Golden-mean and Secret Sharing Matroids

Michael Welsh

VICTORIA UNIVERSITY OF WELLINGTON

Te Whare Wananga o te Upoko o te Ika a Maui

School of Mathematics, Statistics
and Operations Research

Te Kura Mātai Tatauranga, Rangahau Pūnaha

A thesis
submitted to the Victoria University of Wellington
in fulfilment of the requirements for the degree of
Master of Science
in Mathematics.

Victoria University of Wellington
2011

Abstract

Maximum-sized results are an important part of matroid theory, and results currently exist for various classes of matroids. Archer conjectured that the maximum-sized golden-mean matroids fall into three distinct classes, as opposed to the one class of all current results. We will prove a partial result that we hope will lead to a full proof.

In the second part of this thesis, we look at secret sharing matroids, with a particular emphasis on the class of group-induced p-representable matroids, as introduced by Matúš. We give new proofs for results of Matúš', relating to $M(K_4)$, F_7 and F_7^-. We show that the techniques used do not extend in some natural ways, and pose some unanswered questions relating to the structure of secret sharing matroids.

Acknowledgements

I would like to thank Dillon Mayhew for his advice and supervision. I am also grateful to Steven Archer, Rudi Pendavingh, and Geoff Whittle for various assistance given to me during this research.

I would also like to thank the matroid glut at Victoria University.

Thanks go to Joshua Baker, Chris Nimmo, and my father, Bruce Welsh, for proof-reading this thesis.

Lastly, I would like to thank my wife, Melissa.

The research done in this thesis was partially supported by a grant obtained by Dillon Mayhew.

Contents

List of Figures

Chapter 1

Introduction

A rank-r simple matroid from a class of matroids is said to be maximum-sized if none of the other rank-r simple matroids from the class have more elements than the original matroid.

The question of maximum-sized matroids is an important one in matroid theory, with many classes already classified, such as regular matroids [12], dyadic matroids [14, 16], sixth-root-of-unity matroids [21], and near-regular matroids [21].

However, maximum-sized golden-mean matroids have not yet had such a characteristion. Semple [24] and Archer [1] have made progress towards a result for low ranks, while Archer has conjectured the complete characterisation.

Conjecture 1.0.1 (Archer, 2005)**.** *Let M be a maximum-sized golden-mean matroid. If $r(M) = 3$ then $M \cong B_{11}$, otherwise M is isomorphic to one of*

$GI_{r(M)}$, $GP_{r(M)}$ *or* $T^2_{r(M)}$.

We will not prove this conjecture in this thesis. However, we will prove a weaker result.

Theorem 1.0.2. *Let M be a simple rank-r golden-mean matroid with no $F_7^=$ or $S_{10}\backslash f$ minor. Then*

$$|E(M)| \leq \binom{r+3}{2} - 5.$$

Furthermore, equality in this bound is attained if and only if $M \cong T^2_r$.

The work in Part I of this thesis is original, with guidance from Dillon Mayhew. The techniques used were developed by Oxley, Vertigan and Whittle in [21]. No non-original proofs are given, and credit is given for such results as they appear.

Part II of this thesis deals with secret sharing matroids. Secret sharing schemes were independently introduced by Blakley [3] and Shamir [30]. A secret sharing matroid captures the essence of an ideal secret sharing scheme, and, as such, is of interest to various groups of people, including matroid theorists and information theorists.

Almost nothing is known about the structure of secret sharing matroids, and we will give new proofs of a few results by Matúš [19] in this area.

As such, there is little original work in this part of the thesis. Theorem 5.1.4 can be found in [6]. All results from Sections 5.1.2, 5.2, and 5.3 are originally

by Matúš [19]. However, new proofs are given here. The work in Section 5.4 is all original. As in Part I, credit is given where old results are used.

The reader is referred to *Matroid Theory* by Oxley [20] for an introduction to the fundamental concepts in matroid theory. All undefined notation in this thesis will follow [20].

The following definition formalises various intuitive concepts arising from geometry, that will be used throughout this thesis.

Definition 1.0.3. A ***point*** of a matroid is a rank one flat. A ***line*** of a matroid is a rank two flat. A ***long line*** of a matroid is a rank two flat that contains at least three points. A ***very long line*** of a matroid is a rank two flat that contains at least four points. The ***length*** of a line is the number of points on the line.

Part I

Golden-mean Matroids

Chapter 2

Introduction

Partial fields were introduced by Semple and Whittle [27]. However, we will follow the treatment of Van Zwam [34], starting from a ring.

Definition 2.0.4 (Van Zwam [34])**.** A ***partial field*** is a pair (R, G), where R is a commutative ring, and G is a subgroup of the group of units of R such that $-1 \in G$.

If $\mathbb{P} = (R, G)$ is a partial field, and $p \in R$, then we say that p is an ***element*** of $\mathbb{P}$, denoted $p \in \mathbb{P}$, if $p = 0$ or $p \in G$. Note that if $p, q \in \mathbb{P}$ then $pq \in \mathbb{P}$, but $p + q$ need not be an element of $\mathbb{P}$.

Example 2.0.5. Consider the partial field $\mathbb{U}_0 = (\mathbb{Z}, \{-1, 1\})$, known as the ***regular*** partial field. Then $1 \cdot 1 \in \{-1, 1\}$, but $1 + 1 \notin \{-1, 1\}$. $\Diamond$

Definition 2.0.6. A matroid M is said to be ***representable over the partial field*** $\mathbb{P}$ if there is a matrix $\mathfrak{M}$ such that all non-zero subdeterminants

of $\mathfrak{M}$ are in $\mathbb{P}$ and a labelling of the columns of $\mathfrak{M}$ by $E(M)$ such that any subset $\{x_1, \ldots, x_k\}$ is independent in M if and only if the submatrix $[x_1, \ldots, x_k]$ contains a $k \times k$ subdeterminant that is non-zero in $\mathbb{P}$. We say that $\mathfrak{M}$ is a $\mathbb{P}$-***matrix***, and that M is a $\mathbb{P}$-***matroid***.

We are interested in characterising the maximum-sized matroids for classes of matroids representable over partial fields.

Definition 2.0.7 (Kung [15])**.** Let $\mathcal{M}$ be a collection of matroids. A member M of $\mathcal{M}$ is ***extremal in*** $\mathcal{M}$ if M is simple and there is no single element simple extension of M that has the same rank as M and is isomorphic to a member of $\mathcal{M}$.

A member M of $\mathcal{M}$ is ***maximum-sized in*** $\mathcal{M}$ if M is simple and every rank-$r(M)$ simple matroid in $\mathcal{M}$ has a groundset that is no larger than the groundset of M.

Characterisations of the maximum-sized matroids representable over various partial fields are already known.

Recall the regular partial field $\mathbb{U}_0$ from Example 2.0.5. The next theorem follows from work done by Heller [12].

Theorem 2.0.8. *Let M be a simple rank-r regular matroid. Then*

$$|E(M)| \leq \binom{r+1}{2}.$$

Furthermore, equality in this bound is attained if and only if $M \cong M(K_{r+1})$.

□

Definition 2.0.9 (Kung and Oxley [16], Section 6.10 of Oxley [20])**.** Let $\{\omega_1, \ldots, \omega_n\}$ be a basis of an n-dimensional vector space over $GF(3)$. The ***ternary Dowling geometry*** $Q_n(GF(3)^*)$ is the ternary geometry of rank n consisting of the points $\omega_1, \ldots, \omega_n$ and the points $\omega_i - \omega_j$ and $\omega_i + \omega_j$, where $i < j$.

The ***dyadic*** partial field is $\mathbb{D} = (\mathbb{Q}, \langle -1, 2 \rangle)$. The next theorem follows from work done by Kung [14] and Kung and Oxley [16].

Theorem 2.0.10. *Let* M *be a simple rank-*r *dyadic matroid. Then*

$$|E(M)| \leq r^2.$$

Furthermore, equality in this bound is attained if and only if $M \cong Q_r(GF(3)^*)$. □

The ***near-regular*** partial field is $\mathbb{U}_1 = (\mathbb{C}(\xi), \langle -1, \xi, 1 - \xi \rangle)$, where ξ is a transcendental. The ***sixth-roots-of-unity*** ($\sqrt[6]{1}$) partial field is $\mathbb{S} = (\mathbb{C}, \langle \zeta \rangle)$, where ζ is a root of $x^2 - x + 1$. Maximum-sized characterisations for both near-regular and $\sqrt[6]{1}$ matroids were provided by Oxley, Vertigan, and Whittle [21], using the following two results. The matroid T_r is obtained by adding a point freely on a three point line of $M(K_{r+2})$, contracting that point, and simplifying the resulting matroid.

Theorem 2.0.11. *Let M be a simple rank-r $\sqrt[6]{1}$-matroid. Then*

$$|E(M)| \leq \begin{cases} \binom{r+2}{2} - 2 & \text{if } r \neq 3; \\ 9 & \text{if } r = 3. \end{cases}$$

Moreover, equality is attained in this bound if and only if $M \cong T_r$, when $r \neq 3$, or $M \cong AG(2,3)$ when $r = 3$. □

Corollary 2.0.12. *Let M be a simple rank-r near-regular matroid. Then*

$$|E(M)| \leq \binom{r+2}{2} - 2.$$

Moreover, equality is attained in this bound if and only if $M \cong T_r$. □

There are an infinite number of maximum-sized characterisations for classes of matroids, as the maximum-sized rank-r matroid representable over the field $GF(q)$ is the projective geometry $PG(r-1, q)$.

2.1 Maximum-sized Golden-mean Matroids

Definition 2.1.1. The golden-mean partial field, denoted $\mathbb{G}$, is $(\mathbb{R}, \langle -1, \phi \rangle)$, where ϕ is the positive root of $x^2 - x - 1$. A matroid is ***golden-mean*** if it has a $\mathbb{G}$-representation.

The following theorem is an unpublished result of Vertigan. In his masters thesis, Semple [24] proved that (ii) implies (iii). For a proof, see Pendavingh

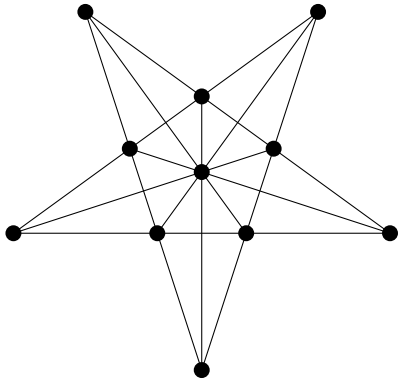

Figure 2.1: The Betsy Ross

and Van Zwam [22, Theorem 1.3].

Theorem 2.1.2. *Let M be a matroid. The following are equivalent:*

(i) M is representable over both $GF(4)$ and $GF(5)$;

(ii) M is golden-mean;

(iii) M is representable over $GF(p)$ for all primes p such that $p = 5$ or $p \equiv \pm 1 \bmod 5$, and also over $GF(p^2)$ for all primes p. □

The Betsy Ross matroid, or B_{11}, was introduced by Brylawski and Kelly [5]. It was shown by Semple [24] that B_{11} is an extremal rank-three golden-mean matroid. Using computer software, Archer [1] was able to show that B_{11} is the unique maximum-sized rank-three golden-mean matroid.

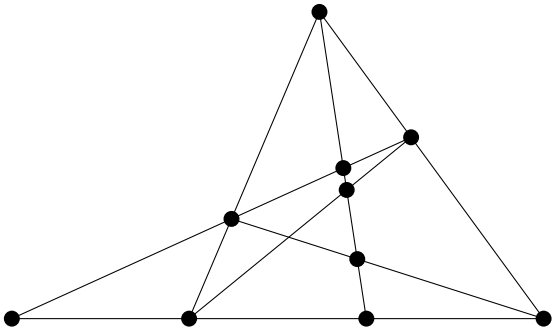

Figure 2.2: GI_3

A geometric representation for B_{11} is given in Figure 2.1. It has the following $\mathbb{G}$ representation.

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

The GI_r family of matroids was introduced by Archer in his PhD thesis [1]. A geometric representation of GI_3 is shown in Figure 2.2.

Let D_m denote the $m \times \binom{m}{2}$ matrix whose columns consist of all m-tuples with two non-zero entries, with the first being 1 and the second being -1. Let 0_m^n denote the $n \times m$ matrix consisting entirely of zeroes. Let I_m^0 denote the $m \times (m+1)$ matrix $[I_m|\mathbf{0}]$. Let $k = r - 2$. Then the GI matroid of rank

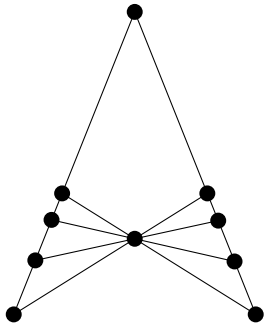

Figure 2.3: T_3^2

r, for $r > 2$, denoted GI_r, is defined by the following matrix.

$$\left[\begin{array}{c|c|c|c|c|c|c} -\phi\ -\phi\ -\phi & 0\cdots 0 & \phi\cdots\phi & 1\cdots 1 & 0\cdots 0 & 0\cdots 0 & 0\cdots 0 \\ 1\quad \phi\quad \phi^2 & 0\cdots 0 & 0\cdots 0 & 0\cdots 0 & \phi\cdots\phi & 1\cdots 1 & 0\cdots 0 \\ \hline 0_3^k & I_k & I_k & I_k^0 & I_k & I_k^0 & D_k \end{array}\right].$$

The T_r^k family of matroids was introduced by Semple in his PhD thesis [25]. We are only interested in the T_r^2 family, a representation of which is given below. A geometric representation of T_3^2 is given in Figure 2.3.

$$\left[\begin{array}{c|ccc|ccc|ccc|ccc|ccc} 1 & 0 & \cdots & 0 & 1 & \cdots & 1 & \phi & \cdots & \phi & \phi^2 & \cdots & \phi^2 & 0 & \cdots & 0 \\ \hline 0 & & & & & & & & & & & & & & & \\ \vdots & \multicolumn{3}{c|}{I_{n-1}} & \multicolumn{3}{c|}{I_{n-1}} & \multicolumn{3}{c|}{I_{n-1}} & \multicolumn{3}{c|}{I_{n-1}} & \multicolumn{3}{c}{D_{n-1}} \\ 0 & & & & & & & & & & & & & & & \end{array}\right].$$

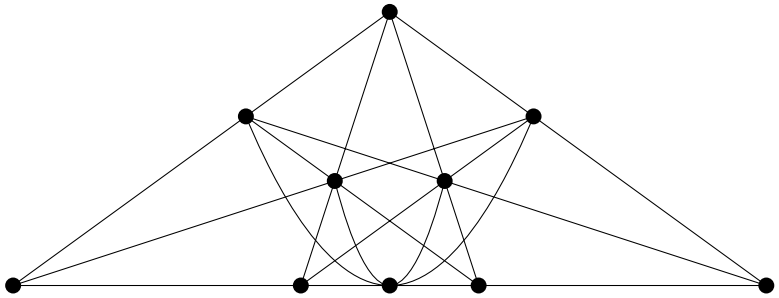

Figure 2.4: GP_3

As we will be interested in the T_r^2 family of matroids later, note that all five-point lines in T_r^2 pass through a common point, and there are $r-1$ such lines. Also, note that the number of elements in T_r^2 is

$$\left|E(T_r^2)\right| = \binom{r+3}{2} - 5.$$

The GP_r family of matroids was introduced by Archer in his PhD thesis [1]. Note that the matrix given here is different from one that was introduced by Archer, as the original matrix has errors. This altered matrix is due to Archer (private correspondence).

First of all, $GP_1 \cong GP_2 \cong U_{2,5}$. Recall that $k = r - 2$. Then GP_r is represented by the following matrix. A geometric representation of GP_3 is

given in Figure 2.4.

$$\left[\begin{array}{c|c|c|c|c|c} \begin{matrix} 0 \cdots 0 & -1 \\ 0 \cdots 0 & \phi \end{matrix} & \begin{matrix} 1 \cdots 1 \\ 0 \cdots 0 \end{matrix} & \begin{matrix} 0 \cdots 0 \\ \phi \cdots \phi \end{matrix} & \begin{matrix} \phi \cdots \phi \\ \phi \cdots \phi \end{matrix} & \begin{matrix} 1 \cdots 1 \\ \phi^2 \cdots \phi^2 \end{matrix} & \begin{matrix} 0 \cdots 0 \\ 0 \cdots 0 \end{matrix} \\ \hline I_k^0 & I_k^0 & I_k^0 & I_k^0 & I_k^0 & D_k \end{array}\right]$$

In his PhD thesis, Archer [1] put forward the following conjecture.

Conjecture 2.1.3 (Archer, 2005)**.** *Let M be a maximum-sized golden-mean matroid. If $r(M) = 3$ then $M \cong B_{11}$, otherwise M is isomorphic to one of $GI_{r(M)}$, $GP_{r(M)}$ or $T^2_{r(M)}$.*

This conjecture is as yet unsolved. However, we will prove a weaker result.

Chapter 3

Results

Let $F_7^=$ be the matroid represented over $\mathbb{G}$ by the matrix below. A geometric representation is shown in Figure 3.1. It is obtained by relaxing a circuit-hyperplane of the non-Fano.

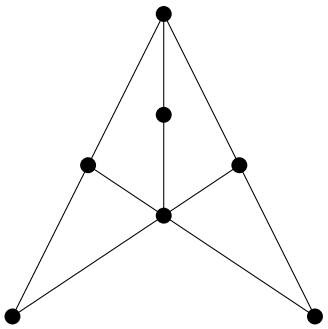

Figure 3.1: $F_7^=$

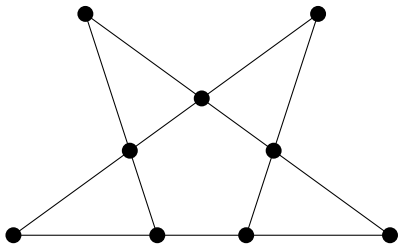

Figure 3.2: $S_{10}\backslash f$

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

$S_{10}\backslash f$ is the matroid obtained by deleting the unique point on multiple three point lines and any other point from the Betsy Ross. A geometric representation is shown in Figure 3.2. We will only consider matroids that have no $F_7^=$ or $S_{10}\backslash f$ minor.

The main theorem that will be proved is the following.

Theorem 3.0.4. *Let M be a simple rank-r golden-mean matroid with no $F_7^=$ or $S_{10}\backslash f$ minor. Then*

$$|E(M)| \leq \binom{r+3}{2} - 5.$$

Furthermore, equality in this bound is attained if and only if $M \cong T_r^2$.

We will prove this theorem inductively, using techniques found in Oxley, Vertigan and Whittle [21].

Firstly, we need to show that T_r^2 is in fact golden-mean. Note that this result also follows from work by Semple [26].

Lemma 3.0.5. *For all $r \geq 2$, T_r^2 is a golden-mean matroid.*

Proof. We will argue by induction on r. By definition, T_2^2 is $U_{2,5}$, which, by page 640 of Oxley [20], is representable over all fields of size greater than or equal to four. In particular, it is representable over $GF(4)$ and $GF(5)$, and so by Theorem 2.1.2, is golden-mean.

Recall that T_r^2 is represented over $\mathbb{G}$ by the following matrix.

$$\mathfrak{T}_r = \left[\begin{array}{c|ccc|ccc|ccc|ccc|ccc} 1 & 0 & \cdots & 0 & 1 & \cdots & 1 & \phi & \cdots & \phi & \phi^2 & \cdots & \phi^2 & 0 & \cdots & 0 \\ \hline 0 & & & & & & & & & & & & & & & \\ \vdots & & I_{r-1} & & & I_{r-1} & & & I_{r-1} & & & I_{r-1} & & & D_{r-1} & \\ 0 & & & & & & & & & & & & & & & \end{array}\right]$$

In order to show that $\mathfrak{T}_r$ is a $\mathbb{G}$-matrix, we need to show that every non-zero subdeterminant of $\mathfrak{T}_r$ falls into the set $\{\pm\phi^i \mid i \in \mathbb{Z}\}$. Now assume that $r > 2$ and that $\mathfrak{T}_{r-k}$ is a $\mathbb{G}$-matrix for all $k \in \{1, \ldots, r-2\}$. Let X be an $n \times n$ submatrix of $\mathfrak{T}_r$. Since the matrix $[I_{r-1}|D_{r-1}]$ is a totally unimodular matrix representation of $M(K_r)$, we may assume that X meets row 1 of $\mathfrak{T}_r$. Furthermore, if X avoids some row of $\mathfrak{T}_r$, then either X has two columns such that one is a scalar multiple of the other, or X can be obtained from a submatrix of $\mathfrak{T}_{r-1}$ by multiplying some columns by -1, ϕ, or ϕ^2. In either case, we can deduce that $\det(X)$ is in the desired set. Hence we can assume

that $n = r$.

Now assume that X has a row with at most one non-zero entry. Then $\det(X)$ is obtained by multiplying the determinant of a submatrix of $\mathfrak{T}_{r-1}$ by some member of $\{0, 1, -1, \phi, -\phi, \phi^2, -\phi^2\}$. Thus $\det(X)$ is in the desired set. Therefore we may assume that every row of X has at most two non-zero entries. However, by inspection, we can see that every column of X has at most two non-zero entries. Thus X has exactly $2n$ non-zero entries, two per row and two per column. Then, after permuting some rows and columns and multiplying some rows or columns by -1, we can get the matrix

$$\begin{bmatrix} x & 0 & 0 & & 0 & y \\ 1 & 1 & 0 & & 0 & 0 \\ 0 & -1 & 1 & & 0 & 0 \\ 0 & 0 & -1 & & 0 & 0 \\ & & & \ddots & & \\ 0 & 0 & 0 & & 1 & 0 \\ 0 & 0 & 0 & & -1 & 1 \end{bmatrix},$$

where $x \in \{1, \phi, \phi^2\}$ and $y \in \{\phi, \phi^2\}$. The determinant of this matrix is $x + (-1)^{1+n} y (-1)^{n-2}$, that is $x - y$. For all six possible values of x and y, the set $\{\pm\phi^i \mid i \in \mathbb{Z}\}$contains $x - y$, and so $\det(X)$ is in the desired set.

Therefore, by induction, $\mathfrak{T}_r$ is a $\mathbb{G}$-matrix and therefore T_r^2 is a golden-mean matroid. $\square$

We also need to show that T_r^2 has no $F_7^=$ or $S_{10}\backslash f$ minor.

