Sym_8$ be an element of order 5, and let $h \in Sym_8$ be a commuting element of order 2. Then $g$ must consist of cycles of length dividing 5, so $g$ is a 5-cycle. Similarly, $h$ is a product of disjoint transpositions. Without loss of generality, let $g = (12345)$ and consider $hgh^{-1}$. We have

$$hgh^{-1} = (h(1), h(2), h(3), h(4), h(5)),$$

so $h(1) \in \{1,2,3,4,5\}$. The value of $h(1)$ determines the value of $h(2), h(3), h(4)$, and $h(5)$, and clearly powers of $g$ commute with $g$, so the only elements commuting with $g$ are powers of $g$. No power of $g$ has order 2, so $h$ must fix the set $\{1,2,3,4,5\}$. Therefore $h \in Sym\{6,7,8\}$, and $h$ is a 2-cycle.

Also, by Lemma 4.3.4(c), $\bar{A}^+$ contains an element of order 7. It is well known that in $Sym_p$ for a prime $p$, a $p$-cycle and a transposition generate all of $Sym_p$. Let $h \in Sym_8$ be a transposition and let $k \in Sym_8$ be a 7-cycle. If the support of $h$ is contained in the support of $k$, then the elements generate $Sym_7$. Otherwise, the support of $h$ is contained in the support of $hkh^{-1}$, and the elements $h$ and $hkh^{-1}$ generate a subgroup isomorphic to $Sym_7$. In this case, let $H = \langle h, k \rangle$. We have $[Sym_8 : H] \leq 4$, and $H \not\leq Alt_8$. But there are no subgroups of index 4 in $Sym_8$ (otherwise there would be a normal subgroup $N$ of $\mathrm{Sym}_8$ with index $4 \leq [Sym_8 : N] \leq 4! = 24$, but $Alt_8$ is the only proper normal subgroup). Therefore $H = Sym_8$. This proves part (a).

Part (b) follows since the only subgroups of index 2 are $Alt_7$ and $Alt_8$, respectively.

□

**Corollary 4.3.6.**

(a) *$A$ is isomorphic to $3 \cdot Alt_7$, $Z_3 \times Alt_7$, or $Z_3 \times Alt_8$.*

(b) *$A^+$ is isomorphic to $3 \cdot Sym_7$, $(Z_3 \times Alt_7).2$, or $(Z_3 \times Alt_8).2$.*

*Proof.* The fiber stabilizer $F$ of order 3 is centralized by the perfect group $\bar{A}$. In [20], Schur proves that the only possible extensions are those given in the statement of the Corollary. □

**Lemma 4.3.7.** *$A$ is isomorphic to $3 \cdot Alt_7$, and $A^+$ is isomorphic to $3 \cdot Sym_7$.*

*Proof.* Suppose to the contrary that $A$ is not isomorphic to $3 \cdot Alt_7$. Let $A_0 = (A^+)''$. By Corollary 4.3.6, we have $A_0 = A''$, and $A_0$ is $Alt_7$ or $Alt_8$.

We claim that $A_0$ has six orbits of length 15 on the vertices of $G'$.

Notice that $A_0 \cap F = 1$, and $A_0$ is a quotient by duality, so $A_0$ acts faithfully on the set of 15 point fibers and also the set of 15 line fibers. Consider the action on

the set of point fibers as a subgroup of $GL_4(2)$, where the point fibers are points of $PG(3,2)$.

A point of $PG(3,2)$ is a 1-dimensional subspace, so up to change of basis, the global stabilizer of a fiber in $GL_4(2) = Alt_8$ is represented by the set of invertible matrices which fix the vector $(1,0,0,0)^T$. This is the set of all invertible matrices of the form

$$\left[\begin{array}{c|ccc} 1 & x & y & z \\ \hline 0 & & & \\ 0 & & M & \\ 0 & & & \end{array}\right],$$

where $x, y, z \in GF(2)$ and $M \in GL_3(2)$. This is a split extension of $GL_3(2)$ by the elementary abelian group $2^3$, which we denote $2^3 : GL_3(2)$. This subgroup has index 15 in $A_0$.

