Identically Self-Dual Matroids

Alexander Giles Budge Perrott

VICTORIA UNIVERSITY OF WELLINGTON

Te Whare Wānanga o te Ūpoko o te Ika a Māui

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
2017

Abstract

In this thesis we focus on identically self-dual matroids and their minors. We show that every sparse paving matroid is a minor of an identically self-dual sparse paving matroid. The same result is true if the property sparse paving is replaced with the property of representability and more specifically, $\mathbb{F}$-representable where $\mathbb{F}$ is a field of characteristic 2, an algebraically closed field, or equal to $GF(p)$ for a prime $p = 3$ (mod 4).

We extend a result of Lindström [11] saying that no identically self-dual matroid is regular and simple. We assert that this also applies to all matroids which can be obtained by contracting an identically self-dual matroid.

Finally, we present a characterisation of identically self-dual frame matroids and prove that the class of self-dual matroids is not axiomatisable.

Acknowledgements

I would like to thank Dr. Dillon Mayhew for supervising this thesis and offering his kind support and wisdom to my academic development over the past year. He should also be credited for his excellent teaching of the matroid theory paper, MATH432, without the inspiration of which it is unlikely I would have discovered my interest in combinatorics.

I also need to thank fellow student, Liam Jolliffe, for enduring listening to many half-baked ideas and helping unravel logical falsehoods which threatened to undermine matroid theory and, in some instances, the entirety of mathematics. I am also thankful for his perceptive proofreading of this thesis and his contagious curiosity for mathematics which made studying more enjoyable.

Thanks also go to my family and friends for their continued support of my studies. In particular I want to thank my mother, Claire Budge, for proofreading the literacy of the thesis and for providing encouragement and understanding at times of difficulty.

Finally, I would like to thank Victoria University for the funding provided by the Victoria Master's scholarship which made this thesis possible.

Contents

List of Figures

Chapter 1

Introduction

Identically self-dual matroids (abbreviated ISD) are matroids which are invariant under duality. Thus identically self-dual matroids are equal to their own duals, $M = M^*$. This is in contrast to self-dual matroids, which are equal to their duals, but only up to isomorphism. There are considerable restrictions on the structure of an ISD matroid M; Every basis of M is the complement of another basis and circuits and hyperplanes are complements of each other. Consequently, identically self-dual matroids are relatively uncommon, but we do have many simple examples. Some infinite families of identically self-dual matroids include; tipless binary spikes of even rank, the set of uniform matroids $U_{r,2r}$, and sparse paving matroids with a single pair of disjoint circuit hyperplanes which partition the ground set. An example of each of these types of ISD matroid is shown in Figure 1.1.

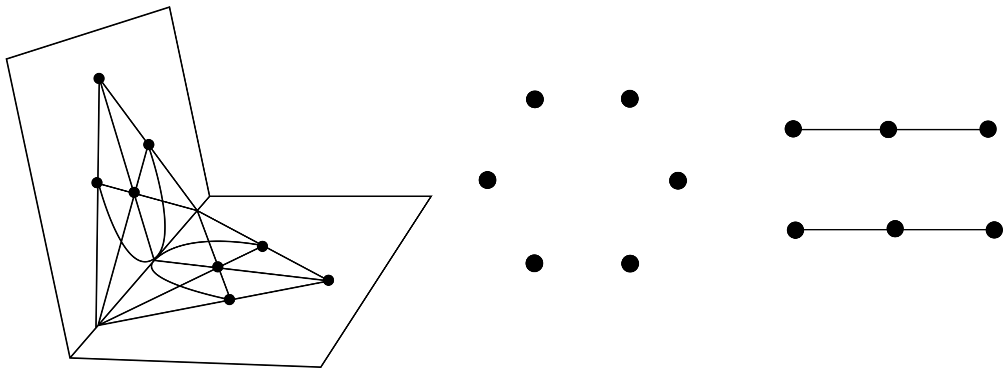

Figure 1.1: Three identically self-dual matroids; $AG(3,2), U_{3,6}$ and R_6.

Identically self-dual matroids have not been studied in great detail from a matroid perspective. These same structures more commonly arise in design theory and in coding theory where a self-dual code is equivalent to an identically self-dual matroid, an unfortunate difference in terminology. Self-dual codes have a long history as noted in the summary article by Rains and Sloane [17]. Though much of this is difficult to apply to ISD matroids, coding literature is useful in proving the results in this chapter and we also use coding techniques in the chapter on representable matroids.

In this thesis, research into identically self-dual matroids and their minors was initiated by their connection to projective planes. In the next section we introduce projective planes and illustrate how they are related to identically self-dual matroids. Subsequently, we will give an overview of the material presented in the remainder of the thesis.