Lemma 3.0.6. *For all $r \geq 3$, T_r^2 has no $F_7^=$ or $S_{10}\backslash f$ minor.*

Proof. We will prove this lemma by induction on r. The base case, when $r = 3$, follows immediately from Lemma 3.1.1. Recall that T_r^2 is represented over $\mathbb{G}$ by the following matrix.

$$\left[\begin{array}{c|ccc|ccc|ccc|ccc|ccc} 1 & 0 & \cdots & 0 & 1 & \cdots & 1 & \phi & \cdots & \phi & \phi^2 & \cdots & \phi^2 & 0 & \cdots & 0 \\ \hline 0 & & & & & & & & & & & & & & & \\ \vdots & & I_{r-1} & & & I_{r-1} & & & I_{r-1} & & & I_{r-1} & & & D_{r-1} & \\ 0 & & & & & & & & & & & & & & & \end{array}\right]$$

When we contract the first element of this matrix, $\begin{bmatrix} 1 & 0 & \dots & 0 \end{bmatrix}^T$, after simplifying we get the following matrix

$$\left[\begin{array}{c|c} I_{r-1} & D_{r-1} \end{array}\right].$$

This is the matrix for $M(K_r)$, and is therefore regular. As neither $F_7^=$ nor $S_{10}\backslash f$ is regular, this contraction does not give a $F_7^=$ or $S_{10}\backslash f$ minor.

When we contract any other element from the standard basis of this matrix,

we get the following matrix upon simplification

$$\left[\begin{array}{c|ccc|ccc|ccc|ccc|ccc} 1 & 0 & \cdots & 0 & 1 & \cdots & 1 & \phi & \cdots & \phi & \phi^2 & \cdots & \phi^2 & 0 & \cdots & 0 \\ \hline 0 & & & & & & & & & & & & & & & \\ \vdots & & I_{r-2} & & & I_{r-2} & & & I_{r-2} & & & I_{r-2} & & & D_{r-2} & \\ 0 & & & & & & & & & & & & & & & \end{array}\right].$$

This is isomorphic to T^2_{r-1}, which has no $F_7^=$ or $S_{10}\backslash f$ minor by induction.

Likewise, when we contract any element from the identity submatrices headed by 1, ϕ, and ϕ^2, we get a matrix equivalent to the following upon simplification

$$\left[\begin{array}{c|ccc|ccc|ccc|ccc|ccc} 1 & 0 & \cdots & 0 & 1 & \cdots & 1 & \phi & \cdots & \phi & \phi^2 & \cdots & \phi^2 & 0 & \cdots & 0 \\ \hline 0 & & & & & & & & & & & & & & & \\ \vdots & & I_{r-2} & & & I_{r-2} & & & I_{r-2} & & & I_{r-2} & & & D_{r-2} & \\ 0 & & & & & & & & & & & & & & & \end{array}\right].$$

This is isomorphic to T^2_{r-1}, which has no $F_7^=$ or $S_{10}\backslash f$ minor by induction.

Finally, when we contract any point from the D_{r-1} section, we also get a matrix equivalent to the following upon simplification

$$\left[\begin{array}{c|ccc|ccc|ccc|ccc|ccc} 1 & 0 & \cdots & 0 & 1 & \cdots & 1 & \phi & \cdots & \phi & \phi^2 & \cdots & \phi^2 & 0 & \cdots & 0 \\ \hline 0 & & & & & & & & & & & & & & & \\ \vdots & & I_{r-2} & & & I_{r-2} & & & I_{r-2} & & & I_{r-2} & & & D_{r-2} & \\ 0 & & & & & & & & & & & & & & & \end{array}\right].$$

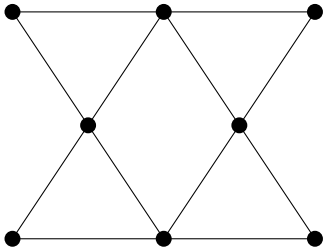

Figure 3.3: $P\backslash c$

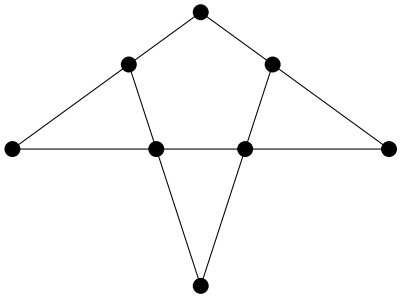

Figure 3.4: IK

This is isomorphic to T^2_{r-1}, which has no $F_7^=$ or $S_{10}\backslash f$ minor by induction.

Therefore, no matter what point in T^2_r we contract, we do not get a $F_7^=$ or $S_{10}\backslash f$ minor. Hence T^2_r has no $F_7^=$ or $S_{10}\backslash f$ minor. $\square$

3.1 Lemmata used in the proof of Theorem 3.0.4

3.1.1 Computer Result

In order to get a base case for our induction, we need to know what all the rank-three golden-mean matroids with no $F_7^=$ or $S_{10}\backslash f$ minor are. To that end, we use a computer search, utilising Sage [32] and Mathematica [36]. This result was independently verified by a different computer search undertaken by Pendavingh (private correspondence).

Lemma 3.1.1. *The extremal rank-three golden-mean matroids with no $F_7^=$ or $S_{10}\backslash f$ minor are as follows:*

- T_3^2 *(Figure* 2.3*)*
- $P\backslash c$ *(Figure* 3.3*)*
- IK *(Figure* 3.4*)*

Proof Sketch. The code used is in Appendix A, along with discussion on how it functions.

When the code is run, a list of 3588 rank-three $\mathbb{G}$-matrices is output. As isomorphism testing was not implemented, a large amount of pencil-and-paper calculation is required to gain the desired result. Firstly, one must remove all matroids that contain $F_7^=$ or $S_{10}\backslash f$ as a restriction. Then, starting from

the largest matrix still remaining in the list, check to see if it is isomorphic to a matroid in the list of extremal matroids. If it is, remove it, and all restrictions of it, from the list of possible matroids. If it is not, add it to the list of extremal matroids and remove it, and all restrictions of it, from the list of possible matroids. Repeat this process until there are no matroids left on the list of possible matroids. Once this stage has been reached, the list of extremal matroids is complete, and the desired result follows. □

3.1.2 Spikes

Definition 3.1.2 (Ding et al. [7])**.** For $n \geq 3$, a simple matroid M is an ***n-spike with tip t*** if it satisfies the following properties.

(i) the ground set is the union of n lines, $L_1, \ldots, L_n$, all having three points and passing through a common point t;

(ii) for all k in $\{1, 2, \ldots, n-1\}$, the union of any k of $L_1, \ldots, L_n$ has rank $k+1$; and

(iii) $r(L_1 \cup \cdots \cup L_n) = n$.

We will refer to an n-spike with tip t as an ***n-spike***.

We need to completely characterise the 4-spikes representable over $GF(4)$. To that end, we use the following result.

Theorem 3.1.3 (Wu, Theorem 1.2 [37])**.** *For each integer $n \geq 3$, the number of distinct quaternary n-spikes is $\lfloor (n^2 + 6n + 24)/12 \rfloor$.* □

Corollary 3.1.4. *There are exactly five distinct quaternary 4-spikes.* □

Let S be an n-spike with tip t representable over a field $\mathbb{F}$. If we choose a basis $\{1, \ldots, n\}$ containing exactly one element from each of the lines L_i, then S can be represented in the form

$$\left[\begin{array}{cccccc|cccccc} 1 & 2 & 3 & \cdots & n & t & & & & & & \\ 1 & 0 & 0 & \cdots & 0 & 1 & 1+x_1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & 0 & \cdots & 0 & 1 & 1 & 1+x_2 & 1 & \cdots & 1 \\ 0 & 0 & 1 & \cdots & 0 & 1 & 1 & 1 & 1+x_3 & \cdots & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 1 & 1 & 1 & 1 & \cdots & 1+x_n \end{array}\right]$$

where $x_1, \ldots, x_n$ are non-zero elements of $\mathbb{F}$.

Lemma 3.1.5. *All 4-spikes representable over $GF(4)$ either have $F_7^=$ as a minor or are not representable over $GF(5)$.*

Proof. We will treat each spike separately. Note that $GF(4)$ consists of the elements $\{0, 1, \alpha, \alpha^2\}$, where $\alpha^2 = \alpha + 1$.

Sublemma 3.1.5.1. *The matroid S_1, as represented over $GF(4)$ by the ma-*

trix below, is not representable over $GF(5)$.

$$\begin{array}{c} \begin{array}{ccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{array} \\ \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \end{bmatrix} \end{array}$$

Subproof. Contract any point (except for the point represented by $\begin{bmatrix} 1 & 1 & 1 & 1 \end{bmatrix}^T$) and simplify the resultant matroid. It is not too hard to see that this gives the Fano matroid. It is well known (page 643 of Oxley [20] for instance) that the Fano matroid is only representable over fields of characteristic 2, so S_1 cannot be $GF(5)$ representable. □

Sublemma 3.1.5.2. *The matroid* S_2*, as represented over* $GF(4)$ *by the matrix below, is not representable over* $GF(5)$.

$$\begin{array}{c} \begin{array}{ccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{array} \\ \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & \alpha^2 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & \alpha^2 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & \alpha^2 \end{bmatrix} \end{array}$$

Subproof. Contract the point represented by $\begin{bmatrix} 0 & 1 & 1 & 1 \end{bmatrix}^T$ and simplify the resultant matroid. It is not too hard to see that this gives the Fano matroid,

so S_2 cannot be $GF(5)$ representable. □

Sublemma 3.1.5.3. *The matroid S_3, as represented over $GF(4)$ by the matrix below, has $F_7^=$ as a minor.*

$$\begin{array}{c} \begin{array}{ccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{array} \\ \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & \alpha^2 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & \alpha \end{bmatrix} \end{array}$$

Subproof. Contract the point represented by $\begin{bmatrix} 1 & 1 & \alpha^2 & 1 \end{bmatrix}^T$ and simplify the resultant matroid. It is not too hard to see that this gives $F_7^=$. □

Sublemma 3.1.5.4. *The matroid S_4, as represented over $GF(4)$ by the matrix below, has $F_7^=$ as a minor.*

$$\begin{array}{c} \begin{array}{ccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{array} \\ \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & \alpha & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & \alpha \end{bmatrix} \end{array}$$

Subproof. Contract the point represented by $\begin{bmatrix} 0 & 0 & 1 & 0 \end{bmatrix}^T$ and simplify the resultant matroid. It is not too hard to see that this gives $F_7^=$. □

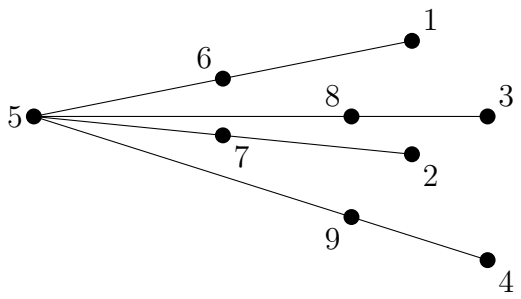

Figure 3.5: Illustration of S_5

Sublemma 3.1.5.5. *The matroid S_5, as represented over $GF(4)$ by the matrix below, is not representable over $GF(5)$.*

$$\begin{array}{c} \begin{array}{ccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{array} \\ \left[\begin{array}{ccccccccc} 1 & 0 & 0 & 0 & 1 & \alpha & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & \alpha & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & \alpha & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & \alpha \end{array}\right] \end{array}$$

Subproof. A geometric representation of S_5 is given in Figure 3.5. We can see that S_5 is the free spike of rank four. As such, it follows from [11, Lemma 11.6] that S_5 is not $GF(5)$-representable. □

Sublemma 3.1.5.6. *S_1, S_2, S_3, S_4, and S_5 are all distinct.*

Subproof. S_1 has eight 4-element circuit-hyperplanes. They are $\{1,2,3,9\}$, $\{1,2,4,8\}$, $\{1,3,4,7\}$, $\{1,7,8,9\}$, $\{2,3,4,6\}$, $\{2,6,8,9\}$, $\{3,6,7,9\}$, and $\{4,6,7,8\}$. S_2 has four 4-element circuit-hyperplanes, with one element, 6, on all four of them. Therefore $S_1 \ncong S_2$. S_3 and S_4 both have four 4-element

circuit-hyperplanes, but neither of them have an element on four 4-element circuit hyperplanes. Therefore $S_2 \ncong S_3$, $S_2 \ncong S_4$, $S_1 \ncong S_3$, and $S_1 \ncong S_4$. S_4 also has the property that picking a non-tip element and looking at the 4-element circuit hyperplanes that it is in, there is a different non-tip element of S_4 that is in the same 4-element circuit hyperplanes. S_3 does not have this property. Therefore $S_3 \ncong S_4$. Finally, S_5 has no 4-element circuit hyperplanes. Therefore $S_5 \ncong S_i$, for $i \in \{1, 2, 3, 4\}$. □

Because of Corollary 3.1.4, we know that there are exactly five distinct quaternary 4-spikes. Sublemma 3.1.5.6 shows that we indeed have five distinct quaternary 4-spikes. The five sublemmata 3.1.5.1 – 3.1.5.5 show that all of them either have a $F_7^=$ minor or are not representable over $GF(5)$. □

Corollary 3.1.6. *There are no golden-mean 4-spikes with no $F_7^=$ or $S_{10}\backslash f$ minor.* □

3.2 Proof of Theorem 3.0.4

The remainder of this part of the thesis will be dedicated to the proof of Theorem 3.0.4.

Recall that Theorem 3.0.4 is

Theorem 3.0.4. *Let M be a simple rank-r golden-mean matroid with no*

$F_7^=$ or $S_{10}\backslash f$ minor. Then

$$|E(M)| \leq \binom{r+3}{2} - 5.$$

Furthermore, equality in this bound is attained if and only if $M \cong T_r^2$.

Proof. We will use induction on r. We will simultaneously prove the bound and the characterisation of the matroids that attain equality in this bound. For $r < 3$, the result is trivial. The case when $r = 3$ follows from Lemma 3.1.1.

So let M be a rank-r maximum-sized golden-mean matroid with no $F_7^=$ or $S_{10}\backslash f$ minor, where $r \geq 4$. Then

$$|E(M)| \geq \left|E(T_r^2)\right| = \binom{r+3}{2} - 5. \tag{3.2.0.1}$$

3.2.1 Connectivity

Definition 3.2.1. Let $M = (E, r)$ be a matroid and let $k > 1$ be an integer. A ***k-separation*** of M is a partition (X, Y) of E with the property that $|X|, |Y| \geq k$, and $r(X) + r(Y) - r(M) < k$. The separation is an ***exact k-separation*** if $r(X) + r(Y) - r(M) = k - 1$. If M has no n-separations for all $n \leq k$, then M is ***(k+1)-connected***.

This result of Seymour is used in the proofs of various lemmata.

Lemma 3.2.2 (Seymour, Theorem 3.1 [28])**.** *If x, y are elements of a non-*

binary 3-connected matroid M, then M has a $U_{2,4}$ minor using both x and y.

□

Lemma 3.2.3. *Let M be a rank-r maximum-sized golden-mean matroid with no $F_7^=$ or $S_{10}\backslash f$ minor. Then M is 2-connected.*

Proof. Assume that M is not 2-connected. Then there exists an exact 1-separation (X_1, X_2) of M. Let $r(X_i) = r_i$. As X_i is simple and golden-mean, by the induction hypothesis, X_i can be no larger than $T^2_{r_i}$. Hence $|X_i| \leq \binom{r_i+3}{2} - 5$, for $i \in \{1, 2\}$. So

$$\begin{aligned} |E(M)| &= |X_1| + |X_2| \\ |E(M)| &\leq \binom{r_1+3}{2} + \binom{r_2+3}{2} - 10 \\ &= \frac{1}{2}\left(r_1^2 + r_2^2 + 5r_1 + 5r_2 - 8\right). \end{aligned} \tag{3.2.3.1}$$

As M is maximum-sized of rank r, it must be at least as big as T^2_r. Hence

$$\begin{aligned} |E(M)| &\geq \binom{r+3}{2} - 5 \\ &= \binom{r_1+r_2+3}{2} - 5 \\ &= \frac{1}{2}\left(r_1^2 + r_2^2 + 5r_1 + 5r_2 + 2r_1r_2 - 4\right). \end{aligned} \tag{3.2.3.2}$$

Combining (3.2.3.1) and (3.2.3.2), we get

$$\frac{1}{2}\left(r_1^2 + r_2^2 + 5r_1 + 5r_2 - 8\right) \geq \frac{1}{2}\left(r_1^2 + r_2^2 + 5r_1 + 5r_2 + 2r_1r_2 - 4\right)$$
$$-8 \geq 2r_1r_2 - 4.$$

As both r_1 and r_2 are positive, this is a contradiction. Therefore M is 2-connected. □

Lemma 3.2.4. *Let M be a rank-r maximum-sized golden-mean matroid with no $F_7^=$ or $S_{10}\backslash f$ minor. Then M is 3-connected.*

Proof. Assume that M is not 3-connected. By Lemma 3.2.3, M is 2-connected, so there are no exact 1-separations. Hence there exists an exact 2-separation (X_1, X_2) of M. Let $r(X_i) = r_i$. As $M|X_i$ is simple and golden-mean, then, by the induction hypothesis, X_i can be no larger than $T^2_{r_i}$. Hence $|X_i| \leq \binom{r_i+3}{2} - 5$, for $i \in \{1, 2\}$. So

$$\begin{aligned} |E(M)| &= |X_1| + |X_2| \\ &\leq \binom{r_1+3}{2} + \binom{r_2+3}{2} - 10 \\ &= \frac{1}{2}\left(r_1^2 + r_2^2 + 5r_1 + 5r_2 - 8\right). \end{aligned} \tag{3.2.4.1}$$

As M is maximum-sized of rank r, it must be at least as big as T^2_r. Hence

$$\begin{aligned} |E(M)| &\geq \binom{r+3}{2} - 5 \\ &= \binom{(r_1 + r_2 - 1) + 3}{2} - 5 \\ &= \frac{1}{2}\left(r_1^2 + r_2^2 + 3r_1 + 3r_2 + 2r_1r_2 - 8\right). \end{aligned} \tag{3.2.4.2}$$

Combining (3.2.4.1) and (3.2.4.2), we get

$$\begin{aligned} \frac{1}{2}\left(r_1^2 + r_2^2 + 5r_1 + 5r_2 - 8\right) &\geq \frac{1}{2}\left(r_1^2 + r_2^2 + 3r_1 + 3r_2 + 2r_1r_2 - 8\right) \\ 2r_1 + 2r_2 &\geq 2r_1r_2 \\ r_1 + r_2 &\geq r_1r_2 \end{aligned}$$

If $r_i = 1$, then M contains a parallel class, and is therefore not simple, contradicting the definition of M.

Hence $r_1 = r_2 = 2$. Then $r(M) = 3$, so, as M is maximum-sized, by Lemma 3.1.1, M is isomorphic to T_r^2. In this case, it is easy to see that M is 3-connected, a contradiction.

Therefore M is 3-connected. □

Definition 3.2.5. Let M be a 3-connected matroid. If every 3-separation (X, Y) of M has the property that $\min\{r(X), r(Y)\} \leq 2$, then M is ***vertically 4-connected***.

The following result is well known. A proof is given here for completeness.

Lemma 3.2.6. *Let M be a vertically 4-connected matroid, and let $e \in E(M)$ be an element of M. Then* $\mathrm{si}(M/e)$ *is 3-connected.*

Proof. Firstly, we will show that $\mathrm{si}(M/e)$ is 2-connected.

Sublemma 3.2.6.1. *The matroid* $\mathrm{si}(M/e)$ *is 2-connected.*

Subproof. Assume that $\mathrm{si}(M/e)$ is not 2-connected. Then there exists a 1-separation, (X_1'', X_2'') of $\mathrm{si}(M/e)$. This induces a 1-separation, (X_1', X_2') of M/e. We now consider what happens to this partition in M. Let (X_1, X_2) be this partition in M. Without loss of generality, we can assume that $e \in X_1$. Then $r_M(X_1) - r_{M/e}(X_1) = 1$, and $r_M(X_2) - r_{M/e}(X_2)$ is at most one. If $r_M(X_1) - r_{M/e}(X_1) = r_M(X_2) - r_{M/e}(X_2) = 1$, then

$$r_M(X_1) + r_M(X_2) - r_M(M) = 1.$$

Therefore (X_1, X_2) is a 2-separation of M, contradicting the fact that M is 3-connected. Hence $\mathrm{si}(M/e)$ must be 2-connected. □

Now assume that $\mathrm{si}(M/e)$ is not 3-connected. Then there exists a 2-separation, (X_1'', X_2'') of $\mathrm{si}(M/e)$. By putting back parallel elements and coloops, there is a 2-separation, (X_1', X_2') of M/e. We now consider what happens to this 2-separation in M. Let (X_1, X_2) be this 2-separation in M. If $r_M(X_1) = r_{M/e}(X_1') + 1$ and $r_M(X_2) = r_{M/e}(X_2')$, then (X_1, X_2)

is a 2-separation of M, contradicting the 3-connectedness of M. Hence $r_M(X_1) = r_{M/e}(X_1') + 1$ and $r_M(X_2) = r_{M/e}(X_2') + 1$. Then

$$\begin{aligned} r_M(X_1) + r_M(X_2) - r_M(M) &= r_{M/e}(X_1') + r_{M/e}(X_2') - (r_{M/e}(M/e) + 1) + 2 \\ &= 1 - 1 + 2 \\ &= 2. \end{aligned}$$

So (X_1, X_2) is a 3-separation of M. However, in $\mathrm{si}(M/e)$, the rank of X_1'' and the rank of X_2'' are both at least two, as it is simple. So in M the rank of X_1 and the rank of X_2 are both at least three. This is a contradiction to M being vertically 4-connected, so $\mathrm{si}(M/e)$ must be 3-connected. □

Lemma 3.2.7. *Let M be a rank-r maximum-sized golden-mean matroid with no $F_7^=$ or $S_{10}\backslash f$ minor. Then M is vertically 4-connected.*

Proof. Let $P = PG(r-1, 4)$. Assume that M has an exact vertical 3-separation (X_1, X_2). View M as a restriction of P. Now,

$$\begin{aligned} r(\mathrm{cl}_P(X_1) \cap \mathrm{cl}_P(X_2)) &\leq r(\mathrm{cl}_P(X_1)) + r(\mathrm{cl}_P(X_2)) - r(\mathrm{cl}_P(X_1) \cup \mathrm{cl}_P(X_2)) \\ &\leq r(X_1) + r(X_2) - r(X_1 \cup X_2) \\ &= r(X_1) + r(X_2) - r(M) \\ &= 2. \end{aligned}$$

So the closures of X_1 and X_2 in P meet in a line L of P. Let $r_i = r(X_i)$. As (X_1, X_2) is a vertical 3-separation of M, both r_1 and r_2 must be at least

three.