The global fiber stabilizer in $Alt_7$ must then be a subgroup of index 8 in the group $2^3 : GL_3(2)$ above. The only possibilities are $GL_3(2)$ and $2^m : H$ where $1 \leq m \leq 3$ and $H \leq GL_3(2)$ with $[GL_3(2) : H] = 2^{3-m}$. But $GL_3(2)$ is a simple group, and if a group has a subgroup of index 4 then it has a normal subgroup of index $\leq 4! = 24$, which is a contradiction. Therefore $m = 3$.

Every subgroup of index 8 in $GL_3(2)$ must contain a 7-Sylow subgroup. Let $n_7$ be the number of 7-Sylow subgroups of $GL_3(2)$. We have $n_7|24$, $7|(n_7 - 1)$, and $n_7 \neq 1$, since that would mean the 7-Sylow subgroup is normal, contradicting the simplicity of $GL_3(2)$. Therefore $n_7 = 8$, and the normalizer of a 7-Sylow subgroup has index 8 in $GL_3(2)$. So every index 8 subgroup of $GL_3(2)$ is of the form $Z_7 : Z_3$.

So the global stabilizer of a fiber in $Alt_7$ is either $GL_3(2)$ or $2^3 : Z_7 : Z_3$. But $Alt_7$ does not contain a subgroup $2^3 : Z_7 : Z_3$, because in particular, the 2-Sylow subgroups of $Alt_7$ have order 8, and are self normalized.

So if $A_0$ is $Alt_8$ then the fiber stabilizer is $2^3 : GL_3(2)$, and if $A_0$ is $Alt_7$ then the fiber stabilizer is $GL_3(2)$. Both of these groups are perfect, so they have no abelian quotients, and therefore they have no quotient which is a subgroup of $Sym_3$. Therefore the global stabilizer of a fiber must actually be the stabilizer of each of the

three points in that fiber. Thus every point stabilizer in $A_0$ has index 15, and $A_0$ has six orbits of length 15.

These six orbits are, therefore, the same as the six orbits of length 15 of $(\mathrm{Sym}_3 \times \mathrm{Sym}_5)'' = Alt_5$ in the construction of the graph $G'$ in Proposition 4.3.2.

Let $X = (S, i)_C \in G$, where $G$ is the graph in Proposition 4.2.3. We let $x = 12, 34$ and consider the point stabilizer $H = (A_0)_{(x,1)_A}$ of $x$ in the group $A_0$. We have $[A_0 : H] = 15$, so $|H| = 168 = 7 \cdot 6 \cdot 4$. We will show that $H$ has no element of order 7, and thereby a contradiction, which will prove the Lemma.

Clearly we have $(x, 1)_B$ fixed, and in fact for any set of points from the same orbit of size 15 which is globally fixed, the corresponding set swapping $A$ for $B$ is also fixed globally.

Consider the two points at distance 3 in the Petersen line graph from $12, 34$. Call them $y$ and $z$. Then the pair of points $\{(y, 2)_B, (z, 2)_B\}$ is fixed globally, because there are edges to these points from $(x, 1)_A$. Since being at distance 3 or distance 0 is an equivalence relation in the Petersen line graph, the set $\{(x, 1)_A, (y, 1)_A, (z, 1)_A\}$ is also fixed globally, and the set $\{(x, 2)_B, (y, 2)_B, (z, 2)_B\}$ is also fixed globally. Therefore the point $(x, 2)_B$ is fixed. Repeating this argument for $(x, 2)_A$ which is a fixed point, we can see that $(x, i)_C$ is fixed for any $i = 1, 2, 3$, and any $C \in \{A, B\}$. Also, the set $\{(y, i)_C, (z, i)_C\}$ is fixed globally for any $i = 1, 2, 3$, and any $C \in \{A, B\}$.

Similarly, we know that the points at distance 1 from $x$ in each of the Petersen line graphs corresponding to the orbits of size 15 are globally fixed sets of size 4. For each $i = 1, 2, 3$, and for each $C \in \{A, B\}$, let $(X, i)_C$ denote that set of 4 points which is fixed globally in $C_i$.