We consider $|L \cap E(M)|$, noting that it is at most five, as this is the maximum line length in a quaternary matroid. The strategy of the proof is to consider, for each $i \in \{1,2\}$, a simple rank-r_i minor M_i of M, obtained by deleting and contracting elements from the complement of X_i, that is spanned by X_i, contains $(X_1 \cup X_2) \cap L$, and has the maximum number of points among such minors. Thus, for $\{i,j\} = \{1,2\}$, M_i is obtained from M by contracting elements in X_j so that as many points in X_j as possible are projected into the span of X_i. Clearly we may view M_i as a restriction of $P|(L \cup X_i)$.

Sublemma 3.2.7.1. *M_i is non-binary, for $i \in \{1,2\}$.*

Subproof. Let $\{i,j\} = \{1,2\}$. Now assume that M_i is binary. Then, by Theorem 6.6.3 of Oxley [20], as M_i is golden-mean and therefore representable over $GF(5)$, it is regular. Then, by Theorem 2.0.8, the maximum size for M_i is $\binom{r_i+1}{2}$. Also, as M_j is simple and golden-mean, then, by induction, it is no larger than $T^2_{r_j}$. Hence $|E(M_j)| \leq \binom{r_j+3}{2} - 5$. Clearly $E(M)$ can be no bigger than $|E(M_i)| + |E(M_j)|$. So

$$\begin{aligned} |E(M)| &\leq |E(M_i)| + |E(M_j)| \\ &\leq \binom{r_i+1}{2} + \binom{r_j+3}{2} - 5 \\ &= \frac{1}{2}(r_i^2 + r_j^2 + r_i + 5r_j - 4) \end{aligned} \tag{3.2.7.1}$$

Also, as M is maximum-sized and golden-mean, it must be at least as big as

T_r^2. Hence

$$|E(M)| \geq \binom{(r_i + r_j - 2) + 3}{2} - 5$$
$$= \frac{1}{2}(r_i^2 + r_j^2 + r_i + r_j + 2r_i r_j - 10) \qquad (3.2.7.2)$$

Combining (3.2.7.1) with (3.2.7.2), we get

$$\frac{1}{2}(r_i^2 + r_j^2 + r_i + r_j + 2r_i r_j - 10) \leq \frac{1}{2}(r_i^2 + r_j^2 + r_i + 5r_j - 4)$$
$$r_i r_j - 2r_j \leq 3 \qquad (3.2.7.3)$$

However, as (X_1, X_2) is a vertical 3-separation of M, both r_i and r_j must be at least three. Hence the only solution for (3.2.7.3) is $r_i = r_j = 3$. Therefore $r = 4$. So, by (3.2.0.1), $|E(M)| \geq 16$. This implies that $|E(M_i)| = 6$ and $|E(M_j)| = 10$, which are the maximum sizes possible. Now, by Theorem 2.0.8, as M_i is a rank-three regular matroid with six elements, it must be isomorphic to $M(K_4)$. Contracting any element of this, in M, leads to a rank-three golden-mean matroid with more than 10 elements, contradicting Lemma 3.1.1. Therefore M_i is non-binary. □

Now

$$|E(M)| = |X_1| + |X_2|$$
$$= (|E(M_1)| - |(E(M_1) \cap L) - X_1|)$$
$$+ (|E(M_2)| - |(E(M_2) \cap L) - X_2|).$$

As M_i is simple and golden-mean, by induction, it can be no larger than $T^2_{r_i}$. Hence $|E(M_i)| \leq \binom{r_i+3}{2} - 5$. Thus

$$|E(M)| \leq \binom{r_1+3}{2} + \binom{r_2+3}{2} - 10 \\ - \left(|(E(M_1) \cap L) - X_1| + |(E(M_2) \cap L) - X_2|\right).$$

But M is maximum-sized, and therefore at least as big as T^2_r, so

$$|E(M)| \geq \binom{(r_1+r_2-2)+3}{2} - 5.$$

So

$$\frac{1}{2}(r_1+r_2)(r_1+r_2+1) \leq \frac{1}{2}((r_1+2)(r_1+3)+(r_2+2)(r_2+3)) - 5 \\ - (|(E(M_1) \cap L) - X_1| + |(E(M_2) \cap L) - X_2|).$$

Expanding out gives

$$\frac{1}{2}(r_1^2+r_2^2+2r_1r_2+r_1+r_2) \leq \frac{1}{2}(r_1^2+r_2^2+5r_1+5r_2+2) \\ - |(E(M_1) \cap L) - X_1| - |(E(M_2) \cap L) - X_2|.$$

Hence

$$r_1r_2 - 2r_1 - 2r_2 - 1 \leq -(|(E(M_1) \cap L) - X_1| + |(E(M_2) \cap L) - X_2|).$$

And so

$$(r_1 - 2)(r_2 - 2) \leq 5 - (|E(M_1) \cap L| - |X_1 \cap L| + |E(M_2) \cap L| - |X_2 \cap L|)\,. \tag{3.2.7.4}$$

But

$$\begin{aligned} |E(M_i) \cap L| &\geq |(X_1 \cup X_2) \cap L| \\ &= |X_1 \cap L| + |X_2 \cap L|\,, \end{aligned} \tag{3.2.7.5}$$

so, for each $i \in \{1, 2\}$,

$$(r_1 - 2)(r_2 - 2) \leq 5 - |E(M_i) \cap L|\,. \tag{3.2.7.6}$$

Next we take a basis B_1 for X_1 and extend it to a basis B for M. Then $|B - B_1| = r(M) - r(X_1) = r(X_2) - 2$. It follows that $r_{M/(B-B_1)}(X_2 - B) = 2$. This means that M_1 can be assumed to satisfy

$$|E(M_1) \cap L| \geq 2. \tag{3.2.7.7}$$

This means that we can always project at least two points from X_2 into the span of X_1 by contracting only points in $X_2 - X_1$.

Similarly,

$$|E(M_2) \cap L| \geq 2. \tag{3.2.7.8}$$

Combining (3.2.7.7) and (3.2.7.8) with (3.2.7.6), we get

$$(r_1 - 2)(r_2 - 2) \leq 3. \tag{3.2.7.9}$$

If r_1 and r_2 are both at least four, then (3.2.7.9) is a contradiction. Therefore, we can assume that $r_1 = 3$. So (3.2.7.9) becomes $r_2 \leq 5$.

Now suppose $|(X_1 \cup X_2) \cap L| \geq 3$.

Sublemma 3.2.7.2. *If $|(X_1 \cup X_2) \cap L| \geq 3$, then M_1 and M_2 are 3-connected.*

Subproof. Let $M_1' = M|(X_1 \cup (X_2 \cap L))$. Note that by definition, X_1 spans L. Now

$$\begin{aligned} r(M_1') &= r(M|(X_1 \cup (X_2 \cap L))) \\ &= r(M|X_1) \\ &= r(X_1). \end{aligned}$$

If (Y_1, Y_2) is a k-separation of M_1' for some $k \leq 2$, then $r(Y_1)+r(Y_2)-r(X_1) \leq$

$k-1$, and, as $r(X_1) = r(M) - r(X_2) + 2$,

$$r(Y_1) + r(Y_2) - r(M) + r(X_2) - 2 \leq k - 1. \tag{3.2.7.10}$$

Without loss of generality, we may assume that $|Y_1 \cap L| \geq 2$. Then

$$\begin{aligned} r(Y_1 \cup X_2) &\leq r(\mathrm{cl}(Y_1) \cup \mathrm{cl}(X_2)) \\ &\leq r(\mathrm{cl}(Y_1)) + r(\mathrm{cl}(X_2)) - r(\mathrm{cl}(Y_1) \cap \mathrm{cl}(X_2)) \\ &\leq r(Y_1) + r(X_2) - r(\mathrm{cl}(Y_1) \cap \mathrm{cl}(X_2)). \end{aligned}$$

Observe that $\mathrm{cl}(Y_1) \cap \mathrm{cl}(X_2)$ contains L, so $r(\mathrm{cl}(Y_1) \cap \mathrm{cl}(X_2)) \geq 2$. Hence

$$r(Y_1 \cup X_2) \leq r(Y_1) + r(X_2) - 2. \tag{3.2.7.11}$$

Combining (3.2.7.10) with (3.2.7.11) gives $r(Y_2) + r(Y_1 \cup X_2) - r(M) \leq k-1$, so $(Y_2, (Y_1 \cup X_2) - Y_2)$ is a k-separation of M, a contradiction. Thus M_1' is 3-connected, and as M_1 is obtained from M_1' by adding elements that are not loops, coloops or in parallel classes, M_1 is also 3-connected. Similarly, M_2 is 3-connected. □

Sublemma 3.2.7.3. *If* $|(X_1 \cup X_2) \cap L| \geq 3$*, then* $|(X_1 \cup X_2) \cap L| \geq 4$*, and* $r_1 = r_2 = 3$.

Subproof. By Sublemma 3.2.7.1, M_i is not binary. Hence by Lemma 3.2.2, for $\{i, j\} = \{1, 2\}$, the matroid M_i has a $U_{2,4}$ minor using $(X_1 \cup X_2) \cap L$ and

so $|E(M_j) \cap L| \geq 4$.

Firstly, assume that $|E(M_1) \cap L| = |E(M_2) \cap L| = 4$. Then (3.2.7.4) becomes

$$\begin{aligned} r_2 &\leq 7 + |X_1 \cap L| + |X_2 \cap L| - 4 - 4 \\ &= |X_1 \cap L| + |X_2 \cap L| - 1 \end{aligned} \tag{3.2.7.12}$$

If $|X_1 \cap L| + |X_2 \cap L| < 4$, then (3.2.7.12) becomes $r_2 \leq 2$, contradicting the fact that (X_1, X_2) is a vertical 3-separation of M.

If $|X_1 \cap L| + |X_2 \cap L| = 5$, then $|E(M_1) \cap L| = |E(M_2) \cap L| = 5$, and (3.2.7.6) implies that $r_1, r_2 \leq 2$, contradicting the fact that (X_1, X_2) is a vertical 3-separation of M.

Hence $|X_1 \cap L| + |X_2 \cap L| = 4$, and (3.2.7.12) becomes $r_2 \leq 3$, and the fact that (X_1, X_2) is a vertical 3-separation of M implies that $r_2 = 3$.

Next, assume that $|E(M_1) \cap L| = 4$ and $|E(M_2) \cap L| = 5$. Then (3.2.7.4) becomes

$$\begin{aligned} r_2 &\leq 7 + |X_1 \cap L| + |X_2 \cap L| - 4 - 5 \\ &= |X_1 \cap L| + |X_2 \cap L| - 2 \end{aligned} \tag{3.2.7.13}$$

L is a line of the projective geometry $PG(r-1, 4)$, so it contains at most five elements. Hence $|X_1 \cap L| + |X_2 \cap L| \leq 5$, and so (3.2.7.13) becomes $r_2 \leq 3$, and the fact that (X_1, X_2) is a vertical 3-separation of M implies that $r_2 = 3$.

Next, assume that $|E(M_1) \cap L| = |E(M_2) \cap L| = 5$. Then (3.2.7.4) becomes

$$\begin{aligned} r_2 &\leq 7 + |X_1 \cap L| + |X_2 \cap L| - 5 - 5 \\ &= |X_1 \cap L| + |X_2 \cap L| - 3 \end{aligned} \tag{3.2.7.14}$$

L is a line of the projective geometry $PG(r-1, 4)$, so it contains exactly five elements. Hence $|X_1 \cap L| + |X_2 \cap L| \leq 5$, and so (3.2.7.14) becomes $r_2 \leq 2$, contradicting the fact that (X_1, X_2) is a vertical 3-separation of M.

So $3 \leq |X_1 \cap L| + |X_2 \cap L| = |(X_1 \cup X_2) \cap L| \leq 4$, and $r_1 = r_2 = 3$. □

We will now show that $|(X_1 \cup X_2) \cap L|$ can be neither three nor four.

Sublemma 3.2.7.4. $|(X_1 \cup X_2) \cap L| \neq 4$.

Subproof. If $|(X_1 \cup X_2) \cap L| = 4$, then, as $M|X_i$ is simple and golden-mean of rank-three, by induction it has at most ten elements. Furthermore, as M is maximum-sized and golden-mean of rank four it must have at least sixteen elements. Hence $|X_1 - L| = |X_2 - L| = 6$, and so $M|(X_i \cup L)$, for $i \in \{1, 2\}$, is isomorphic to T_3^2.

But T_3^2 has no line of exactly four points, so there is no way to obtain M by identifying two copies of T_3^2 along a four-point line. Hence $|(X_1 \cup X_2) \cap L| \neq 4$. □

Sublemma 3.2.7.5. $|(X_1 \cup X_2) \cap L| \neq 3$.

Subproof. If $|(X_1 \cup X_2) \cap L| = 3$, then, as $M|X_i$ is simple and golden-mean of rank-three, by induction, it has at most ten elements. Furthermore, as

M is simple and golden-mean of rank four it must have at least sixteen elements. Hence we can assume that $|X_1 \cup L|$ is 10 and $|X_2 \cup L|$ is 9 or 10. So $(X_1 \cup L) \cong T_3^2$. Furthermore, $X_2 \cup L$ is isomorphic to either T_2^3 (see Figure 2.3) or $T_2^3 \backslash f$ (where f is any point not on four 3-point lines). In both cases, it is easy to see that two extra points can be projected onto L, meaning that $|E(M_1) \cap L| = 5$, which is a contradiction to (3.2.7.6). So $|(X_1 \cup X_2) \cap L| \neq 3$. □

Hence $|(X_1 \cup X_2) \cap L| \leq 2$. Then (3.2.7.4) becomes

$$3 \leq r_2 \leq 7 - |E(M_1) \cap L| - |E(M_2) \cap L| + |(X_1 \cup X_2) \cap L|\,. \qquad (3.2.7.15)$$

We will now show that there is no possible value for $|(X_1 \cup X_2) \cap L|$.

Sublemma 3.2.7.6. $|(X_1 \cup X_2) \cap L| \neq 0$.

Subproof. Assume that $|(X_1 \cup X_2) \cap L| = 0$. From (3.2.7.7) and (3.2.7.8) we know that both $|E(M_1) \cap L|$ and $|E(M_2) \cap L|$ are at least two. Combining this information with (3.2.7.15), we see that $r_2 = 3$ and both $|E(M_1) \cap L|$ and $|E(M_2) \cap L|$ must be exactly two. By induction, $|E(M)| \geq 16$, so, without loss of generality, $|X_2| \geq 8$. As $M|(X_2)$ is $GF(5)$-representable, if $M|(X_2)$ has no $U_{2,4}$-minor, then it is regular, and so it must be no larger than $M(K_4)$. If $M|(X_2)$ has a $U_{2,4}$-minor, then it is possible to contract a point from $M|(X_2)$ and put four points on L, so $|E(M_1) \cap L| = 4$, which is a contradiction to $|E(M_1) \cap L|$ being equal to two. Hence $|M|(X_2)| \leq 6$, a contradiction to $|X_2| \geq 8$. So $|(X_1 \cup X_2) \cap L|$ cannot equal zero. □

Sublemma 3.2.7.7. $|(X_1 \cup X_2) \cap L| \neq 1$.

Subproof. Assume that $|(X_1 \cup X_2) \cap L| = 1$, and suppose that $r_2 = 3$. Then $r = 4$. Then, by (3.2.7.7), (3.2.7.8), and (3.2.7.15), we see that $2 \leq |E(M_i) \cap L| \leq 3$, for $i \in \{1, 2\}$. So, as M is maximum-sized and golden-mean, it must be at least as large as T_4^2. So $|X_1 \cup X_2| \geq 16$. Hence, without loss of generality, $|X_1| \geq 8$. Now pick $x \in X_1 - L$. As $|E(M_2) \cap L| \leq 3$, there can be no more than three lines passing through x. No matter how we place the remaining points on those lines, we always get a four point line. Now contract an element not on that line, giving $|E(M_2) \cap L| = 4$, a contradiction. So $r_2 \neq 3$. From (3.2.7.7) and (3.2.7.8), we know that both $|E(M_1) \cap L|$ and $|E(M_2) \cap L|$ are at least two. Combining this information with (3.2.7.15), we see that $r_2 = 4$, and $|E(M_i) \cap L| = 2$, for $i \in \{1, 2\}$. So $r = 5$. As M is maximum-sized and golden-mean, it must be at least as large as T_5^2. So $|X_1 \cup X_2| \geq 23$. By induction, $M|X_2$ can be no larger than T_4^2, so $|X_2| \leq 16$. Therefore $|X_1| \geq 7$. Now pick $x \in X_1 - L$. Because $|E(M_2) \cap L| = 2$, x is on at most two lines. Therefore, one of these lines has at least four points and we can contract an element on the other line to get $|E(M_2) \cap L| = 4$, a contradiction. So $|(X_1 \cup X_2) \cap L|$ cannot equal one. □

Sublemma 3.2.7.8. $|(X_1 \cup X_2) \cap L| \neq 2$.

Subproof. Assume $|(X_1 \cup X_2) \cap L| = 2$. So (3.2.7.15) becomes

$$3 \leq r_2 \leq 9 - |E(M_1) \cap L| - |E(M_2) \cap L|\,. \tag{3.2.7.16}$$

Assume that $|E(M_j) \cap L| = 2$, and let $E(M_j) \cap L = \{s, t\}$. Then pick $x \in X_i - L$. As $|E(M_j) \cap L| = 2$, everything in X_i must be on a line with x and either s or t. So $r_i = 3$. Hence r_j can be 3, 4, or 5. If $r_j = 3$, then, as M is maximum-sized and golden-mean, it must be at least as large as T_4^2. Hence $|E(M)| \geq 16$, so $|X_j \cup ((X_1 \cup X_2) \cap L)| \leq 10$, and therefore $|X_i \cup ((X_1 \cup X_2) \cap L)| \geq 8$. Using the same reasoning, we see that if $r_j = 4$, then $|X_i \cup ((X_1 \cup X_2) \cap L)| \geq 9$, and if $r_j = 5$, then $|X_i \cup ((X_1 \cup X_2) \cap L)| \geq 10$. In all three cases, both lines through x must have at least three points on them, and we contract a point from $X_i - \{x, s, t\}$ to project at least three points onto L, implying that $|E(M_j) \cap L| \geq 3$, a contradiction.

So now it follows from (3.2.7.7), (3.2.7.8), and (3.2.7.16) that $|E(M_1) \cap L| = |E(M_2) \cap L| = 3$, and $r_2 = 3$. As M is maximum-sized and golden-mean, it must be at least as large as T_4^2, so $|E(M)| \geq 16$. Then, without loss of generality, $|X_1| \geq 8$. Pick $x \in X_1 - L$. Then, as $|E(M_2) \cap L| = 3$, the element x can be on at most three lines. However we place the remaining five points, we will always get one of these lines having at least four points, which can be projected onto L, implying that $|E(M_j) \cap L| \geq 4$, a contradiction.

Therefore $|(X_1 \cup X_2) \cap L| \neq 2$. □

Therefore, by Sublemmata 3.2.7.4 – 3.2.7.8, there are no possible values for $|(X_1 \cup X_2) \cap L|$, so our original assumption, that M has an exact vertical 3-separation, is incorrect. Therefore M is vertically 4-connected. □

3.2.2 Intersecting Very Long Lines

In this section we consider the case that M, our maximum-sized golden-mean matroid with no $F_7^=$ minor, has intersecting very long lines.

We often consider the matroid obtained by restricting to the long lines through e, contracting e and then simplifying.

Definition 3.2.8. Let M be a matroid, and let e be an element of M, and let $\mathfrak{L}$ be the set of the long lines of M. Let $X = \{e\} \cup \{f \in E(M) \mid \exists L \in \mathfrak{L} \text{ with } e, f \in L\}$. Then $\mathcal{L}(M, e)$ is defined to be $\mathrm{si}((M|X)/e)$.

Lemma 3.2.9. *Let M be a maximum-sized golden-mean matroid with no $F_7^=$ or $S_{10}\backslash f$ minor. If $e \in E(M)$ is on at least two very long lines, then M/e is regular.*

Proof. Let L_1 and L_2 be very long lines containing e and assume that M/e is non-regular. By Theorem 6.6.3 of Oxley [20], any matroid that is representable over $GF(2)$ and $GF(5)$ is regular. Then M/e is non-binary. By Lemma 3.2.7, M is vertically 4-connected, so, by Lemma 3.2.6, $\mathrm{si}(M/e)$ is 3-connected. Let $x_1 \in L_1 - e$ and $x_2 \in L_2 - e$. We can assume that x_1 and x_2 are points of $\mathrm{si}(M/e)$. Then, by Lemma 3.2.2, $\mathrm{si}(M/e)$ has a four-point line minor using $\{x_1, x_2\}$. Hence there exists a subset I of $E(M/e)$ such that $(M/e)/I$ has rank two, and contains at least four points. Moreover, $L_1 - e$ and $L_2 - e$ are parallel classes of $(M/e)/I$. Then M/I is a rank-three matroid containing two very long lines and one four-point line, contradicting Lemma 3.1.1. Hence M/e is regular. □

Note that $\mathcal{L}(M, e)$ is a restriction of M/e, so it is also regular.

Lemma 3.2.10. *Let M be a maximum-sized golden-mean matroid with no $F_7^=$ or $S_{10}\backslash f$ minor and let e be a point of M on at least two very long lines. Then all the circuits in the regular matroid $\mathcal{L}(M, e)$ have size exactly three.*

Proof. Let C be a circuit of $\mathcal{L}(M, e)$ such that $|C| \geq 4$. Let $c_1, \ldots, c_4$ be distinct elements of C. Let $L_1, \ldots, L_4$ be long lines of M such that $e, c_i \in L_i$ for $i \in \{1, 2, 3, 4\}$. Then $(M/(C - \{c_1, \ldots, c_4\}))|(L_1 \cup \cdots \cup L_4)$ obviously contains a 4-spike, contradicting Corollary 3.1.6. Hence there can be no circuit in $\mathcal{L}(M, e)$ of size greater than three, so all circuits have size at most three. As $\mathcal{L}(M, e)$ is simple by definition, all circuits have size at least three. Therefore all circuits in $\mathcal{L}(M, e)$ have size exactly three. □

Corollary 3.2.11. *Let M be a maximum-sized golden-mean matroid with no $F_7^=$ or $S_{10}\backslash f$ minor that has a point, $e \in E(M)$, on at least two very long lines. Then all the circuits in the regular matroid $\mathcal{L}(M, e)$ are pairwise disjoint.*

Proof. From Lemma 3.2.10, we know that all circuits in $\mathcal{L}(M, e)$ have size three. Let C_1 and C_2 be two circuits of $\mathcal{L}(M, e)$ such that $C_1 \cap C_2 \neq \varnothing$. Because $\mathcal{L}(M, e)$ is simple and binary, C_1 and C_2 meet at a single point, x, and $(C_1 \cup C_2) - \{x\}$ is a disjoint union of circuits, so is therefore itself a circuit. However, $|(C_1 \cup C_2) - \{x\}| = 4$, contradicting Lemma 3.2.10. Therefore $C_1 \cap C_2 = \varnothing$ and all circuits in $\mathcal{L}(M, e)$ are pairwise disjoint. □

Lemma 3.2.12. *Let M be a rank-r maximum-sized golden-mean matroid with no $F_7^=$ or $S_{10}\backslash f$ minor, and let $e \in E(M)$ be a point on at least two very long lines. Then $\mathcal{L}(M, e)$ is a collection of coloops.*

Proof. As M is maximum-sized and has rank r, it must be at least as large as T_r^2. So

$$|E(M)| \geq \binom{r+3}{2} - 5. \tag{3.2.12.1}$$

By Lemma 3.2.9, $\mathrm{si}(M/e)$ is regular, and by Theorem 2.0.8 the maximum size of a simple regular matroid of rank s is $\binom{s+1}{2}$. Hence

$$|E(\mathrm{si}(M/e))| \leq \binom{r}{2}. \tag{3.2.12.2}$$

Combining (3.2.12.1) with (3.2.12.2), we get

$$|E(M)| - |E(\mathrm{si}(M/e))| \geq \binom{r+3}{2} - 5 - \binom{r}{2} = 3r - 2. \tag{3.2.12.3}$$

Let k be the number of long lines that go through e, and let the ith long line have length w_i. Then when e is contracted and the resulting matroid simplified, e and every element bar one from each of the long lines through e are removed, for a total of

$$1 + \sum_{i=1}^{k} (w_i - 2)$$

points. Hence

$$|E(M)| - |E(\mathrm{si}(M/e))| = 1 + \sum_{i=1}^{k}(w_i - 2). \tag{3.2.12.4}$$

Combining (3.2.12.3) with (3.2.12.4), we get

$$\sum_{i=1}^{k} w_i \geq 3r + 2k - 3. \tag{3.2.12.5}$$

Recall from Lemma 3.2.10 that every circuit in $\mathcal{L}(M, e)$ has size exactly three.

Sublemma 3.2.12.1. *Let $C = \{c_1, c_2, c_3\}$ be a circuit of $\mathcal{L}(M, e)$, such that $c_i \in L_i$ for $i \in \{1, 2, 3\}$. Then $w_1 = w_2 = w_3 = 3$.*

Subproof. $M|(L_1 \cup L_2 \cup L_3)$ is a rank-three matroid, with three long lines passing through a point. Looking at Figure 3.4, we can see that IK has no point on three long lines. Looking at Figures 2.3 and 3.3, we can see that T_3^2 has exactly one point on three long lines, while $P\backslash c$ has two such points. In all cases, all three lines have length three. It follows from Lemma 3.1.1 that $w_1 = w_2 = w_3 = 3$. □

Let B be a basis of $\mathcal{L}(M, e)$. Then $|B| \leq r - 1$. Suppose C is a circuit of $\mathcal{L}(M, e)$, and $|C - B| > 1$. Let $x \in C - B$. Then $B \cup x$ contains a circuit C', with $x \in C'$. As $|C' - B| = 1$, $C \neq C'$, but $C \cap C' \neq \varnothing$, contradicting Corollary 3.2.11. Therefore every circuit in $\mathcal{L}(M, e)$ is a fundamental circuit with respect to B, so there are $|E(\mathcal{L}(M, e))| - |B|$ circuits in $\mathcal{L}(M, e)$. Then

as $k = |E(\mathcal{L}(M, e))|$, there are at least $k - r + 1$ circuits in $\mathcal{L}(M, e)$. Now let c be the number of circuits in $\mathcal{L}(M, e)$. Then

$$k \leq r + c - 1. \tag{3.2.12.6}$$

As $\mathcal{L}(M, e)$ is representable over $GF(4)$, the maximum value for w_i is five. Combining this with Sublemma 3.2.12.1, we get

$$\begin{aligned} \sum_{i=1}^{k} w_i &\leq 3(3c) + 5(k - 3c) \\ &= 5k - 6c \end{aligned} \tag{3.2.12.7}$$

Combining (3.2.12.5) with (3.2.12.7), we get

$$\begin{aligned} 5k - 6c &\geq 3r + 2k - 3 \\ 3k &\geq 3r + 6c - 3 \\ k &\geq r + 2c - 1. \end{aligned}$$

Together with (3.2.12.6), this implies

$$c \geq 2c.$$

Hence we deduce that $c = 0$, so $\mathcal{L}(M, e)$ is a collection of coloops. □

Corollary 3.2.13. *Let M be a rank-r maximum-sized golden-mean matroid*

with no $F_7^=$ or $S_{10}\backslash f$ minor, and let $e \in E(M)$ be a point on at least two very long lines. Then there are exactly $r-1$ lines through e, all of length five.

Proof. As in the proof of Lemma 3.2.12, let k be the number of lines through e, and let the ith long line have length w_i.

Now assume that $k < r-1$. Then $k = (r-1) - t$, where $t > 0$, and so (3.2.12.7) becomes

$$\sum_{i=1}^{k} w_i \leq 5r - 5t - 5. \tag{3.2.13.1}$$

Also, (3.2.12.5) becomes

$$\begin{aligned} \sum_{i=1}^{k} w_i &\geq 3r + 2(r-1-t) - 3 \\ &= 5r - 2t - 5. \end{aligned} \tag{3.2.13.2}$$

Combining (3.2.13.1) with (3.2.13.2), we see that

$$\begin{aligned} 5r - 5t - 5 &\geq 5r - 2t - 5 \\ -5t &\geq -2t \\ t &\leq 0. \end{aligned}$$

This contradicts our definition of t. Hence $k \not< r-1$, and so

$$k \geq r - 1. \tag{3.2.13.3}$$

By Lemma 3.2.12, there are no circuits in $\mathcal{L}(M, e)$, so (3.2.12.6) becomes

$$k \leq r - 1. \tag{3.2.13.4}$$

Now, (3.2.13.3) combined with (3.2.13.4) implies that $k = r - 1$, so there are exactly $r - 1$ lines through e.

Combining this new information with (3.2.12.5) and (3.2.12.7), we see that

$$\sum_{i=1}^{k} w_i = 5k,$$

and so every line through e has length five. □

Lemma 3.2.14. *Let M be a rank-r maximum-sized golden-mean matroid with no $F_7^=$ or $S_{10}\backslash f$ minor, and let $e \in E(M)$ be a point on at least two very long lines. Then* $\mathrm{si}(M/e) \cong M(K_r)$.

Proof. As M is maximum-sized, it must be at least as big as T_r^2. Hence

$$|E(M)| \geq \binom{r+3}{2} - 5.$$

It follows from Corollary 3.2.13 that

$$|E(M)| - |E(\mathrm{si}(M/e))| = 3r - 2.$$

So

$$|E(\mathrm{si}(M/e))| \geq \binom{r+3}{2} - 5 - 3r + 2 = \binom{r}{2}.$$

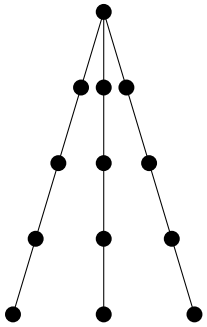

Figure 3.6: Forbidden Configuration from Lemma 3.2.15

However, by Lemma 3.2.9, $\mathrm{si}(M/e)$ is regular, and it has rank at most $r-1$, so it follows from Theorem 2.0.8 that

$$|E(\mathrm{si}(M/e))| \leq \binom{r}{2}.$$

Hence

$$|E(\mathrm{si}(M/e))| = \binom{r}{2}$$

and it follows from Theorem 2.0.8 that $\mathrm{si}(M/e) \cong M(K_r)$. □

Lemma 3.2.15. *Let M be a rank-r maximum-sized golden-mean matroid with no $F_7^=$ or $S_{10}\backslash f$ minor, and let $e \in E(M)$ be a point on at least two very long lines. Then any two elements in $\mathcal{L}(M,e)$ will be on a triangle in* $\mathrm{si}(M/e)$.

Proof. Firstly, note that it follows from Lemma 3.2.12 that the elements of $\mathcal{L}(M,e)$ form a basis of $\mathrm{si}(M/e)$. Now let x be an element from $\mathrm{si}(M/e)$ that is not in a triangle with two elements from $\mathcal{L}(M,e)$. If L_i and L_j are any

long lines containing e, then $r(L_i \cup L_j) = 3$, and $r(L_i \cup L_j \cup x) = 4$. Hence $r_{M/x}(L_i \cup L_j) = 3$, so $L_1, \ldots, L_{r-1}$ are distinct lines of M/x. Hence $\mathcal{L}(M/x, e)$ has $r-1$ points and rank at most $r-2$, so $\mathcal{L}(M/x, e)$ contains a circuit, C. If $|C| = 3$, then there exists a configuration in rank-three that looks like Figure 3.6, a contradiction to Lemma 3.1.1. If $|C| \geq 4$, then using the same technique as in Lemma 3.2.10 a 4-spike can be found, contradicting Corollary 3.1.6. Hence C does not exist, so x must be on a triangle with two elements from $\mathcal{L}(M, e)$. As $\mathrm{si}(M/e)$ is isomorphic to $M(K_r)$, and $\mathcal{L}(M, e)$ is a basis of $\mathrm{si}(M/e)$, any two elements in $\mathcal{L}(M, e)$ will be on a triangle in $\mathrm{si}(M/e)$. □

Lemma 3.2.16. *Let M be a rank-r maximum-sized golden-mean matroid with no $F_7^=$ or $S_{10}\backslash f$ minor, with a point e on at least two very long lines. Then $M \cong T_r^2$.*

Proof. We are going to construct a $GF(4)$-representation for M. Let L_i and L_j be lines passing through e. Then there is a unique element $f \in \mathrm{si}(M/e)$ that is on the line between the point corresponding to $L_i - e$ and the point corresponding to $L_j - e$. Let us consider M restricted to the union of L_i, L_j, and f. This has rank-three, and contains two lines of length five. When we contract f, we must get a copy of $U_{2,5}$ since M is representable over $GF(5)$. This means that f is on four different triangles. So the rank-three restriction is just a copy of T_3^2, as in Figure 2.3.

Now pick an arbitrary element $x_i \in L_i$. For every other line L_j consider the element $f_{i,j}$ that is on the line between $L_i - e$ and $L_j - e$ in $\mathrm{si}(M/e)$. Let x_j be the element of L_j that is contained in a triangle with x_i and $f_{i,j}$.

Then $\{e, x_1, \ldots, x_{r-1}\}$ is a basis of M, and so we get the identity matrix. By Lemma 3.2.12 every line through e has length five so there are three extra points needed. There are no extra dependencies in these points, so we require three sections of the matrix headed by 1's and consisting of scaled identity elements. Over $GF(4)$, there are only three possible ways to do this, so our sections are I_{n-1}, $\alpha(I_{n-1})$, and $\alpha^2(I_{n-1})$. Now all that is left is the regular matroid. From Lemma 3.2.15, we know that any two basis elements are on a triangle in the regular matroid, which gives us the last section of the matrix, D_{n-1}. So this matrix has the form

$$\left[\begin{array}{c|c|c|c|c|c} 1 & 0 \cdots 0 & 1 \cdots 1 & 1 \quad \cdots \quad 1 & 1 \quad \cdots \quad 1 & 0 \cdots 0 \\ \hline 0 & & & & & \\ \vdots & I_{n-1} & I_{n-1} & \alpha(I_{n-1}) & \alpha^2(I_{n-1}) & D_{n-1} \\ 0 & & & & & \end{array}\right].$$

Now consider the following $\mathbb{G}$-matrix for T_r^2, as given in Lemma 3.0.5.

$$\left[\begin{array}{c|c|c|c|c|c} 1 & 0 \cdots 0 & 1 \cdots 1 & 1 \quad \cdots \quad 1 & 1 \quad \cdots \quad 1 & 0 \cdots 0 \\ \hline 0 & & & & & \\ \vdots & I_{n-1} & I_{n-1} & \phi(I_{n-1}) & \phi^2(I_{n-1}) & D_{n-1} \\ 0 & & & & & \end{array}\right].$$

It is easy to check that f, as defined below, is a homomorphism from $\mathbb{G}$ to

$GF(4)$.

$$f : 0 \longmapsto 0$$

$$f : 1 \longmapsto 1$$

$$f : \phi^k \longmapsto \alpha^k.$$

We now apply f to the $\mathbb{G}$-matrix given earlier, giving us the constructed $GF(4)$-matrix. As the $\mathbb{G}$-matrix represents T_r^2, the $GF(4)$-matrix must also, and so M is isomorphic to T_r^2. □

3.2.3 No Intersecting Very Long Lines

Now we consider the case where M has no intersecting very long lines. There are two subcases. The first is that there are no very long lines, and the second is that the very long lines in M are pairwise disjoint. We consider each subcase in turn.

We make use of the following result multiple times in this section.

Lemma 3.2.17 (Bixby, Theorem 1 [2])**.** *Let M be a 3-connected matroid on E, and let $a \in E$. Then either $\mathrm{co}(M\backslash a)$ or $\mathrm{si}(M/a)$ is 3-connected.* □

3.2.3.1 No Very Long Lines

This section deals with golden-mean matroids that have no very long lines. So every line has length at most three.

Lemma 3.2.18. *Let M be a rank-r maximum-sized golden-mean matroid with no $F_7^=$ or $S_{10}\backslash f$ minor, with no very long lines. Then every point of M must be on at least $r+1$ long lines.*

Proof. Let e be an element of M. As M is maximum-sized of rank r, it must be at least as big as T_r^2. Hence

$$\begin{aligned}|E(M)| &\geq \binom{r+3}{2} - 5 \\ &= \frac{1}{2}(r+2)(r+3) - 5 \\ &= \frac{1}{2}(r^2+5r-4).\end{aligned}$$

Now consider $\mathrm{si}(M/e)$. It has rank at most $r-1$, so, by the induction hypothesis, it can be no larger than T_{r-1}^2. Hence

$$\begin{aligned}|E(\mathrm{si}(M/e))| &\leq \binom{r+2}{2} - 5 \\ &= \frac{1}{2}(r+1)(r+2) - 5 \\ &= \frac{1}{2}(r^2+3r-8).\end{aligned}$$

Now, when $\mathrm{si}(M/e)$ is constructed, the number of elements removed by simplification is at least

$$\begin{aligned}|E(M)| - |E(\mathrm{si}(M/e)| &\geq \frac{1}{2}(r^2+5r-4) - \frac{1}{2}(r^2+3r-8) \\ &= \frac{1}{2}(2r+4)\end{aligned}$$

$$= r + 2$$

So we must remove at least $r+1$ points and e from M. As the lines through e have length at most three, we can only remove one point for each line. Hence there must be at least $r + 1$ long lines through e. □

Lemma 3.2.19. *Let M be a rank-r maximum-sized golden-mean matroid with no $F_7^=$ or $S_{10}\backslash f$ minor having no very long lines, and let e be an element of M. Then all circuits in $\mathcal{L}(M, e)$ have size exactly three.*

Proof. Let C be a circuit of $\mathcal{L}(M, e)$ such that $|C| \geq 4$. Let $c_1, \ldots, c_4$ be distinct elements of C. Let $L_1, \ldots, L_4$ be long lines of M such that $e, c_i \in L_i$ for $i \in \{1, 2, 3, 4\}$. Then $(M/(C - \{c_1, \ldots, c_4\}))|(L_1 \cup \cdots \cup L_4)$ obviously contains a 4-spike, contradicting Corollary 3.1.6. Hence there can be no circuit in $\mathcal{L}(M, e)$ of size greater than three, so all circuits have size at most three. As $\mathcal{L}(M, e)$ is simple, all circuits have size at least three. Therefore all circuits in $\mathcal{L}(M, e)$ have size exactly three. □

Corollary 3.2.20. *Let M be a rank-r maximum-sized golden-mean matroid with no $F_7^=$ or $S_{10}\backslash f$ minor having no very long lines, and let e be an element of M. Then all circuits in $\mathcal{L}(M, e)$ are pairwise disjoint.*

Proof. From Lemma 3.2.19, we know that all circuits in $\mathcal{L}(M, e)$ have size three. Let C_1 and C_2 be two circuits of $\mathcal{L}(M, e)$ such that $C_1 \cap C_2 \neq \varnothing$. If $|C_1 \cap C_2| > 1$, then $\mathcal{L}(M, e)$ has a $U_{2,4}$ restriction. Let $X_1, \ldots, X_4$ be the parallel classes in M/e that correspond to the points in the $U_{2,4}$ restriction.

Then M restricted to the union of $X_1, \ldots, X_4$ and e has rank-three, and contains four lines of length three that pass through e. By Lemma 3.1.1, this matroid must be a restriction of T_3^2, which contains two lines of length four. Hence M contains two lines of length four, which is a contradiction as M has no four point lines by definition. Therefore $|C_1 \cap C_2| = 1$, so we can assume that $C_1 = \{c_1, c_2, x\}$ and $C_2 = \{d_1, d_2, x\}$. Then $\{c_1, c_2, d_1, d_2\}$ is also a circuit of $\mathcal{L}(M, e)$, contradicting Lemma 3.2.19. Therefore $C_1 \cap C_2 = \varnothing$ and all circuits in $\mathcal{L}(M, e)$ are pairwise disjoint. □

Lemma 3.2.21. *Let M be a 3-connected golden-mean matroid with no $F_7^=$ or $S_{10}\backslash f$ minor having no very long lines, and let e be an element of M. Then $\mathcal{L}(M, e)$ has at most one circuit.*

Proof. Assume that $\mathcal{L}(M, e)$ has more than one circuit. Let two of these circuits be C_X and C_Y. Then $r(\mathcal{L}(M, e)|(C_X \cup C_Y)) = 4$, as if it is three, then it is possible to find a four element circuit in $\mathcal{L}(M, e)$, contradicting Lemma 3.2.19. In M, these circuits correspond to 3-spikes, X and Y. Note that $M|(X \cup Y)$ has rank five. Consider the closure of $X \cup Y$. If there is an element x not in this closure, then by Lemma 3.2.17, either $\mathrm{si}(M/x)$ or $\mathrm{co}(M\backslash x)$ is 3-connected, and has $M|(X \cup Y)$ as a restriction. By repeating this argument, we find a minor N of M such that N is 3-connected and has $M|(X \cup Y)$ as a restriction. It follows that N has an element f such that $f \notin (\mathrm{cl}_N(X) \cup \mathrm{cl}_N(Y))$, as otherwise N would not be 3-connected. Thus $\mathrm{si}(N/f)$ is a 3-connected golden-mean matroid of rank four having two distinct 3-spike restrictions such that the tip of one is the tip of the other.

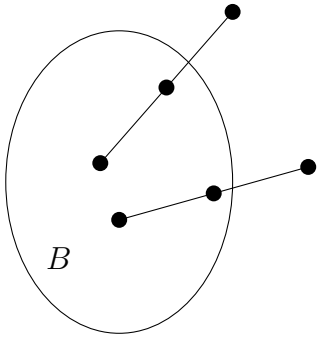

Figure 3.7: Schematic for Lemmata 3.2.22 and 3.2.26

In the contraction, either one line of X and one line of Y merge, or they do not. This is because if f lies in the span of more than one pair of lines, then $M|(X \cup Y)$ must have rank four, contradicting the fact that it has rank five. In either case we get a 4-spike, which is not golden-mean by Corollary 3.1.6. This contradiction means that there can be at most one circuit. □

Lemma 3.2.22. *Let M be a maximum-sized golden-mean matroid with no $F_7^=$ or $S_{10}\backslash f$ minor having no very long lines, and let e be an element of this matroid. Then $\mathcal{L}(M, e)$ must have at least two circuits.*

Proof. By Lemma 3.2.18, M has at least $r+1$ lines through e. So $\mathcal{L}(M, e)$ has at least $r+1$ points in at most rank $r-1$ space. Let B be a basis of $\mathcal{L}(M, e)$. Then $|B| = r(\mathcal{L}(M, e)) \leq r - 1$, so there are at least two points outside of B, each with a fundamental circuit. This situation is illustrated by Figure 3.7. So $\mathcal{L}(M, e)$ has at least two circuits. □

Corollary 3.2.23. *There is no maximum-sized golden-mean matroid with no $F_7^=$ or $S_{10}\backslash f$ minor having no very long lines.*

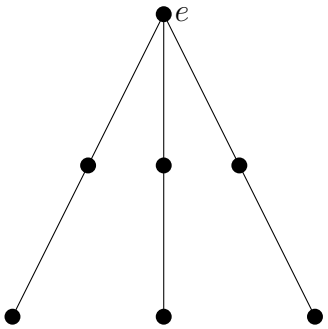

Figure 3.8: rank-three restriction from Lemma 3.2.24

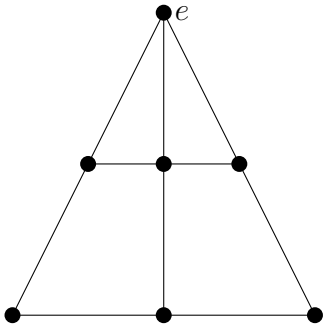

Figure 3.9: P_7

Proof. Combining Lemmata 3.2.21 and 3.2.22, we see that if M is a maximum-sized golden-mean matroid with no $F_7^=$ or $S_{10}\backslash f$ minor having no very long lines, and e is an element of M, then $\mathcal{L}(M, e)$ must have at most one and at least two circuits. This travesty cannot happen, so $\mathcal{L}(M, e)$, and therefore M cannot exist. Hence, there is no maximum-sized golden-mean matroid with no $F_7^=$ minor having no very long lines. □

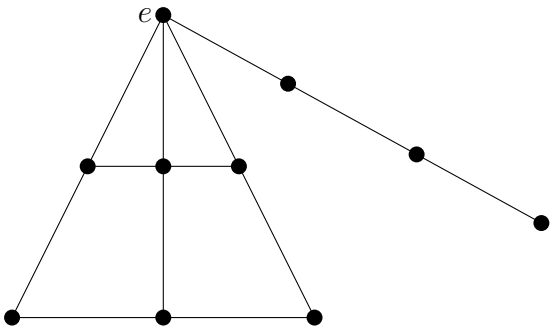

Figure 3.10: N, the rank four restriction from Lemma 3.2.24

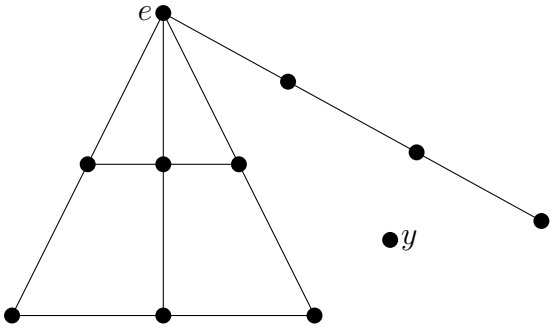

Figure 3.11: Rank four minor from Lemma 3.2.24

3.2.3.2 Pairwise Disjoint Very Long Lines

In this section, we consider golden-mean matroids with pairwise disjoint very long lines.