For each $i = 1, 2, 3$, and for each $C \in \{A, B\}$, let $(Y, i)_C$ denote the set of points at distance 1 from $y$ in the Petersen line graph $C_i$, and $(Z, i)_C$ the set of points at distance 1 from $z$ in same. We always have $(Y, i)_C \cup (Z, i)_C$ fixed globally for each $i = 1, 2, 3$, and for each $C \in \{A, B\}$. In any case, the two indicated subsets of size 4 in this union are either each fixed globally, which happens whenever $y$ and $z$ are fixed pointwise, or they are swapped globally which happens whenever $y$ and $z$ are swapped.

Therefore, in the point stabilizer $H$, the orbits are of maximum lengths $1, 2, 4, 8$. For each group element, each of the length 8 orbits is either split into two orbits of size 4 or the two sets of size 4 in the orbit are swapped, giving only even length cycles. In any case, there cannot be a cycle of length 7, proving the Lemma. □

## 4.4 Cage graphs

**Definition 4.4.1.** *Let $f(v, g)$ be the minimum number of vertices such that a regular graph of valency $v$ and girth $g$ exists. A graph of order $f(v, g)$ with valency $v$ and girth $g$ is called a* $(v, g)$ cage.

For every $v$ and $g$, the value $f(v, g)$ has been proven to exist by Erdös and Sachs [21], but only a few cases have been completely solved.

Let $g$ be an even number $g = 2r \geq 4$ and $v \geq 3$. Then we have

$$f(v, g) \geq 2\{1 + (k-1) + (k-1)^2 + \cdots + (k-1)^{r-1}\}.$$

For any graph $G$ with valency $v$ and girth $g$, let $e = f(v, g) - |G|$. This $e$ is called the *excess* of $G$. If a graph with girth 6 has excess $e = 0$, then it is the incidence graph of a projective plane.

For an edge $\{\sigma, \tau\}$ in a graph $G$ of girth 6, let $X_{\sigma\tau}$ be the set of vertices which are at distance $\geq 3$ from both $\tau$ and $\sigma$. $X_{\sigma\tau}$ is called the excess of the edge $\{\sigma, \tau\}$. The next theorem shows that a graph with small excess is bipartite, and if it satisfies another condition on the excess of each edge, then it is the incidence graph of an elliptic semiplane.

**Theorem 4.4.2.** [2] *Let $G$ be regular with valency $k \geq 3$, girth 6, $e \leq k - 2$. Then $G$ is bipartite. Further suppose that for each edge $\{\sigma, \tau\}$ of $G$ the excess set $X_{\sigma\tau}$ induces a subgraph with just $\frac{1}{2}e$ edges. Then $G$ is a $\lambda$-fold cover of a graph representing a $\lambda$-design with $\lambda = \frac{1}{2}e + 1$, and so is an elliptic semiplane.*

In the case of excess $e = 2$, the excess $X_{\sigma\tau}$ of every edge has at most 1 edge since $X_{\sigma\tau}$ has only two vertices. So Theorem 4.4.2 applies, and shows that there must exist

a certain design with $\lambda = 2$, also known as a *biplane*, in order for the graph with excess $e = 2$ to exist. Furthermore it must have a 2-fold cover, an elliptic semiplane. In the particular case of $k = 7$, there is no biplane of the appropriate parameters, as shown in [4].

So a $(7, 6)$ cage graph has excess of at least 4. In fact, we have constructed a graph with valency 7, girth 6 and $e = 4$, by Proposition 4.2.3. A $(7, 6)$ cage graph with 90 vertices is also given by O'Keefe and Wong [18] [19], using a computer construction. Their computations further show that the $(7, 6)$ cage is unique up to isomorphism.

With a better understanding of the excess of an edge in a $(7, 6)$ graph on 90 vertices, or in general for excess $e = 4$ and valency $k$, we may be able to use Theorem 4.4.2 to show that the $(7, 6)$ cage, or perhaps a girth 6 cage with some other valency, is an elliptic semiplane without the use of a computer. Thus far, efforts in this direction have been unsuccessful.

In the previous section we gave a simple construction using the line graph of the Petersen graph. These two constructions are both 3-fold covers, that is, elliptic semiplanes, so are isomorphic by Theorem 4.2.2, which we have proven without appealing to computer results.

The computer results of O'Keefe and Wong further prove the following Theorem, which we have been unable to prove without the use of a computer.