Lemma 3.2.24. *Let M be a rank-r golden-mean matroid with no $F_7^=$ or $S_{10}\backslash f$ minor such that all very long lines are pairwise disjoint. Then M has no four point lines.*

Proof. Let e be a point in M that is on a four point line. Construct $\mathcal{L}(M, e)$. When e is contracted in M, by the same argument as in Lemma 3.2.18, at least $r + 2$ elements need to be removed after simplification. So e is also on at least $r - 1$ three point lines, and M has a rank-three restriction that looks like Figure 3.8, but with some extra dependencies. By Lemma 3.1.1, M must have P_7 (see Figure 3.9) as a rank-three restriction. By Lemma 3.1.1, the four point line that e is on cannot be in this plane. Thus M has N, as shown in Figure 3.10, as a rank four restriction. Consider the closure of N in M. If there is an element x that is not in this closure, then by Lemma 3.2.17, either $\mathrm{si}(M/x)$ or $\mathrm{co}(M\backslash x)$ is 3-connected, and has N as a restriction. By repeating this argument, we see that M has a 3-connected rank four minor with N as a restriction, as shown in Figure 3.11. Contracting y leads to a rank-three minor of M with an element in at least three long lines, one of which is very long, contradicting Lemma 3.1.1. Hence M can have no four point lines. □

Lemma 3.2.25. *Let M be a rank-r golden-mean matroid with no $F_7^=$ or*

$S_{10}\backslash f$ minor such that all very long lines are pairwise disjoint. Then $\mathcal{L}(M, e)$ has no four point lines.

Proof. Assume that $\mathcal{L}(M, e)$ has a four point line. Suppose that the parallel classes that correspond to this line in M/e are $X_1, \ldots, X_4$. The restriction of M to the union of $X_1, \ldots, X_4$ and e has rank-three, and contains four lines of length three passing through e. Hence, by Lemma 3.1.1, it must be a restriction of T_3^2, and therefore it contains at least one line of length four, contradicting Lemma 3.2.24. Hence $\mathcal{L}(M, e)$ has no four point lines. □

Lemma 3.2.26. *Let M be a rank-r golden-mean matroid with no $F_7^=$ or $S_{10}\backslash f$ minor such that all very long lines are pairwise disjoint. Then every element of M is on exactly one five point line.*

Proof. Let e be an element of M such that e is not on any five point lines. Then, as M is at least as large as T_r^2,

$$|E(M)| \geq \binom{r+3}{2} - 5.$$

Also, as $\mathrm{si}(M/e)$ is no larger than T_{r-1}^2,

$$|E(\mathrm{si}(M/e))| \leq \binom{r+2}{2} - 5.$$

Therefore, when we contract e, we lose at least $r+2$ points, so e must be on at least $r+1$ lines.

From Lemma 3.2.25 we know that $\mathcal{L}(M, e)$ has no four-point lines. So

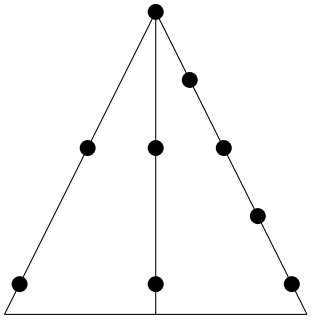

Figure 3.12: rank-three restriction from Lemma 3.2.27

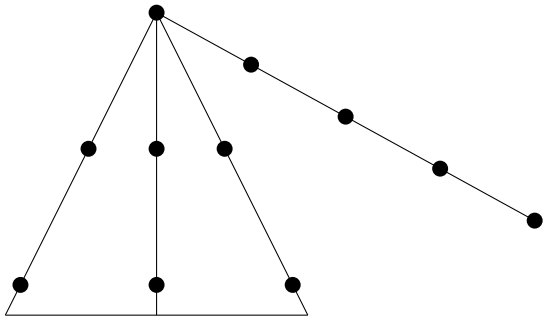

Figure 3.13: N, the rank four restriction from Lemma 3.2.27

$\mathcal{L}(M, e)$ has at least two disjoint three element circuits, as in Figure 3.7. From this, using the same technique as in Lemma 3.2.21, we can show that M has a 4-spike as a minor, contradicting Corollary 3.1.6. Hence such a point e can not exist, and, as all very long lines of M are pairwise disjoint, every element of M is on exactly one line of length five. □

Lemma 3.2.27. *Let M be a rank-r golden-mean matroid with no $F_7^=$ or $S_{10}\backslash f$ minor such that all very long lines are pairwise disjoint. Then $\mathcal{L}(M, e)$ has no circuits.*

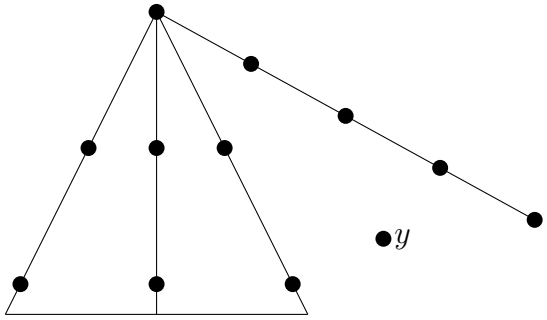

Figure 3.14: Rank four minor from Lemma 3.2.27

Proof. Let e be any element of M and assume that $\mathcal{L}(M, e)$ has a circuit. By Lemma 3.2.25, we know that this circuit must have size three. This means that M has either the matroid shown in Figure 3.12 as a rank-three restriction or N, as shown in Figure 3.13, as a rank four restriction. Note that there may be extra dependencies within the rank-three parts of both restrictions. In the first case, by Lemma 3.1.1, there is no rank-three golden-mean matroid with a line of length five and two lines of length three all going through a common point, so this case is contradictory. In the second case, consider the closure of N in M. If there is an element x not in this closure, then by Lemma 3.2.17 either $\mathrm{si}(M/x)$ or $\mathrm{co}(M\backslash x)$ is 3-connected, and has N as a restriction. By repeating this argument, we see that M has a 3-connected rank four minor with N as a restriction, as shown in Figure 3.14. Contracting y leads to a rank-three minor akin to Figure 3.12, contradicting Lemma 3.1.1, as before. Therefore $\mathcal{L}(M, e)$ can no have circuits. □

Lemma 3.2.28. *Let M be a rank-r golden-mean matroid with no $F_7^=$ or $S_{10}\backslash f$ minor such that all very long lines are pairwise disjoint. Then M is*

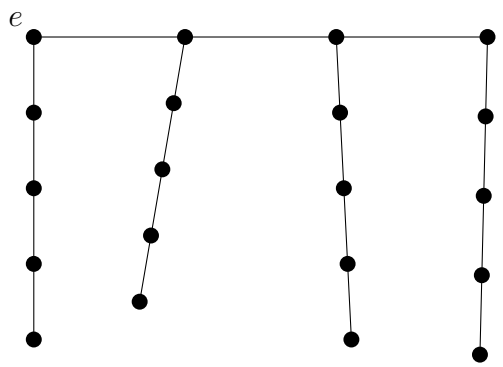

Figure 3.15: Schematic drawing for Lemma 3.2.28.

not maximum-sized.

Proof. By Lemma 3.2.27, $\mathcal{L}(M, e)$ has no circuits. Therefore, $\mathcal{L}(M, e)$ has at most $r - 1$ points. So, in M, e is on at most $r - 2$ lines of length three and one line of length five. So, when e is contracted and the resulting matroid simplified, $r - 2 + 4$ points are lost, meaning that $\mathrm{si}(M/e)$ is at least as large as T^2_{r-1}. Therefore, by the induction assumption, it must be isomorphic to T^2_{r-1}. In T^2_{r-1}, no five point lines are pairwise disjoint. Since $|E(M)| \geq 16$, there must be at least four lines of length five in M, looking something like Figure 3.15. As is clear in that Figure, e must be on two very long lines, contradicting the definition of M. Therefore M is not maximum-sized. □

3.2.4 Conclusion

We will now complete the proof of Theorem 3.0.4.

The lemmata in Section 3.2.2 show that, if M has a point on at least two

very long lines, then M is isomorphic to T_r^2. In Section 3.2.3, we show that if M does not have a point on at least two very long lines, then M is not maximum-sized. The theorem follows immediately from these observations.$\square$

Appendix A

Code

The basic idea behind this computer search is to take a golden-mean representation of $U_{3,5}$ and add on normalised $GF(4)$ vectors, checking for $GF(5)$ representability each time. This works as it follows from work by Whittle [35], using ideas developed by Kahn [13], that $U_{3,5}$ is a stabiliser for $GF(4)$ matroids.

The code itself runs in Sage [32], with Mathematica [36] being called in order to check for $GF(5)$ representability.

```
# Set initial variables
mathematica('SetSystemOptions["ReduceOptions"␣->
␣␣"MaxModularPoints"␣->␣999999999999999999]');

FOUR.<alpha> = GF(4, 'alpha'); # Set GF(4) to be
  generated by alpha
```

```
FIVE = GF(5) # Set GF(5)
FOURLIST = matrix(FOUR, [[1,0,1],[1,0,alpha],
  [1,0,alpha+1],[1,1,0],[1,1,alpha],[1,1,alpha+1],
  [1,alpha,0],[1,alpha,1],[1,alpha,alpha],
  [1,alpha+1,0],[1,alpha+1,1],[1,alpha+1,alpha],
  [1,alpha+1,alpha+1],[0,1,1],[0,1,alpha],
  [0,1,alpha+1],[1,1,1],[1,alpha,alpha+1]]); # all
  possible GF(4) vectors
FOURLIST = FOURLIST.transpose();
var('a,b,c,d,e,f,g,h,i,j,k,l,m,n,o,p,q,
␣␣r,s,t,u,v,w,x,y');
FIVELIST = matrix([[1,0,a],[1,0,b],[1,0,c],[1,d,0],
  [1,e,f],[1,g,h],[1,i,0],[1,j,k],[1,l,m],[1,n,0],
  [1,o,p],[1,q,r],[1,s,t],[0,1,u],[0,1,v],[0,1,w],
  [1,1,1],[1,x,y]]); # all possible GF(5) vectors
FIVELIST = FIVELIST.transpose();
```

This code sets the initial variables.

```
def real_one(guess): # This takes a mathematica
  object, and checks to see if it is {} or not.
  if (guess == mathematica('{}')):
    blank = 0 # I should make it do *something*
  else:
    return true
```

```
  return false
```

This function, `real_one`, takes a Mathematica object, and checks to see if it is {} or not. If it is, then `false` is returned, otherwise `true` is returned. It is needed because if Mathematica returns {} as a possible solution for representation over $GF(5)$, then the matroid being checked is not representable over $GF(5)$.

```
def what_gf5(M,N): # This takes a matrix over GF(4)
  (M), and one over GF(5), (N) and returns all
  possible solutions for the representability
  of N over GF(5)
  equations = []
  ncols = M.ncols();
  combin = range(0, ncols);
  # 3x3 first - they're the easiest
  delta = combinations(combin,3);
  for stuff in delta:
    littleM = M.matrix_from_columns(stuff);
    littleN = N.matrix_from_columns(stuff);
    deter = det(littleM);
    if deter == 0:
      # the equivalent submatrix in the GF(5)
        matrix has determinant = 0
      equations.append(det(littleN) == 0);
```

```
    else:
      equations.append(det(littleN) != 0);
  # now the 2x2 - lots to do here.
  line = combinations(combin,2);
  for stuff in line:
    oblongM = M.matrix_from_columns(stuff);
    oblongN = N.matrix_from_columns(stuff);
    topM = oblongM[0:2]; # rows 1 and 2
    topN = oblongN[0:2];
    middleM = oblongM[0:3:2]; # rows 1 and 3
    middleN = oblongN[0:3:2];
    bottomM = oblongM[1:3]; # rows 2 and 3
    bottomN = oblongN[1:3];
    deter = det(topM)
    if deter == 0:
      # the equivalent submatrix in the GF(5)
        matrix has determinant = 0
      equations.append(det(topN) == 0)
    else:
      equations.append(det(topN) != 0);
    deter = det(middleM);
    if deter == 0:
      # the equivalent submatrix in the GF(5)
```

```
        matrix has det = 0
      equations.append(det(middleN) == 0)
    else:
      equations.append(det(middleN) != 0);
    deter = det(bottomM);
    if deter == 0:
      # the equivalent submatrix in the GF(5)
        matrix has determinant = 0
      equations.append(det(bottomN) == 0)
    else:
      equations.append(det(bottomN) != 0);
  # Now I solve the bunch of equations
  return equations
```

This function, `what_gf5`, takes two matrices – one that is a submatrix of `FOURLIST` over $GF(4)$, and an equivalent one that is a submatrix of `FIVELIST` over $GF(5)$. It takes the $GF(4)$ matrix, `M`, and calculates all 3×3 and 2×2 subdeterminants. It then checks to see if the subdeterminant is zero or not. If it is, the equivalent subdeterminant from the $GF(5)$ matrix, `N`, is set to equal zero. If not, the equivalent subdeterminant from `N` is set to not equal zero. These inequations are collected for all subdeterminants, and a system of inequations, `equations` is returned.

```
def what_variables(vectors): # This takes a tuple,
  and outputs the variables used in said tuple.
```

```
used_vars = [x,y];
if 0 in vectors:
  used_vars.append(a)
if 1 in vectors:
  used_vars.append(b)
if 2 in vectors:
  used_vars.append(c)
if 3 in vectors:
  used_vars.append(d)
if 4 in vectors:
  used_vars.append(e)
  used_vars.append(f)
if 5 in vectors:
  used_vars.append(g)
  used_vars.append(h)
if 6 in vectors:
  used_vars.append(i)
if 7 in vectors:
  used_vars.append(j)
  used_vars.append(k)
if 8 in vectors:
  used_vars.append(l)
  used_vars.append(m)
```

```
  if 9 in vectors:
    used_vars.append(n)
  if 10 in vectors:
    used_vars.append(o)
    used_vars.append(p)
  if 11 in vectors:
    used_vars.append(q)
    used_vars.append(r)
  if 12 in vectors:
    used_vars.append(s)
    used_vars.append(t)
  if 13 in vectors:
    used_vars.append(u)
  if 14 in vectors:
    used_vars.append(v)
  if 15 in vectors:
    used_vars.append(w)
  return used_vars
```

If we look at `FIVELIST`, we can see that it mostly consists of variables. This function, `what_variables`, takes a submatrix of `FIVELIST` and returns the variables used in that submatrix. It is required because solving for all variables is too time-consuming.

```
def is_gm(): # This does everything
```

```
  combin = range(16) # as there are 16 columns to
    add on
  answer = []
  for stuff in combin:
    toy = combinations(combin, stuff+1)
    count = 0;
    while count < len(toy):
      vects = toy[count];
      variables = what_variables(vects);
      vects.append(16);
      vects.append(17);
      test4 = FOURLIST.matrix_from_columns(vects)
      test5 = FIVELIST.matrix_from_columns(vects)
      equations = what_gf5(test4, test5)
      sys = mathematica(equations);
      eqns = mathematica(variables);
      solution = sys.FindInstance(eqns,
        'Modulus->5');
      if real_one(solution):
        answer.append(vects)
      count = count + 1;
      mathematica('Clear[a,b,c,d,e,f,g,h,i,j,k,l,
␣␣␣␣␣␣␣␣m,o,p,q,r,s,t,u,v,w,x,y]')
```

```
return answer
```

This function systematically goes through all possible submatrices of `FOURLIST` and passes them, along with the equivalent `FIVELIST` submatrix, to `what_gf5()`, which gives a system of equations. This system is then converted to Mathematica format, and passed to Mathematica's `FindInstance` function, which solves the system over $GF(5)$, returning a possible solution, `solution`. Finally, `solution` is passed to `real_one()`, to determine whether the possible solution is a real solution or not. Once all possible submatrices of `FOURLIST` have been checked, we have our list of vectors, `answer`, corresponding to all rank-three golden-mean matroids.

Part II

Secret Sharing Matroids

Chapter 4

Introduction

Consider the following scenario, proposed by Liu [17]. You are involved in top secret research with ten other people, and all your work is kept in a secure safe. Because of distrust, it has been decided that any group of six or more researchers can open the safe, but a group of only five people can not get in. How many locks do you need, and how many keys should each person carry?

It turns out that you will need 462 locks, with each researcher carrying 252 keys. Since such a situation is obviously impractical, a new approach is needed. That approach is through secret sharing schemes.

In a secret sharing scheme, we want to share a ***secret***, K, among a bunch of ***participants***, $\mathcal{P}$. Each participant is a p_i. The value of K is chosen by a special player, D (we assume that $D \notin \mathcal{P}$), called a ***dealer***, and each participant receives a ***share***, S_{p_i}. The set of all shares is denoted $\mathcal{S}$.

As the actual details of the secret and the shares are not too important, the way to distinguish between different secret sharing schemes is by distinguishing which subsets of participants are allowed to know the secret. This definition formalises this concept.

Definition 4.0.1. Let $\Gamma \subseteq \wp(\mathcal{P})$. Γ is known as an ***access structure***. If $\gamma \in \Gamma$ then γ is an ***authorised subset*** and is allowed to calculate K.

If $\gamma \in \wp(\mathcal{P})$ is allowed to calculate K, but $\xi \supset \gamma$ is not, then the secret sharing scheme is rather silly. In other words, gaining some more participants means that a particular group of people can no longer calculate the secret. An access structure in which this does not happen has a special property, given by this definition.

Definition 4.0.2. Let Γ be an access structure, and let γ be an arbitrary element of Γ. If, for all $\xi \in \wp(\mathcal{P})$ such that $\gamma \subset \xi$, ξ is also in Γ, then Γ is a ***monotone access structure***.

We will only deal with monotone access structures in this thesis.

Secret sharing schemes were independently introduced by Blakley [3] and Shamir [30], who both introduced a special kind of scheme, known as a threshold scheme. A threshold scheme is akin to the one given earlier, in which t or more participants can calculate K, but fewer than t can not. Formally, a threshold access structure is $\Gamma = \{\gamma \subseteq \mathcal{P} \mid |\gamma| \geq t\}$.

Definition 4.0.3. A secret sharing scheme is a ***perfect secret sharing scheme*** with access structure Γ if the following two properties hold:

(i) If $\gamma \in \Gamma$, then γ can compute K; and

(ii) If $\gamma \notin \Gamma$, then γ can determine nothing at all about K (that is, given the information available to γ, no value of K is more likely than any other).

Definition 4.0.4. A perfect secret sharing scheme is ***ideal*** if $|S_{p_i}| = |K|$. That is, if the secret and the shares have the same length.

A powerful way to think of ideal secret sharing schemes is as a matrix.

Definition 4.0.5. Let $A = [a_{ij} \mid i \in I,\ j \in J]$ be a finite matrix with entries from a finite set S such that $|S| > 1$. For $i \in I$, $j \in J$, and $X \subseteq J - \{j\}$, let

$$n(i, j, X) = \{a_{kj} \mid k \in I,\ a_{kx} = a_{ix} \text{ for all } x \in X\}.$$

Then A is a ***secret sharing matrix*** over S if for all $j \in J$ and all $X \subseteq J - \{j\}$, either $n(i, j, X) = S$ for all $i \in I$, or $|n(i, j, X)| = 1$ for all $i \in I$.

Example 4.0.6. This is a secret-sharing matrix with $S = \{\heartsuit, \spadesuit\}$.

	D	p_1	p_2	p_3	p_4	p_5
1	♡	♠	♡	♠	♡	♠
2	♡	♠	♠	♡	♡	♡
3	♡	♡	♡	♡	♠	♠
4	♡	♡	♠	♠	♠	♡
5	♠	♡	♡	♠	♡	♡
6	♠	♡	♠	♡	♡	♠
7	♠	♠	♡	♡	♠	♡
8	♠	♠	♠	♠	♠	♠

It is often simple yet tedious to show that a particular matrix is secret-sharing, so we will only do a few checks.

Firstly, consider $j = p_3$ and $X = \{D, p_1\}$. Then

$$
\begin{aligned}
n(1, p_3, \{D, p_1\}) &= \{a_{1p_3}, a_{2p_3}\} = \{\spadesuit, \heartsuit\} \\
n(2, p_3, \{D, p_1\}) &= \{a_{1p_3}, a_{2p_3}\} = \{\spadesuit, \heartsuit\} \\
n(3, p_3, \{D, p_1\}) &= \{a_{3p_3}, a_{4p_3}\} = \{\heartsuit, \spadesuit\} \\
n(4, p_3, \{D, p_1\}) &= \{a_{3p_3}, a_{4p_3}\} = \{\heartsuit, \spadesuit\} \\
n(5, p_3, \{D, p_1\}) &= \{a_{5p_3}, a_{6p_3}\} = \{\spadesuit, \heartsuit\} \\
n(6, p_3, \{D, p_1\}) &= \{a_{5p_3}, a_{6p_3}\} = \{\spadesuit, \heartsuit\} \\
n(7, p_3, \{D, p_1\}) &= \{a_{7p_3}, a_{8p_3}\} = \{\heartsuit, \spadesuit\} \\
n(8, p_3, \{D, p_1\}) &= \{a_{7p_3}, a_{8p_3}\} = \{\heartsuit, \spadesuit\}\,.
\end{aligned}
$$

So $n(i, p_3, \{D, p_1\}) = \{\heartsuit, \spadesuit\} = S$ for all $i \in I$.

Next, consider $j = p_3$ and $X = \{p_2, p_4\}$. Then

$$\begin{aligned}
n(1, p_3, \{p_2, p_4\}) &= \{a_{1p_3}, a_{5p_3}\} = \{\spadesuit\} \\
n(2, p_3, \{p_2, p_4\}) &= \{a_{2p_3}, a_{6p_3}\} = \{\heartsuit\} \\
n(3, p_3, \{p_2, p_4\}) &= \{a_{3p_3}, a_{7p_3}\} = \{\heartsuit\} \\
n(4, p_3, \{p_2, p_4\}) &= \{a_{4p_3}, a_{8p_3}\} = \{\spadesuit\} \\
n(5, p_3, \{p_2, p_4\}) &= \{a_{1p_3}, a_{5p_3}\} = \{\spadesuit\} \\
n(6, p_3, \{p_2, p_4\}) &= \{a_{2p_3}, a_{6p_3}\} = \{\heartsuit\} \\
n(7, p_3, \{p_2, p_4\}) &= \{a_{3p_3}, a_{7p_3}\} = \{\heartsuit\} \\
n(8, p_3, \{p_2, p_4\}) &= \{a_{4p_3}, a_{8p_3}\} = \{\spadesuit\}\,.
\end{aligned}$$

So $|n(i, p_3, \{p_2, p_4\})| = 1$ for all $i \in I$. $\Diamond$

Let A be a secret sharing matrix, which is public knowledge. Label the columns of A with $\{D\} \cup \mathcal{P}$. Then D picks row q uniformly at random from A. Without loss of generality, we can assume that the column headed by D is the first column. Then the secret is a_{q1}, and participant p_i gets given share a_{qp_i}. It is not too hard to see that this gives an ideal secret sharing scheme, with $\gamma \in \wp(\mathcal{P})$ being authorised if $|n(i, 1, \gamma)| = 1$ and not authorised otherwise.

In Example 4.0.6, if we pick row 3, then the secret is $\heartsuit$. If p_2 and p_4 get together, they can combine their knowledge and reduce the possible rows to 3 or 7. However, the secret could still be either $\heartsuit$ or $\spadesuit$, so they know nothing

about the secret. However, if p_1 joins in, then they are able to figure out that the row picked was row 3, and the secret is ♡.

Definition 4.0.7. Let $A = [a_{ij} \mid i \in I, j \in J]$ be a secret sharing matrix. Then $X \subseteq J$ ***spans*** $j \in J - X$ if $|n(i, j, X)| = 1$ for all $i \in I$, and $Y \subseteq J$ is ***independent*** if for all $j \in Y$, $Y - \{j\}$ does not span j.

This Theorem follows from Theorem 1 of Brickell and Davenport [4].

Theorem 4.0.8. *Let $A = [a_{ij} \mid i \in I, j \in J]$ be a secret sharing matrix, and let $\mathcal{I}$ be the collection of independent sets. Then $M = (J, \mathcal{I})$ is a matroid with ground set J and independent sets $\mathcal{I}$. M is said to be a* ***secret sharing matroid****, and A is a secret sharing matrix for M.* □

It is known that all representable matroids are secret sharing (see [18] for instance). Also, Seymour [29] has shown that the Vamos matroid is not secret sharing, so not all matroids are secret sharing. This part of the thesis is devoted to summarising some of the other known results.

The secret sharing matrix from Example 4.0.6 is actually a secret sharing matrix for $M(K_4)$, with labels as in Figure 4.1.

There is a more natural relation between the secret sharing matrix and the secret sharing matroid.

Lemma 4.0.9 (Seymour, Theorem 1.1 [29])**.** *Let $A = [a_{ij} \mid i \in I, j \in J]$ be a matrix with entries from some finite set S, and let M be a matroid with ground set J. Then A is a secret sharing matrix for M if and only if for all $X \subseteq J$, the submatrix $[a_{ij} \mid i \in I, j \in X]$ has exactly $|S|^{r(X)}$ distinct rows.* □

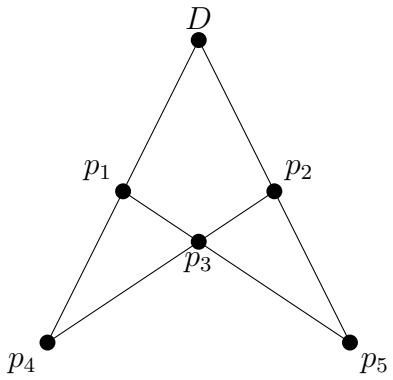

Figure 4.1: Examples 4.0.6 and 4.1.5

Note that loops are just columns consisting of one symbol and all entries from a parallel class have identical columns, so neither element gives any useful information. Hence we can assume that all matroids in this part of the thesis are simple.

4.1 Partitions

There are alternate definitions for secret sharing matroids (see [31], for example). One of particular interest has been developed by Matúš [19] and utilises partitions.

Definition 4.1.1. Let Ω be a set. A family ϖ of nonempty sets is a ***partition*** of Ω if the union of the elements of ϖ is equal to Ω and the elements of ϖ are pairwise disjoint. Elements of ϖ are called the ***blocks*** of the partition.

Definition 4.1.2. Let Ω be a set, and let ϖ and ϖ' be two partitions of

Ω. If every member of ϖ' is a subset of some element of ϖ, then ϖ' is a ***refinement*** of ϖ, denoted $\varpi' \leq \varpi$. We say that ϖ' is ***finer*** than ϖ and that ϖ is ***coarser*** than ϖ'.

The "finer-than" relation on the set of partitions of Ω is a partial order, so a meet can be defined:

Definition 4.1.3. Let $\mathfrak{S}$ be a set with partial order $\leq$, and let $\mathfrak{a}$ and $\mathfrak{b}$ be two elements of $\mathfrak{S}$. An element $\mathfrak{m}$ of $\mathfrak{S}$ is the ***meet*** of $\mathfrak{a}$ and $\mathfrak{b}$ if:

1. $\mathfrak{m} \leq \mathfrak{a}$ and $\mathfrak{m} \leq \mathfrak{b}$, and
2. for any $\mathfrak{n}$ in $\mathfrak{S}$, if $\mathfrak{n} \leq \mathfrak{a}$ and $\mathfrak{n} \leq \mathfrak{b}$, then $\mathfrak{n} \leq \mathfrak{m}$.

If the meet of $\mathfrak{a}$ and $\mathfrak{b}$ exists, it is denoted $\mathfrak{a} \wedge \mathfrak{b}$.

Note that the meet of multiple elements is defined in the obvious way

$$\bigwedge_{i=1}^{k} \mathfrak{a}_i = \mathfrak{a}_1 \wedge \cdots \wedge \mathfrak{a}_k.$$

Also note that the meet of two partitions is always defined. If ϖ and ϱ are two partitions of a set S, then the blocks of $\varpi \wedge \varrho$ are defined as

$$\{a \cap b \mid a \text{ is a block of } \varpi, b \text{ is a block of } \varrho\}.$$

Definition 4.1.4 (Matúš [19])**.** Let $M = (E, r)$ be a matroid with rank function r, and let $d \geq 2$ be an integer. M is ***partition representable***

(p-representable) of degree d if there exists a finite set Ω of cardinality $d^{r(M)}$ and partitions ϖ_i of Ω, $i \in E$, such that for every $F \subseteq E$ the meet-partition $\varpi_F = \bigwedge_{i \in F} \varpi_i$ has $d^{r(F)}$ blocks all of the same cardinality.

Example 4.1.5. Let $\Omega = \{\alpha, \beta, \gamma, \delta, \varepsilon, \zeta, \eta, \vartheta\}$. Then the following partitions of Ω give a p-representation of $M(K_4)$, with labels as in Figure 4.1.

$$\varpi_D = \{\{\alpha, \beta, \gamma, \delta\}, \{\varepsilon, \zeta, \eta, \vartheta\}\}$$
$$\varpi_{p_1} = \{\{\alpha, \beta, \eta, \vartheta\}, \{\gamma, \delta, \varepsilon, \zeta\}\}$$
$$\varpi_{p_2} = \{\{\alpha, \gamma, \varepsilon, \eta\}, \{\beta, \delta, \zeta, \vartheta\}\}$$
$$\varpi_{p_3} = \{\{\alpha, \delta, \varepsilon, \vartheta\}, \{\beta, \gamma, \zeta, \eta\}\}$$
$$\varpi_{p_4} = \{\{\alpha, \beta, \varepsilon, \zeta\}, \{\gamma, \delta, \eta, \vartheta\}\}$$
$$\varpi_{p_5} = \{\{\alpha, \gamma, \zeta, \vartheta\}, \{\beta, \delta, \varepsilon, \eta\}\}$$

$\Diamond$

It was noted without proof by Matúš [19] that p-representable matroids are exactly the same as secret-sharing matroids. A proof is given here.

Proposition 4.1.6. *A matroid is p-representable if and only if it is secret sharing.*

Proof. Let M be a p-representable matroid of degree d. Then there is a finite set, $\Omega = \{\omega_1, \ldots, \omega_n\}$, of cardinality $d^{r(M)}$ and partitions ϖ_i, $i \in E$, such that for every $F \in \wp(E)$ the meet-partition ϖ_F has $d^{r(F)}$ equicardinal blocks. In particular, each ϖ_i has $d^{r(i)} = d$ blocks. Without loss of generality, these

blocks can be labelled by the integers $\{1, \ldots, d\}$. Construct a matrix with columns headed by ϖ_i, $i \in E$, and rows labelled by Ω. In the entry of the matrix defined by ϖ_i and ω_j, place an integer corresponding to whichever block of ϖ_i contains ω_j. For example, if we look at ϖ_{p_2} from Example 4.1.5, we would put a 1 in the row labelled by ζ. Note that the order of the blocks does not matter, as we are only interested in distinct rows. Let X be an arbitrary subset of E. The meet partition ϖ_X is defined by the columns of the matrix headed by $\{\varpi_i \mid i \in X\}$. The elements of this partition are $|X|$-tuples of elements of $\{1, \ldots, d\}$. This partition has $d^{r(X)}$ equicardinal blocks. So the submatrix headed by the partitions of the elements of X has $d^{r(X)}$ distinct rows. Therefore the matrix we have constructed is a secret sharing matrix for M.

Conversely, let M be a secret-sharing matroid. So there exists a secret-sharing matrix for M, with entries from some finite set $S = \{1, \ldots, d\}$. This matrix must have at least $d^{r(M)}$ rows. If it has more, then it has duplicate rows, and we can ignore all duplicates without losing the secret-sharing property. Therefore the matrix has exactly $d^{r(M)}$ rows. Let B be a basis of M. Then the submatrix headed by elements of B has $d^{r(B)} = d^{r(M)}$ distinct rows. These rows are all possible $|B|$-tuples. Removing one column from this will leave behind exactly d copies of each $(|B| - 1)$-tuple, and so on. Hence, if I is an independent set, then the submatrix headed by the elements of I has $d^{r(I)}$ rows, all repeated the same number of times. Now let X be an arbitrary subset of E. If X is independent, then, by the previous argument,

we are done. So X is dependent. Let I be the largest independent subset of X. Then the submatrix headed by the elements of I has $d^{r(I)} = d^{r(X)}$ distinct rows, all repeated the same number of times. Clearly, adding a new column from $X - I$ to this matrix cannot decrease the number of distinct rows. As this matrix is secret-sharing, and adding the new column does not increase the rank, the submatrix with the new column added on also has $d^{r(X)}$ distinct rows, each repeated the same number of times. This process can be continued until the submatrix headed by X is created, with the same condition. As X is an arbitrary subset of E, and the matrix has exactly $d^{r(M)}$ rows, this matrix is a matrix formed by partitions, as in the earlier part of the proof. So $\Omega = \{\omega_1, \ldots, \omega_n\}$ is the set that indexes the rows of this matrix, with partitions ϖ_i, $i \in E$, each having d blocks, defined by the values in the ith column of the matrix. This is a p-representation of M, so M is p-representable. □

Chapter 5

Results

5.1 $M(K_4)$

5.1.1 Quadrangle Criterion

The quadrangle criterion is a well-known property (see [6] for instance) of latin squares, and forms an important link with groups.

Definition 5.1.1 (Euler [8])**.** A ***latin square*** is a $n \times n$ matrix over some set, $\mathfrak{S}$, such that $|\mathfrak{S}| = n$ and all elements of $\mathfrak{S}$ occur in each row and each column of the matrix exactly once.

Definition 5.1.2. A 4-tuple, (a, b, c, d) of elements of a matrix M is said to be a ***quadrangle*** if it is of the form $(m_{i,j}, m_{i,k}, m_{l,k}, m_{l,j})$. That is, if the four elements are the corners of a rectangular block in M, with at least two rows and two columns, such that a and c lie on one of the diagonals of the

rectangular block.

Definition 5.1.3 (Frolov [10])**.** A matrix M is said to satisfy the ***quadrangle criterion*** if whenever (a, b, c, d) and (a', b', c', d') are two quadrangles satisfying $a = a'$, $b = b'$, and $c = c'$; then $d = d'$.

Theorem 5.1.4. *Let M be a latin square of order n. Then M is the multiplication table of a finite group (of order n) if and only if the quadrangle criterion holds for M.*

Proof. Assume that M is a multiplication table of a finite group. Let $(m_{i,j}, m_{i,k}, m_{l,k}, m_{l,j})$ and $(m_{i',j'}, m_{i',k'}, m_{l',k'}, m_{l',j'})$ be two quadrangles from M such that $m_{i,j} = m_{i',j'}$, $m_{i,k} = m_{i',k'}$, and $m_{l,k} = m_{l',k'}$. Then:

$$\begin{aligned}
m_{l,j} &= m_l m_j \\
&= m_l(m_k m_k^{-1})(m_i^{-1} m_i)m_j \\
&= (m_l m_k)(m_i m_k)^{-1}(m_i m_j) \\
&= m_{l,k} m_{i,k}^{-1} m_{i,j} \\
&= m_{l',k'} m_{i',k'}^{-1} m_{i',j'} \\
&= (m_{l'} m_{k'})(m_{i'} m_{k'})^{-1}(m_{i'} m_{j'}) \\
&= m_{l'}(m_{k'} m_{k'}^{-1})(m_{i'}^{-1} m_{i'})m_{j'} \\
&= m_{l'} m_{j'} \\
&= m_{l',j'}
\end{aligned}$$

Conversely, we will show that if the quadrangle criterion holds for M, then

M is a Cayley table of a finite group, G.

For M to be a group table, we need to pick a header and a sideline. Without loss of generality, we pick the first row and first column, respectively. Then $m_{1,1}$ will be e, the identity element of G. Since M is a latin square, e occurs once in each row and column, so $m_i x = e$ and $y m_j = e$ are soluble for every choice of m_i and m_j. Thus inverses exist.

Let a, b, and c be arbitrary elements from M. If one of them is equal to e, then $a(bc) = (ab)c$ is trivial. So, we can assume that none of them are equal to e. Consider the following two portions of M:

	b	bc
e	b	bc
a	ab	$a(bc)$

	e	c
b	b	bc
ab	ab	$(ab)c$

By the quadrangle criterion, $a(bc) = (ab)c$ and so associativity is satisfied. Hence M is the multiplication table of some finite group. □

5.1.2 All p-representations of $M(K_4)$ arise from a group

Intuitively, two p-representations are the same if one can get from one to the other by relabelling the partitions. These next definitions formalise the concept.

Definition 5.1.5. Let ϖ, partitioning $\Omega = \{\omega_1, \ldots, \omega_n\}$, be a p-representation of a matroid, and let f be a function operating on ϖ. We say that f is ***ϖ-invariant*** if ω_i and ω_j are in the same block of ϖ_k, $f(\omega_i)$

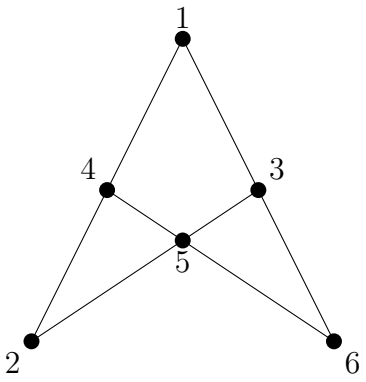

Figure 5.1: Example 5.1.8

and $f(\omega_j)$ must be in the same block of $f(\varpi_k)$.

Definition 5.1.6. Let ϖ, partitioning Ω_ϖ, and ϱ, partitioning Ω_ϱ, be two p-representations of a matroid (E, r). Then ϖ and ϱ are ***equivalent*** if there exists a bijection f from Ω_ϖ to Ω_ϱ such that $f(\varpi_i) = \varrho_i$ for all $i \in E$.

Partitions can get rather unwieldy. It would be good if we could get some more powerful machinery. For example, groups. This concept was introduced by Matúš [19].

Definition 5.1.7. A p-representation of a rank-r matroid M is ***group-induced*** (we say it arises from a group) if there is a group G and functions, f_i, $i \in E$, from G^r to G, such that the blocks of ϖ_i are $\{(g_1, \ldots, g_r) \in G^r \mid f_i(g_1, \ldots, g_r) = g\}$, for all $g \in G$, giving a p-representation of M that is equivalent to the original p-representation.

Example 5.1.8. Consider $M(K_4)$, as shown in Figure 5.1, and let G be a group. Then a group-induced p-representation of $M(K_4)$ is defined by the following functions on G^3:

$$\varpi_1 \text{ has blocks } \left\{(g_1, g_2, g_3) \in G^3 \mid g_1 = h\right\} \text{ for all } h \in G$$
$$\varpi_2 \text{ has blocks } \left\{(g_1, g_2, g_3) \in G^3 \mid g_2 = h\right\} \text{ for all } h \in G$$
$$\varpi_3 \text{ has blocks } \left\{(g_1, g_2, g_3) \in G^3 \mid g_3 = h\right\} \text{ for all } h \in G$$
$$\varpi_4 \text{ has blocks } \left\{(g_1, g_2, g_3) \in G^3 \mid g_1 g_2^{-1} = h\right\} \text{ for all } h \in G$$
$$\varpi_5 \text{ has blocks } \left\{(g_1, g_2, g_3) \in G^3 \mid g_2 g_3^{-1} = h\right\} \text{ for all } h \in G$$
$$\varpi_6 \text{ has blocks } \left\{(g_1, g_2, g_3) \in G^3 \mid g_3 g_1^{-1} = h\right\} \text{ for all } h \in G \qquad \Diamond$$

In this example, the first three partitions are defined by the coordinates of G^3. This is a particular type of p-representation, defined as follows.

Definition 5.1.9. Let $B = \{b_1, \ldots, b_r\}$ be a basis of a p-representable matroid, M, and let ϖ be a p-representation of M, partitioning G^r, where G is a finite set. Then ϖ is in ***coordinate form*** with respect to B if for all $b_i \in B$, ϖ_i has blocks $\{(g_1, g_2 \ldots, g_r) \in G^r \mid g_i = h\}$ for all $h \in G$.

Matúš [19] states, but does not prove, the following claim.

Proposition 5.1.10. *Let M be a p-representable matroid with basis B, and let ϖ be a p-representation of M, partitioning G, a finite set. Then there exists an equivalent p-representation of M in coordinate form with respect to B.*

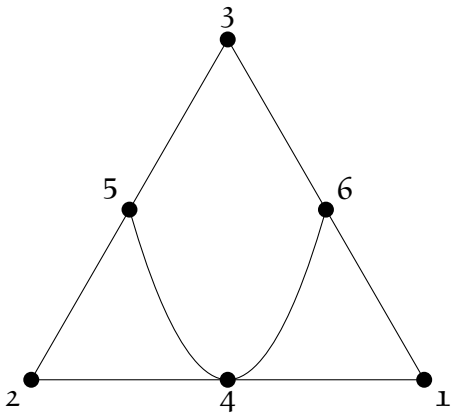

Figure 5.2: $M(K_4)$ as used in the proof of Proposition 5.1.11

Proof. Let $B = \{b_1, \ldots, b_r\}$. We label the blocks of ϖ_i, where $i \in \{1, \ldots, r\}$, with the integers $1, \ldots, d$. Now every element $x \in G$ is uniquely determined by the blocks $(\mathfrak{b}_1, \ldots, \mathfrak{b}_r)$, where $\mathfrak{b}_i$ is the block of ϖ_i that contains x. Therefore there is a one-to-one correspondence between elements of G and r-tuples with entries from $\{1, \ldots, d\}$. This induces a p-representation of M on the set consisting of these tuples, and it is in coordinate form with respect to B. □

Before we prove the following proposition, which is based on Proposition 3.1 of Matúš [19], we will define some notation.

Let ϖ be a p-representation, partitioning $\Omega = \{\omega_1, \ldots, \omega_k\}$. The notation $\omega_j \overset{i}{\sim} \omega_k$ means that ω_j and ω_k are in the same block of ϖ_i.

Proposition 5.1.11. *All p-representations of $M(K_4)$ arise from a group. In particular, if the p-representation is in coordinate form with respect to the basis $\{1, 2, 3\}$, taken from Figure 5.2, then $f_4 = xy^{-1}$, $f_5 = yz^{-1}$, and*

$f_6 = zx^{-1}$.

Proof. Let ϖ be a p-representation of $M(K_4)$ (as in Figure 5.2), partitioning G^3, where G is some finite set. The proof of Proposition 5.1.10 explains why we are able to assume that Ω, the set we are partitioning, has the form G^r, where G is a set of cardinality d. By Proposition 5.1.10, we can assume that ϖ is in coordinate form with respect to the basis $\{1, 2, 3\}$ – that is, ϖ_1 is the x-coordinate, ϖ_2 is the y-coordinate, and ϖ_3 is the z-coordinate. Since $\{1, 2, 4\}$ is a triangle, if two triples belong to the same block of ϖ_1 and ϖ_2, they must belong to the same block of ϖ_4. This means that the blocks of ϖ_4 are defined entirely by the x and y coordinates. That is, if (a, b, c) and (d, e, f) are in the same block of ϖ_4, then (a, b, c') and (d, e, f') are also in this particular block, for all possible choices of c, c', f, and f'. By a cyclic argument, the blocks of ϖ_5 are defined entirely by the y and z coordinates, and the blocks of ϖ_6 are defined entirely by the x and z coordinates.

Another way to look at ϖ_4 is as a matrix, $\mathfrak{M}_4$, with rows and columns labelled by elements of G, and consisting of elements of G. Assign (a, b) and (c, d) the same symbol in $\mathfrak{M}_4$ if and only if $(a, b, g) \overset{4}{\sim} (c, d, h)$ for all $g, h \in G$. This is well-defined because the blocks of ϖ_4 are defined entirely by the x and y coordinates. $\mathfrak{M}_5$ is constructed in the same way, with (a, b) and (c, d) being assigned the same symbol in $\mathfrak{M}_5$ if and only if $(g, a, b) \overset{5}{\sim} (h, c, d)$ for all $g, h \in G$. Likewise, (a, b) and (c, d) are assigned the same symbol in $\mathfrak{M}_6$ if and only if $(a, g, b) \overset{6}{\sim} (c, h, d)$ for all $g, h \in G$. The actual symbol is not important, as we are only concerned with distinct elements, not what those

elements are.