**Theorem 4.4.3.** [18] *A* $(7, 6)$*-cage is the incidence graph of an elliptic semiplane, a* 3*-fold cover of a symmetric* 2*-*$(15, 7, 3)$ *design.*

# Bibliography

[1] Baker, R. D., *Note: an elliptic semiplane*, J. Combin. Theory (Ser. A) **25** (1978), 193–195.

[2] Biggs, N. L.; Ito, T., *Graphs with even girth and small excess*, Math. Proc. Camb. Phil. Soc. **88** (1980), 1–10.

[3] Biggs, N. L.; Ito, T., Covering graphs and symmetric designs, "Finite geometries and designs (Proc. Conf. Chelwood Gate, 1980)," 40–51, London Math. Soc. Lecture Note Ser., 49, Cambridge Univ. Press, Cambridge-New York, 1981.

[4] Cameron, P. J., *Biplanes*, Math Z. **131** (1973), 85–101.

[5] Egorychev, G. P., *The Solution of van der Waerden's Problem for Permanents*, Adv Math **42** (1981), 299–305.

[6] Falikman, D. I., *Proof of the van der Waerden Conjecture Regarding the Permanent of a Doubly Stochastic Matrix*, Math Notes **29** 1981, 475–479.

[7] Gold, R., *Maximal recursive sequences with 3-valued recursive crosscorrelation functions*, Information Theory, IEEE Transactions on **14** (1968), 154–156.

[8] Hernando, Fernando; McGuire, Gary, *Proof of a Conjecture on the Sequence of Exceptional Numbers, Classifying Cyclic Codes and APN functions.*

[9] Hartshorne, Robin, *Algbebraic Geometry*, Springer (1977).

[10] Ito, T., *On a graph of O'Keefe and Wong*, J. Graph Th. **5** (1981), 87–94.

[11] Janwa, H.; McGuire, G.; Wilson, R. M., *Double-error-correcting cyclic codes and absolutely irreducible polynomials over GF(2)*, J. Algebra **178** (1995), no. 2, 665-676.

[12] Janwa, H.; Wilson, R. M., *Hyperplane sections of Fermat varieties in P3 in char. 2 and some applications to cyclic codes*, Applied algebra, algebraic algorithms and error-correcting codes (San Juan, PR, 1993), 180-194, Lecture Notes in Comput. Sci., 673, Springer, Berlin, 1993.

[13] Kasami, T., *The weight enumerators for several classes of subcodes of the 2nd order binary Reed-Muller codes*, Information and Control **18** (1971), 369-394.

[14] Knuth, Donald E., *A Permanent Inequality*, Am Math Mon **88** (1981), 731–740.

[15] Lagarias, J. C., *The van der Waerden Conjecture: Two Soviet Solutions*, Some journal, 130–133.

[16] Minc, Henryk, *A Note on Egorycev's Proof of the van der Waerden Conjecture*, Linear Multilinear A **11** (1982), 367–371.

[17] Nandi, H., *A further note on non-isomorphic solutions of incomplete block designs*, Sankya **7** (1946), 313–316.

[18] O'Keefe, M.; Wong, P. K., *The smallest graph of girth 6 and valency 7*, J. of Graph Th. **5** (1981), 79–85.

[19] O'Keefe, M.; Wong, P. K., *On certain regular graphs of girth six*, Ars Comb. **17** (1984), 113–116.

[20] Schur, I., *Über die Darstellungen der symmetrischen und der alternierenden Gruppen durch gebrochene lineare Substitution*, J. Rein Angew. Math. **139** (1911), 155–250.

[21] Tutte, W. T., *Connectivity in Graphs*, University Toronto Press, Toronto (1966).

[22] van Lint, J. H.; Wilson, R. M., *The van der Waerden Conjecture: Two Proofs in One Year*, Math Intell **4** (1982), 72–77.

[23] van Lint, J. H., *Notes on Egoritsjev's Proof of the van der Waerden Conjecture*, Linear Algebra Appl **39** (1981), 1–8.

[24] van Lint, J. H.; Wilson, R. M., *A Course in Combinatorics, Second Edition*, Cambridge University Press (1992, 2001).

[25] Wong, P. K., *Cages—a survey*, J. of Graph Th. **6** (1982), 1–22.

[26] Zeng, J., *The generating function for the difference in even and odd three-line latin rectangles*, Ann. Sci. Math. Quebec **20/1** (1996), 105–108.