Example 5.1.11.1. Let $G = \{\spadesuit, \heartsuit, \clubsuit, \diamondsuit\}$. Then a possible $\mathfrak{M}_4$ is shown below

$$\mathfrak{M}_4 = \begin{array}{c} \\ \spadesuit \\ \heartsuit \\ \clubsuit \\ \diamondsuit \end{array} \begin{array}{c} \begin{array}{cccc} \spadesuit & \heartsuit & \clubsuit & \diamondsuit \end{array} \\ \begin{bmatrix} \diamondsuit & \clubsuit & \heartsuit & \spadesuit \\ \spadesuit & \diamondsuit & \clubsuit & \heartsuit \\ \heartsuit & \spadesuit & \diamondsuit & \clubsuit \\ \clubsuit & \heartsuit & \spadesuit & \diamondsuit \end{bmatrix} \end{array}$$

This shows that, for example, $(\clubsuit, \heartsuit, a) \overset{4}{\sim} (\spadesuit, \diamondsuit, b)$ for all $a, b \in G$. $\diamondsuit$

If we look at Example 5.1.11.1, we can see that $\mathfrak{M}_4$ is a latin square, and all elements on the diagonal are the same. It turns out that these two properties are not just a coincidence, as the next two sublemmata show.

Sublemma 5.1.11.2. *$\mathfrak{M}_i$ is a latin square, for $i \in \{4, 5, 6\}$.*

Subproof. We will only show this for $\mathfrak{M}_4$. It follows by a cyclic argument for $\mathfrak{M}_5$ and $\mathfrak{M}_6$.

Assume that $\mathfrak{M}_4$ is not a latin square. Then, without loss of generality, (a, b) and (a, b') have the same symbol, but $b \neq b'$. So $(a, b, g) \overset{4}{\sim} (a, b', h)$ for all $g, h \in G$. As ϖ_1 is defined entirely by the x coordinate, $(a, b, g) \overset{1}{\sim} (a, b', h)$ for all $g, h \in G$. As $\{1, 2, 4\}$ is a triangle, two elements of G^3 are in the same block of ϖ_2 if and only if they are in the same block of ϖ_1 and the same block of ϖ_4. Hence $(a, b, g) \overset{2}{\sim} (a, b', h)$ for all $g, h \in G$. As ϖ_2 is defined by the y

coordinate, this implies that $b = b'$, and so $(a, b) = (a, b')$, a contradiction. Therefore, $\mathfrak{M}_4$ must be a latin square. $\square$

The partition ϖ_i contains the diagonal as a block if for all $a, b \in G$, (a, a) and (b, b) have the same symbol in $\mathfrak{M}_{\mathfrak{i}}$.

Sublemma 5.1.11.3. *ϖ_4 and ϖ_5 contain the diagonal as a block.*

Subproof. Without loss of generality, let $(g_i, g_j, \square)$ be in a block of ϖ_4, where $\square$ ranges over all elements of G. By the pigeonhole principle, there exists a permutation, ς, of G, such that $\varsigma(g_j) = g_i$, for all g_j and g_i in G. If we apply ς to the y coordinate layer of G^3, we see that our block of ϖ_4 now contains $(g_i, g_i, \square)$. This block is known as the xy-diagonal. Likewise, if $(\square, g_i, g_j)$ is in a block of ϖ_5, there exists a permutation, τ, of G, such that $\tau(g_j) = g_i$. When we apply τ to the z coordinate layer of G^3, we see that our block of ϖ_5 now contains $(\square, g_i, g_i)$. This block is known as the yz-diagonal. $\square$

Sublemma 5.1.11.4. *ϖ_6 contains the diagonal as a block.*

Subproof. By Sublemma 5.1.11.3, we can assume that ϖ_4 contains the xy-diagonal as a block, and ϖ_5 contains the yz-diagonal as a block. We use the notation $(a, a, \square) \overset{i}{\sim} (a', a', \square)$ to mean that $(a, a, x) \overset{i}{\sim} (a', a', y)$ for all

$x, y \in G$.

$$(a,a,a) \overset{4}{\sim} (a',a',a) \qquad \text{(As the } xy\text{-diagonal is a block of } \varpi_4\text{)}$$
$$(a',a',a) \overset{4}{\sim} (a',a',a') \qquad \text{(As } \varpi_4 \text{ only depends on the } x \text{ and } y \text{ coordinates)}$$
$$(a,a,a) \overset{5}{\sim} (a,a',a') \qquad \text{(As the } yz\text{-diagonal is a block of } \varpi_5\text{)}$$
$$(a,a',a') \overset{5}{\sim} (a',a',a') \qquad \text{(As } \varpi_5 \text{ only depends on the } y \text{ and } z \text{ coordinates)}$$

As $\{4,5,6\}$ is a triangle, and (a,a,a) and (a',a',a') are in the same block of ϖ_4 and in the same block of ϖ_5, they must also be in the same block of ϖ_6. As the blocks of ϖ_6 only depend on the x and z coordinates, $(a,\square,a) \overset{6}{\sim} (a',\square,a')$, and so the xz-diagonal is a block of ϖ_6. $\square$

Sublemma 5.1.11.5. *The latin squares associated with ϖ_4, ϖ_5, and ϖ_6 are identical.*

Subproof. To begin with, we show that if $(\square,a,b) \overset{5}{\sim} (\square,a',b')$ then $(a,\square,b) \overset{6}{\sim} (a',\square,b')$.

$$(\square,a,b) \overset{5}{\sim} (\square,a',b') \qquad \text{(By assumption)}$$
$$(a,a,b) \overset{5}{\sim} (a',a',b') \qquad \text{(Special case of the previous statement)}$$
$$(a,a,b) \overset{4}{\sim} (a',a',b') \qquad \text{(As the } xy\text{-diagonal is a block of } \varpi_4\text{)}$$
$$(a,a,b) \overset{6}{\sim} (a',a',b') \qquad \text{(As } \varpi_6 \text{ cannot refine } \varpi_4 \wedge \varpi_5\text{)}$$
$$(a,\square,b) \overset{6}{\sim} (a',\square,b') \qquad \text{(As } \varpi_6 \text{ only depends on the } x \text{ and } z \text{ coordinates)}$$

The converse follows a similar argument. So, $(\square,a,b) \overset{5}{\sim} (\square,a',b')$ if and only

if $(a, \square, b) \overset{6}{\sim} (a', \square, b')$. Using a cyclic argument, we can see that $(a, b, \square) \overset{4}{\sim} (a', b', \square)$ if and only if $(a, \square, b) \overset{6}{\sim} (a', \square, b')$, and that $(a, b, \square) \overset{4}{\sim} (a', b', \square)$ if and only if $(\square, a, b) \overset{5}{\sim} (\square, a', b')$. So, if we view ϖ_4, ϖ_5, and ϖ_6 as latin squares, they are identical. We express this using the notation $\varpi_4 \doteq \varpi_5 \doteq \varpi_6$. □

Sublemma 5.1.11.6. *ϖ_4, ϖ_5, and ϖ_6 are closed under transposition. That is, if (a, b) and (a', b') have the same symbol in $\mathfrak{M}_\mathfrak{i}$, then (b, a) and (b', a') also have the same symbol in $\mathfrak{M}_\mathfrak{i}$.*

Subproof. As normal, we will only show this for ϖ_4, with ϖ_5 and ϖ_6 following via a cyclic argument.

$$
\begin{aligned}
(a, b, \square) &\overset{4}{\sim} (a', b', \square) && \text{(By assumption)} \\
(a, b, a) &\overset{4}{\sim} (a', b', a') && \text{(As } \varpi_4 \text{ only depends on the } x \text{ and } y \text{ coordinates)} \\
(a, b, a) &\overset{6}{\sim} (a', b', a') && \text{(As the } xz\text{-diagonal is a block of } \varpi_6) \\
(a, b, a) &\overset{5}{\sim} (a', b', a') && \text{(As } \varpi_5 \text{ cannot refine } \varpi_4 \wedge \varpi_6) \\
(\square, b, a) &\overset{5}{\sim} (\square, b', a') && \text{(As } \varpi_5 \text{ only depends on the } y \text{ and } z \text{ coordinates)} \\
(b, a, \square) &\overset{4}{\sim} (b', a', \square) && \text{(As } \varpi_4 \doteq \varpi_5)
\end{aligned}
$$

This shows that $(a, b, \square) \overset{4}{\sim} (a', b', \square)$ if and only if $(b, a, \square) \overset{4}{\sim} (b', a', \square)$. In other words, the xy coordinates of the blocks of ϖ_4 are closed under transposition. Under a cyclic argument, the same thing happens with the blocks of ϖ_5 and ϖ_6. □

Note that this does not imply that (a, b) and (b, a) have the same symbol. For example, if we look at Example 5.1.11.1, we can see that it possesses this property. For example, $(\clubsuit, \heartsuit)$ and $(\diamondsuit, \clubsuit)$ have the same symbol, as do $(\heartsuit, \clubsuit)$ and $(\clubsuit, \diamondsuit)$, but $(\clubsuit, \heartsuit)$ and $(\heartsuit, \clubsuit)$ have different symbols.

Sublemma 5.1.11.7. *G is a group. Furthermore, the blocks of ϖ_4 are $\{(x, y, z) \in G^3 \mid xy^{-1} = g,\ g \in G\}$.*

Subproof.

$$(a, c, \square) \overset{4}{\sim} (a', c', \square) \qquad \text{(By assumption)}$$

$$(a, d, \square) \overset{4}{\sim} (a', d', \square) \qquad \text{(By assumption)}$$

$$(b, c, \square) \overset{4}{\sim} (b', c', \square) \qquad \text{(By assumption)}$$

$$(d, a, \square) \overset{4}{\sim} (d', a', \square) \qquad \text{(As blocks of } \varpi_4 \text{ are closed under transposition)}$$

$$(d, a, c) \overset{4}{\sim} (d', a', c') \qquad \text{(As } \varpi_4 \text{ only depends on the } x \text{ and } y \text{ coordinates)}$$

$$(\square, a, c) \overset{5}{\sim} (\square, a', c') \qquad \text{(As } \varpi_4 \doteq \varpi_5\text{)}$$

$$(d, a, c) \overset{5}{\sim} (d', a', c') \qquad \text{(As } \varpi_5 \text{ only depends on the } y \text{ and } z \text{ coordinates)}$$

$$(d, a, c) \overset{6}{\sim} (d', a', c') \qquad \text{(As } \varpi_6 \text{ cannot refine } \varpi_4 \wedge \varpi_5\text{)}$$

$$(d, \square, c) \overset{6}{\sim} (d', \square, c') \qquad \text{(As } \varpi_6 \text{ only depends on the } x \text{ and } z \text{ coordinates)}$$

$$(d, c, \square) \overset{4}{\sim} (d', c', \square) \qquad \text{(As } \varpi_6 \doteq \varpi_4\text{)}$$

$$(d, c, b) \overset{4}{\sim} (d', c', b') \qquad \text{(As } \varpi_4 \text{ only depends on the } x \text{ and } y \text{ coordinates)}$$

$$(\square, b, c) \overset{5}{\sim} (\square, b', c') \qquad \text{(As } \varpi_4 \doteq \varpi_5\text{)}$$

$$(\square, c, b) \overset{5}{\sim} (\square, c', b') \qquad \text{(As blocks of } \varpi_5 \text{ are closed under transposition)}$$

$$(d, c, b) \overset{5}{\sim} (d', c', b') \qquad \text{(As } \varpi_5 \text{ only depends on the } y \text{ and } z \text{ coordinates)}$$

$(d, c, b) \overset{6}{\sim} (d', c', b')$ (As ϖ_6 cannot refine $\varpi_4 \wedge \varpi_5$)

$(d, \square, b) \overset{6}{\sim} (d', \square, b')$ (As ϖ_6 only depends on the x and z coordinates)

$(d, b, \square) \overset{4}{\sim} (d', b', \square)$ (As $\varpi_6 \doteq \varpi_4$)

$(b, d, \square) \overset{4}{\sim} (b', d', \square)$ (As blocks of ϖ_4 are closed under transposition)

This shows that if $(a, c, \square) \overset{4}{\sim} (a', c', \square)$, $(a, d, \square) \overset{4}{\sim} (a', d', \square)$, and $(b, c, \square) \overset{4}{\sim} (b', c', \square)$, then $(b, d, \square) \overset{4}{\sim} (b', d', \square)$. In terms of the latin square representation of ϖ_4, this is the quadrangle criterion.

Now, by Theorem 5.1.4, $\mathfrak{M}_4$ is a group table. Without loss of generality, we can assume that the entry in the diagonal is the identity of this group. Furthermore, we can take the first row and the first column to be the header and the sideline. If we consider the sideline to be $g_1, \ldots, g_n$, where $n = |G|$, then, as the identity element fills the diagonal, the header is $g_1^{-1}, \ldots, g_n^{-1}$. Therefore this table is constant under the function xy^{-1}. Hence the blocks of ϖ_4 are $\{(x, y, z) \in G^3 \mid xy^{-1} = g,\ g \in G\}$. Because of the symmetry of $M(K_4)$, the blocks of ϖ_5 are $\{(x, y, z) \in G^3 \mid yz^{-1} = g,\ g \in G\}$ and the blocks of ϖ_6 are $\{(x, y, z) \in G^3 \mid zx^{-1} = g,\ g \in G\}$. $\square$

Note that in $\mathfrak{M}_6$, we pick the header (as opposed to the sideline) to be $g_1, \ldots, g_n$. This is for purely aesthetic reasons, and we can freely switch between f and f^{-1}, where f is a group function. We will make further use of this ability.

The proof of the proposition follows immediately from Sublemma 5.1.11.7.$\square$

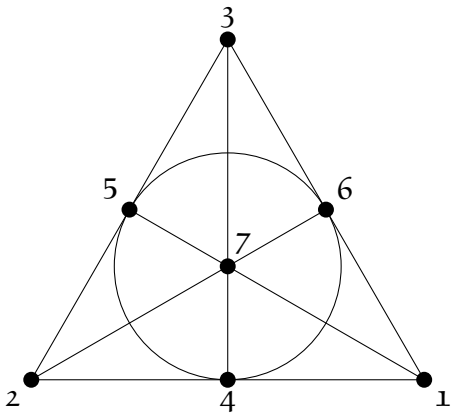

Figure 5.3: F_7 as used in the proof of Proposition 5.2.1

5.2 Fano

The work done in this section is based on work done by Matúš [19].

Take a p-representation, ϖ, of F_7, as labelled in Figure 5.3. Transform this p-representation so that it is in coordinate form with respect to the basis $\{1, 2, 3\}$. Delete ϖ_7 to get a p-representation of $M(K_4)$. By Proposition 5.1.11, we know that this p-representation must be group-induced. We now study ϖ_7.

Proposition 5.2.1. *Let G be a group that defines a p-representation of the Fano matroid. Then G is a power of $\mathbb{Z}_2$.*

Proof. Let ϖ be a p-representation of the Fano matroid in coordinate form with respect to $\{1, 2, 3\}$ and let $(G, \cdot)$ be a finite group defining the six partitions of ϖ as in $M(K_4)$. ϖ_7, the seventh partition of ϖ, will be treated as an equivalence, $\overset{7}{\sim}$, on G^3. So, if $(x, y, z) \overset{7}{\sim} (x', y', z')$, then (x, y, z) and

(x', y', z') are in the same block of ϖ_7. Let e be the identity element of $(G, \cdot)$, and let a, b, c be arbitrary elements of G.

$$(a,a,e) \overset{3}{\sim} (e,e,e) \qquad \text{(As } \varpi_3 \text{ only depends on the } z \text{ coordinate)}$$

$$(a,a,e) \overset{4}{\sim} (e,e,e) \qquad \text{(As blocks of } \varpi_4 \text{ are constant under } xy^{-1})$$

$$(a,a,e) \overset{7}{\sim} (e,e,e) \qquad \text{(As } \varpi_7 \text{ cannot refine } \varpi_3 \wedge \varpi_4)$$

$$(e,e,e) \overset{1}{\sim} (e,b,b) \qquad \text{(As } \varpi_1 \text{ only depends on the } x \text{ coordinate)}$$

$$(e,e,e) \overset{5}{\sim} (e,b,b) \qquad \text{(As blocks of } \varpi_5 \text{ are constant under } yz^{-1})$$

$$(e,e,e) \overset{7}{\sim} (e,b,b) \qquad \text{(As } \varpi_7 \text{ cannot refine } \varpi_1 \wedge \varpi_5)$$

$$(e,b,b) \overset{2}{\sim} (c,b,bc) \qquad \text{(As } \varpi_2 \text{ only depends on the } y \text{ coordinate)}$$

$$(e,b,b) \overset{6}{\sim} (c,b,bc) \qquad \text{(As blocks of } \varpi_6 \text{ are constant under } zx^{-1})$$

$$(e,b,b) \overset{7}{\sim} (c,b,bc) \qquad \text{(As } \varpi_7 \text{ cannot refine } \varpi_2 \wedge \varpi_6)$$

$$(a,a,e) \overset{7}{\sim} (c,b,bc) \qquad \text{(As } \overset{7}{\sim} \text{ is transitive)}$$

$$(a,a,e) \overset{7}{\sim} (a,a,a^2) \qquad \text{(Let } b = a \text{ and } c = a)$$

$$(a,a,e) \overset{4}{\sim} (a,a,a^2) \qquad \text{(As blocks of } \varpi_4 \text{ are constant under } xy^{-1})$$

$$(a,a,e) \overset{3}{\sim} (a,a,a^2) \qquad \text{(As } \varpi_3 \text{ cannot refine } \varpi_4 \wedge \varpi_7)$$

But ϖ_3 is completely defined by the z coordinate layer. So if (a, a, a^2) and (a, a, e) are in the same block of ϖ_3, then $a^2 = e$, and, as a is an arbitrary element of G, $g^2 = e$ for all $g \in G$. It follows from Theorem 5.1.9 of Scott [23] that the group must be a power of $\mathbb{Z}_2$. □

As $\mathbb{Z}_2^n$ is abelian, we will use additive notation.

Proposition 5.2.2. *The blocks of ϖ_7 are defined by $x+y+z$. Or, $a+b+c = a'+b'+c'$ if and only if $(a,b,c) \overset{7}{\sim} (a',b',c')$.*

Proof. To begin with, we show that if $(a,b,c) \overset{7}{\sim} (a',b',c')$, then $a+b+c = a'+b'+c'$.

$$
\begin{aligned}
(a,b',b+c-b') &\overset{1}{\sim} (a,b,c) && \text{(As } \varpi_1 \text{ only depends on the } x \text{ coordinate)}\\
(a,b',b+c-b') &\overset{5}{\sim} (a,b,c) && \text{(As blocks of } \varpi_5 \text{ are constant under } y+z)\\
(a,b',b+c-b') &\overset{7}{\sim} (a,b,c) && \text{(As } \varpi_7 \text{ cannot refine } \varpi_1 \wedge \varpi_5)\\
(a,b,c) &\overset{7}{\sim} (a',b',c') && \text{(By assumption)}\\
(a,b',b+c-b') &\overset{7}{\sim} (a',b',c') && \text{(As } \overset{7}{\sim} \text{ is transitive)}\\
(a,b',b+c-b') &\overset{2}{\sim} (a',b',c') && \text{(As } \varpi_2 \text{ only depends on the } y \text{ coordinate)}\\
(a,b',b+c-b') &\overset{6}{\sim} (a',b',c') && \text{(As } \varpi_6 \text{ cannot refine } \varpi_2 \wedge \varpi_7)\\
a+b+c-b' &= a'+c' && \text{(As blocks of } \varpi_6 \text{ are constant under } x+z)\\
a+b+c &= a'+b'+c'
\end{aligned}
$$

Conversely, let $|G| = n$. Then ϖ_7 has n blocks, all of cardinality n^2. Let $\mathfrak{b}$ be one of the blocks of ϖ_7, and arbitrarily pick (a,b,c) from $\mathfrak{b}$. Let (a',b',c') be any other triple from $\mathfrak{b}$. As (a,b,c) and (a',b',c') are in the same block of ϖ_7, $a+b+c = a'+b'+c' = k$. As we chose (a',b',c') arbitrarily from $\mathfrak{b}$, this statement is true for all triples in $\mathfrak{b}$. Therefore $\mathfrak{b} \subseteq \{(x,y,z) \mid x+y+z = k\}$. Furthermore, $|\{(x,y,z) \mid x+y+z = k\}| = n^2$, as any choice of x and y determines what z must be. Therefore $\mathfrak{b} = \{(x,y,z) \mid x+y+z = k\}$, and

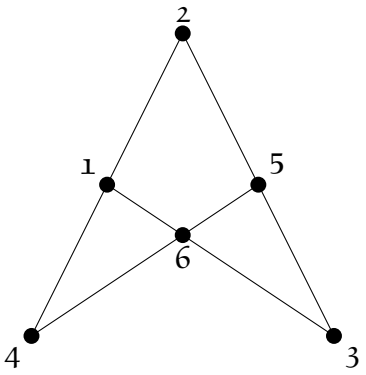

Figure 5.4: $M(K_4)$ labelled for Example 5.3.1

this is true for all choices of $\mathfrak{b} \in \varpi_7$. □

5.3 non-Fano

The work done in this section is based on work done by Matúš [19].

We wish to apply a permutation to G^3, and we are interested in how this will affect our functions that define blocks of a partition of G^3. Let σ be a permutation of G^3. Then $(a, b, c) \sim (a', b', c')$ if and only if $\sigma(a, b, c) \sim \sigma(a', b', c')$. Let g be a function on G^3 such that $g(a, b, c) = g(a', b', c')$ if and only if $(a, b, c) \sim (a', b', c')$. Then there exists some other function on G^3, g', such that $g'(\sigma(a, b, c)) = g(a, b, c)$. Therefore $g' = g \circ \sigma^{-1}$.

Let f be a function from G^3 to G that defines the blocks of a partition of G^3. Recall from the proof of Proposition 5.1.11 that we are able to freely switch between f and f^{-1}, and this does not affect the blocks of our partition.

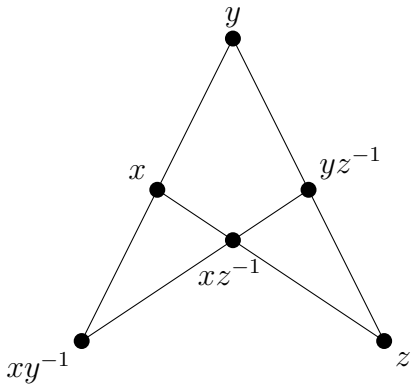

Figure 5.5: Functions defining blocks before application of σ

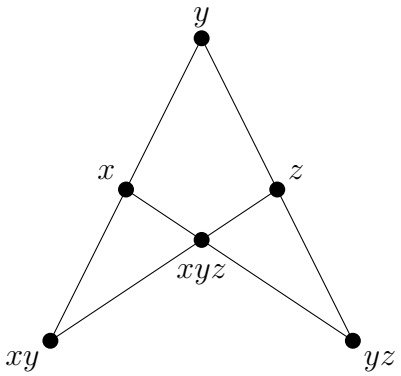

Figure 5.6: Functions defining blocks after application of σ

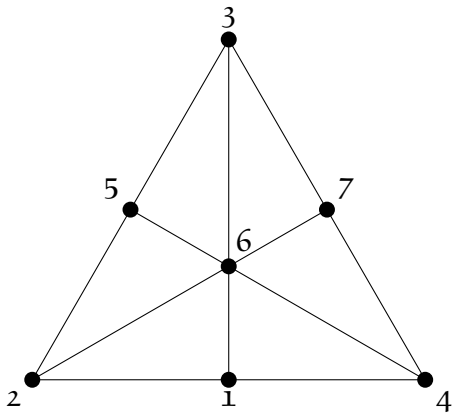

Figure 5.7: F_7^- for Proposition 5.3.2

Example 5.3.1. Consider a p-representation of $M(K_4)$, labelled as in Figure 5.4, with blocks defined by functions as shown in Figure 5.5. Let ς be a permutation of G^3 such that $\varsigma(x, y, z) = (x, y^{-1}, yz^{-1})$. Then the blocks of our p-representation are defined by the functions shown in Figure 5.6. Note that we sometimes pick the inverse function for aesthetic reasons. $\Diamond$

Take a p-representation, ϖ, of F_7^-, as labelled in Figure 5.7. Transform this p-representation so that it is in coordinate form with respect to the basis $\{1, 2, 3\}$. Delete ϖ_7 to get a p-representation of $M(K_4)$. Apply ς as in Example 5.3.1 to get a p-representation of $M(K_4)$ that is coordinate form with respect to the basis $\{1, 2, 5\}$. By Proposition 5.1.11, we know that this p-representation must be group-induced. We now study ϖ_7.

Proposition 5.3.2. *Let G be a group that defines a p-representation of the non-Fano matroid. Then G is abelian.*

Proof. Let ϖ be a p-representation of the non-Fano matroid in coordinate form with respect to $\{1, 2, 5\}$ and let $(G, \cdot)$ be a finite group defining the six partitions of ϖ as in Example 5.3.1. ϖ_7, the seventh partition of ϖ, will be treated as an equivalence, $\overset{7}{\sim}$, on G^3. Let e be the identity element of $(G, \cdot)$, and let a and b be arbitrary elements of G.

$$(e, e, e) \overset{2}{\sim} (a^{-1}b^{-1}, e, ba)$$

(As ϖ_2 only depends on the y coordinate)

$$(e, e, e) \overset{6}{\sim} (a^{-1}b^{-1}, e, ba)$$

(As blocks of ϖ_6 are constant under xyz)

$$(e, e, e) \overset{7}{\sim} (a^{-1}b^{-1}, e, ba) \qquad \text{(As } \varpi_7 \text{ cannot refine } \varpi_2 \wedge \varpi_6\text{)}$$

$$(a^{-1}b^{-1}, e, ba) \overset{3}{\sim} (a^{-1}b^{-2}, b, a) \quad \text{(As blocks of } \varpi_3 \text{ are constant under } yz\text{)}$$

$$(a^{-1}b^{-1}, e, ba) \overset{4}{\sim} (a^{-1}b^{-2}, b, a) \quad \text{(As blocks of } \varpi_4 \text{ are constant under } xy\text{)}$$

$$(a^{-1}b^{-1}, e, ba) \overset{7}{\sim} (a^{-1}b^{-2}, b, a) \qquad \text{(As } \varpi_7 \text{ cannot refine } \varpi_3 \wedge \varpi_4\text{)}$$

$$(e, e, e) \overset{3}{\sim} (b^{-1}, b, b^{-1}) \quad \text{(As blocks of } \varpi_3 \text{ are constant under } yz\text{)}$$

$$(e, e, e) \overset{4}{\sim} (b^{-1}, b, b^{-1}) \quad \text{(As blocks of } \varpi_4 \text{ are constant under } xy\text{)}$$

$$(e, e, e) \overset{7}{\sim} (b^{-1}, b, b^{-1}) \qquad \text{(As } \varpi_7 \text{ cannot refine } \varpi_3 \wedge \varpi_4\text{)}$$

$$(b^{-1}, b, b^{-1}) \overset{2}{\sim} (b^{-1}a^{-1}b^{-1}, b, a)$$

(As ϖ_2 only depends on the y coordinate)

$$(b^{-1}, b, b^{-1}) \overset{6}{\sim} (b^{-1}a^{-1}b^{-1}, b, a)$$

(As blocks of ϖ_6 are constant under xyz)

$$(b^{-1}, b, b^{-1}) \overset{7}{\sim} (b^{-1}a^{-1}b^{-1}, b, a) \qquad \text{(As } \varpi_7 \text{ cannot refine } \varpi_2 \wedge \varpi_6\text{)}$$

$(b^{-1}a^{-1}b^{-1}, b, a) \overset{7}{\sim} (a^{-1}b^{-2}, b, a)$ (As $\overset{7}{\sim}$ is transitive)

$(b^{-1}a^{-1}b^{-1}, b, a) \overset{3}{\sim} (a^{-1}b^{-2}, b, a)$ (As blocks of ϖ_3 are constant under yz)

$(b^{-1}a^{-1}b^{-1}, b, a) \overset{4}{\sim} (a^{-1}b^{-2}, b, a)$ (As ϖ_4 cannot refine $\varpi_3 \wedge \varpi_7$)

Now, we know that blocks of ϖ_4 are constant under the function xy. Hence

$$b^{-1}a^{-1}b^{-1} \cdot b = a^{-1}b^{-1}b^{-1} \cdot b$$

$$b^{-1}a^{-1} = a^{-1}b^{-1}$$

Hence $\cdot$ is commutative, and therefore G is abelian. □

As G is abelian, we will use additive notation.

Proposition 5.3.3. *The blocks of ϖ_7 are defined by $x + 2y + z$. That is, $a + 2b + c = a' + 2b' + c'$ if and only if $(a, b, c) \overset{7}{\sim} (a', b', c')$.*

Proof. To begin with, we show that if $(a, b, c) \overset{7}{\sim} (a', b', c')$, then $a + 2b + c = a' + 2b' + c'$.

$(a, b, c) \overset{7}{\sim} (a', b', c')$ (By assumption)

$(a', b', c') \overset{2}{\sim} (a + b - b', b', a' + b' + c' - a - b)$

(As ϖ_2 only depends on the y coordinate)

$(a', b', c') \overset{6}{\sim} (a + b - b', b', a' + b' + c' - a - b)$

(As blocks of ϖ_6 are constant under $x + y + z$)

$$(a', b', c') \overset{7}{\sim} (a + b - b', b', a' + b' + c' - a - b)$$

(As ϖ_7 cannot refine $\varpi_2 \wedge \varpi_6$)

$$(a, b, c) \overset{7}{\sim} (a + b - b', b', a' + b' + c' - a - b)$$

(As $\overset{7}{\sim}$ is an equivalence relation)

$$(a, b, c) \overset{4}{\sim} (a + b - b', b', a' + b' + c' - a - b)$$

(As blocks of ϖ_4 are constant under $x + y$)

$$(a, b, c) \overset{3}{\sim} (a + b - b', b', a' + b' + c' - a - b)$$

(As ϖ_3 cannot refine $\varpi_4 \wedge \varpi_7$)

$$b + c = b' + a' + b' + c' - a - b$$

(As blocks of ϖ_3 are constant under $y + z$)

$$a + 2b + c = a' + 2b' + c'$$

Conversely, let $|G| = n$. Then ϖ_7 has n blocks, all of cardinality n^2. Let $\mathfrak{b}$ be one of the blocks of ϖ_7, and arbitrarily pick (a, b, c) from $\mathfrak{b}$. Let (a', b', c') be any other triple from $\mathfrak{b}$. As (a, b, c) and (a', b', c') are in the same block of ϖ_7, $a+2b+c = a'+2b'+c' = k$. As we chose (a', b', c') arbitrarily from $\mathfrak{b}$, this statement is true for all triples in $\mathfrak{b}$. Therefore $\mathfrak{b} \subseteq \{(x, y, z) \mid x + 2y + z = k\}$. Furthermore, $|\{(x, y, z) \mid x + 2y + z = k\}| = n^2$, as any choice of x and y determines what z must be. Therefore $\mathfrak{b} = \{(x, y, z) \mid x + 2y + z = k\}$, and this argument works for all choices of $\mathfrak{b} \in \varpi_7$. □

Proposition 5.3.4. *The group must have odd order.*

Proof. Assume G has even order. Then it follows from Theorem 11.6 of

Fraleigh [9] that there are elements y and y' of G such that y is not equal to y', but $y + y = y' + y'$. Then the triples (x, y, z) and (x, y', z) belong to the same block of ϖ_1, because the blocks of ϖ_1 are defined by the x coordinate. Furthermore, they belong to the same block of ϖ_5, as the blocks of ϖ_5 are defined by the z coordinate. As $\{1, 5, 7\}$ is a basis, they must also belong to different blocks of ϖ_7. Hence, as Proposition 5.3.3 shows that the blocks of ϖ_7 are defined by $x+y+y+z$, it follows that $y+y \neq y'+y'$, a contradiction to our definition of y. Hence G cannot have even order, so it must have odd order. □

5.4 Other Results

5.4.1 Representable Matroids

It is well known ([18] for instance) that all representable matroids are also p-representable. A natural question to ask is which representable matroids also have a group-induced p-representation. In this section, we show that all matroids representable over a prime field have a group-induced p-representation.

Definition 5.4.1. Let M be a matrix of rank r. If $M = [I_r|A]$, where I_r is the identity matrix, then M is said to be in ***standard form***.

Proposition 5.4.2. *Every matroid representable over a prime field has a group-induced p-representation.*

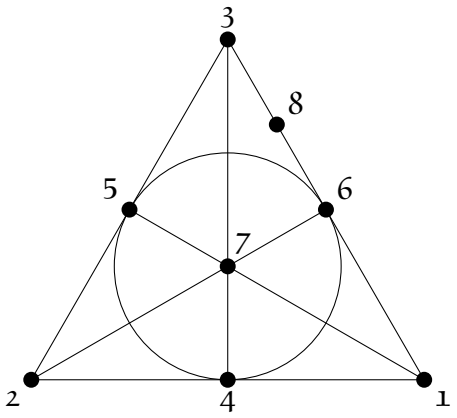

Figure 5.8: F_{7^+} as used in Example 5.4.3

Proof. Let M be a matroid that is representable over a prime field and let G be the additive group of said field. Then by results in Section 2.2 of Oxley [20], there exists a matrix in standard form such that $M = M[I_r|A]$. For $i \in \{1, \ldots, r\}$, let the blocks of ϖ_i be $\{(x_1, \ldots, x_r) \in G^r \mid x_i = g,\ g \in G\}$. The remaining blocks of the p-representation are generated from elements of A. Let $\mathbf{v} = [v_1 \cdots v_r]^T$ be an element from A. Then the blocks of $\varpi_{\mathbf{v}}$ are $\{(x_1, \ldots, x_r) \in G^r \mid \sum v_i x_i = g,\ g \in G\}$, where $v_i x_i = \underbrace{x_i + \cdots + x_i}_{v_i \text{times}}$. This is obviously a p-representation of M. □

This construction fails for matroids not representable over a prime field, as multiplication is not just repeated addition in such fields. In fact, matroids not representable over a prime field do not need to have a group-induced p-representation, as the next example shows.

Example 5.4.3. Let F_{7^+} be the matroid shown in Figure 5.8. Note that F_{7^+} is only representable over $GF(2^n)$, where $n \geq 2$. So F_{7^+} is not representable

over any prime field.

Take a p-representation, ϖ, of F_{7^+}, partitioning G^3, where G is some finite set. Transform this p-representation so that it is in coordinate form with respect to the basis $\{1, 2, 3\}$. Delete ϖ_8 to get a p-representation of F_7. By Proposition 5.2.1, we know that this p-representation is group induced, and the group that induces this p-representation is $\mathbb{Z}_2^n$, for some $n \in \mathbb{Z}^+ \cup \{0\}$. Also, we find that the blocks of ϖ_1 are defined by x, the blocks of ϖ_3 are defined by z and the blocks of ϖ_6 are defined by $x + z$.

Consider ϖ_8. In particular, consider the function that defines blocks of ϖ_8. As it cannot refine $\varpi_1 \cap \varpi_6$, it can only have x and z as variables. Since $x + z$ is taken by ϖ_6, it cannot be this. Hence, it must have extra terms. If we add on more variables, say $x + x + z$, as the order of every element in $\mathbb{Z}_2^n$ is two, $x + x = 0$, and we are just left with z, which implies that $\varpi_8 = \varpi_3$, a contradiction. So we must add some constant, k, from the group. Hence the blocks of ϖ_8 are defined by $x + z + k$, where $k \neq 0$. But then the meet partition between 6 and 8 will have $|G|$ blocks, when it needs to have $|G|^2$ blocks. Hence there can be no function that defines blocks of ϖ_8, and so F_{7^+} has no group-induced p-representations. $\Diamond$

5.4.2 Uniqueness

Another natural question is whether functions defining blocks of a p-representation are unique or not. The following example answers this ques-

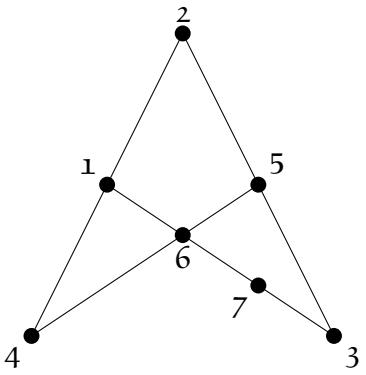

Figure 5.9: Labelling of O_7 as used in Example 5.4.4

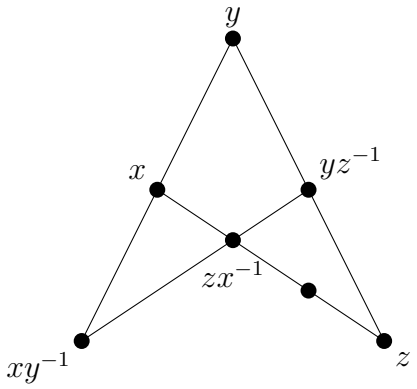

Figure 5.10: Functions defining blocks of O_7

tion.

Example 5.4.4. Let O_7 be the matroid displayed in Figure 5.9, with blocks defined by functions as shown in Figure 5.10. Let $G = \mathbb{Z}_5$. Then the blocks of ϖ_7 can be defined by either xz or x^2z. It is not too hard to see that these two p-representations are not equivalent. ◊

So, the functions defining blocks of group-induced p-representable matroids do not need to be group induced.

5.4.3 Uniform Matroids

We now consider one last family of matroids.

It is well known, see [33] for example, that $U_{r,n}$ is secret sharing, and that one needs $n-r$ mutually orthogonal latin r-hypercubes of order $|S|$ in order to construct a secret sharing matrix for $U_{r,n}$ over a set S. To construct such a matrix, we take all possible $|S|$-tuples from S and assign them to the first $|S|$ columns of our matrix. This defines a coordinate system, with which we assign coordinates to our latin hypercubes, and place the entries from the hypercubes in the obvious place in the matrix, until we have the n rows required.

For example, if we want to construct a secret sharing matrix for $U_{2,4}$ over the set $S = \{0, 1, a, b\}$, then we will need two mutually orthogonal latin squares, as given here.

	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

	0	1	a	b
0	0	a	b	1
1	1	b	a	0
a	a	0	1	b
b	b	1	0	a

Then the secret sharing matrix is as follows.

$$\left[\begin{array}{cccc}
0 & 0 & 0 & 0 \\
0 & 1 & 1 & a \\
0 & a & a & b \\
0 & b & b & 1 \\
1 & 0 & 1 & 1 \\
1 & 1 & 0 & b \\
1 & a & b & a \\
1 & b & a & 0 \\
a & 0 & a & a \\
a & 1 & b & 0 \\
a & a & 0 & 1 \\
a & b & 1 & b \\
b & 0 & b & b \\
b & 1 & a & 1 \\
b & a & 1 & 0 \\
b & b & 0 & a
\end{array}\right]$$

Note that this is not a group-induced p-representation, as the second latin square is not a group table, as it has four elements, but is not commutative.

Chapter 6

Open Questions

There are many open questions remaining in the realm of secret sharing matroids. We will give a small sample of them here.

These first two questions are the natural questions posed by matroid structure theorists, and neither has been answered. The first question was posed by Matúš [18] in the language of p-representable matroids.

Question 1. Are secret sharing matroids closed under duality?

Question 2. Are secret sharing matroids minor closed?

The largest known class of matroids that is contained within secret sharing is multilinear matroids, as defined by Simonis and Ashikhmin [31]. This class has more structure than general secret sharing matroids, but it is unknown whether there exist secret sharing matroids that are not multilinear. This first question was posed in [31]. The second question is deliberately vague.

Question 3. Are all secret sharing matroids multilinear?

Question 4. Is there a naturally defined class of matroids that is identical to secret sharing matroids, yet has more structure?

In this thesis, we often consider word functions from G^k to G, where G is a group.

Question 5. If f is a word function from G^k to G, when are the sets $\{f(g_1, \ldots, g_k) = g \mid g \in G\}$ equicardinal? If $f_1, \ldots, f_n$ is a sequence of such equations, when do the partitions $\{(f_i(g_1, \ldots, g_k) = g \mid g \in G\}$ for $i = 1, \ldots, n$ induce a p-representation of a matroid?

Bibliography

[1] Archer, S. *Near Varieties and Extremal Matroids.* PhD thesis, Victoria University of Wellington, 2005.

[2] Bixby, R. A simple theorem on 3-connectivity. *Linear Algebra and Its Applications 45* (1982), 123–126.

[3] Blakley, G. Safeguarding cryptographic keys. In *Proceedings of the AFIPS 1979 National Computer Conference* (1979), vol. 48, pp. 313 – 317.

[4] Brickell, E., and Davenport, D. On the classification of ideal secret sharing schemes. *Journal of Cryptology 4*, 2 (1991), 123 – 134.

[5] Brylawski, T., and Kelly, D. *Matroids and combinatorial geometries.* Dept. of Mathematics, University of North Carolina at Chapel Hill, 1980.

[6] Dénes, J., and Keedwell, A. *Latin squares and their applications.* Akadémiai Kiadó, 1974.

[7] Ding, G., Oporowski, B., Oxley, J., and Vertigan, D. Unavoidable minors of large 3-connected matroids. *J. Comb. Theory Ser. B 71*, 2 (1997), 244–293.

[8] Euler, L. Recherches sur une nouvelle espece de quarrés magiques, verh. *Zeeuwsch Gennot. Weten Vliss 9* (1782), 85–239.

[9] Fraleigh, J. *A first course in abstract algebra, seventh edition.* Pearson Education Inc., 2003.

[10] Frolov, M. *Recherches sur les permutations carrées.* Ch. Delagrave, 1890.

[11] Geelen, J., Oxley, J., Vertigan, D., and Whittle, G. Totally free expansions of matroids. *J. Combin. Theory Ser. B 84*, 1 (2002), 130–179.

[12] Heller, I. On linear systems with integral valued solutions. *Pacific J. Math 7* (1957), 1351–1364.

[13] Kahn, J. On the uniqueness of matroid representations over $GF(4)$. *Bull. London Math. Soc 20*, 1 (1988), 5–10.

[14] Kung, J. Combinatorial geometries representable over $GF(3)$ and $GF(q)$. I. The number of points. *Discrete and Computational Geometry 5*, 1 (1990), 83–95.

[15] Kung, J. Extremal matroid theory. *Graph Structure Theory, Amer. Math. Soc., Providence, RI* (1993), 21–62.

[16] Kung, J., and Oxley, J. Combinatorial geometries representable over $GF(3)$ and $GF(q)$. II. Dowling geometries. *Graphs and Combinatorics 4*, 1 (1988), 323–332.

[17] Liu, C. *Introduction to Combinatorial Mathematics*. McGraw-Hill, New York, 1968.

[18] Matúš, F. Ascending and descending conditional independence relations. In *Transactions of the 11th Prague Conference on Information Theory, Statistical Decision Functions and Random Processes, Vol. B* (1992), pp. 189 – 200.

[19] Matúš, F. Matroid representations by partitions. *Discrete Mathematics 203*, 1 (1999), 169 – 194.

[20] Oxley, J. *Matroid theory, second edition*. Oxford University Press, USA, 2011.

[21] Oxley, J., Vertigan, D., and Whittle, G. On maximum-sized near-regular and $\sqrt[6]{1}$-matroids. *Graphs and Combinatorics 14*, 2 (1998), 163–179.

[22] Pendavingh, R., and Van Zwam, S. Lifts of matroid representations over partial fields. *Journal of Combinatorial Theory, Series B 100*, 1 (2010), 36–67.

[23] Scott, W. *Group theory*. Prentice Hall, 1964.

[24] Semple, C. Matroid representation over partial fields. Master's thesis, Victoria University of Wellington, 1995.

[25] Semple, C. *k-Regular Matroids.* PhD thesis, Victoria University of Wellington, 1998.

[26] Semple, C. On maximum-sized k-regular matroids. *Graphs Combin. 15*, 4 (1999), 441–462.

[27] Semple, C., and Whittle, G. Partial fields and matroid representation. *Advances in Applied Mathematics 17* (1996), 184–208.

[28] Seymour, P. On minors of non-binary matroids. *Combinatorica 1*, 4 (1981), 387–394.

[29] Seymour, P. On secret-sharing matroids. *Journal of Combinatorial Theory Series B 56*, 1 (1992), 69 – 73.

[30] Shamir, A. How to share a secret. *Communications of the ACM 22*, 11 (1979), 612 – 613.

[31] Simonis, J., and Ashikhmin, A. Almost affine codes. *Designs, Codes and Cryptography 14*, 2 (1998), 179 – 197.

[32] Stein, W., et al. *Sage Mathematics Software (Version 4.6.1).* The Sage Development Team, 2011. `http://www.sagemath.org`.

[33] Stinson, D. An explication of secret sharing schemes. *Designs, Codes and Cryptography 2*, 4 (1992), 357 – 390.

[34] Van Zwam, S. *Partial Fields in Matroid Theory.* PhD thesis, Technische Universiteit Eindhoven, 2009.

[35] Whittle, G. Stabilizers of classes of representable matroids. *Journal of Combinatorial Theory, Series B 77*, 1 (1999), 39–72.

[36] Wolfram Research, Inc. *Mathematica, Version 7.0.* Champaign, Illinois, 2008.

[37] Wu, Z. On the number of spikes over finite fields. *Discrete mathematics 265*, 1-3 (2003), 261–296.

Index