1.1 Projective Planes

Projective geometry originated from perspective drawings and is not concerned with distance, rather how lines and points intersect. Projective planes are simply a specific type of projective geometry. Their origin is hard to place, but they were mentioned as early as 1904 by Veblen [21].

The concept of a projective plane is not overly complex. We take a set of points P and a set of lines L consisting of subsets of points. We say that a point p *lies on*, is *contained* in, or is *incident* with line l if $p \in l$. The pair (P,L) is a *projective plane* if it obeys the following properties:

1. For any pair of distinct lines there is a unique point that lies in their intersection.

2. For any pair of distinct points there is a unique line containing both points.

3. There exists a set of four points no three of which are collinear (a quadrangle).

Projective planes can also be viewed as an extension of affine planes. An *affine plane* must fulfill all but the first property of the three above properties. That is, an affine plane can contain parallel lines. Any affine plane can be extended to a projective plane by including a unique point for each parallel class of the plane which is added to every line in the class. One new line is added containing the additional points. It is easily verified that every pair of lines now has a unique point of intersection so this method will result in a projective plane. The Euclidean plane is one example of an affine plane which can be extended to a projective plane. Augmenting this plane by the line at infinity will result in the extended Euclidean plane which is also called the real projective plane.

As we have now seen, there are projective planes of infinite size like the extended Euclidean plane, but for the purposes of this thesis we will be focusing on those of finite size such as the planes in Figures 1.2 and 1.3. It can be observed that they fulfill the three properties described earlier and that some of the lines have to represented by curves as neither of these projective planes can be drawn in Euclidian space with straight lines.

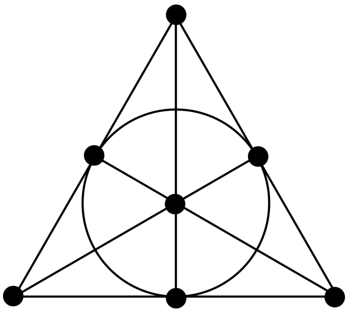

Figure 1.2: The projective plane of order 2 (Fano plane).

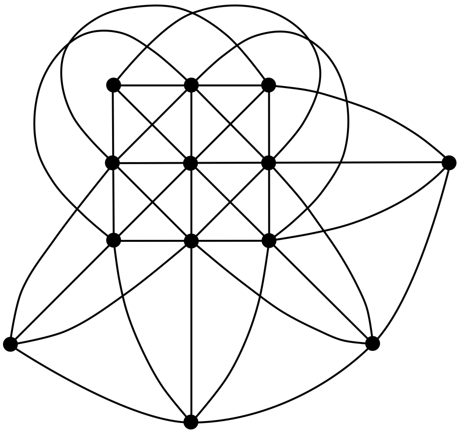

Figure 1.3: The projective plane of order 3.

It may seem that discrete planes are less applicable to physical problems than their infinite counterparts, but they are closely related to finite designs and coding theory, which are both well suited to finite constructions. In addition, there are benefits to studying finite planes as they are more tractable for computer work and they have interesting structural properties. One such property of finite projective planes allows us to characterise them by the number of points and lines in the plane. Lemma 1.1.1 shows that we are justified in describing finite projective planes this way.

Lemma 1.1.1. *In a finite projective plane each line contains the same number of points and furthermore this is equal to the number of lines containing each point.*

Proof. First we prove that for any pair of lines l_1, l_2 in the plane there is a point x which is not contained in either line. Assume that this fails and that there are no points which are not incident with l_1 or l_2. Let p be the point of intersection of l_1 and l_2 and note that since the plane contains four points, no three of which are collinear, each of the lines must contain at least two points other than p. We let l_1 contain points a and a' and l_2 contain b and b'. Any pair of points is contained in a line of the plane so there is a line l_3 containing a and b and a line l_4 containing a' and b'. We know the lines l_3 and l_4 intersect l_1 and l_2 in the points $\{a, a', b, b'\}$ but they must also intersect each other in an element x which is not incident with l_1 or l_2. This contradicts our assumption, therefore for any pair of lines we can always find a point which is not incident with either line.

Consider two lines l_1 and l_2 and a point x which is not contained in either line. Let l_1 contain k points and note that for any point on l_1 there is another line which contains this point and x. These k lines must all be distinct because l_1 is the only line which contains more than one point of l_1. Thus there must be at least k lines containing x. Now assume that x is incident with more than k lines. Each of these lines must intersect l_1 in a distinct point so l_1 must contain more than k points contrary to our assumption. Therefore the number of points incident with l_1 must be equal to the number of lines incident with $x \notin l_1$. The same argument can be applied to l_2 and x so l_1 and l_2 must contain the same number of points. This is true of any pair of lines so all lines of the plane must contain the same number of points. Finally, the existence of a quadrangle in the plane ensures that no point is contained in every line and that every point is incident with k lines. □

Having established this fact, there is a clear way to define a finite projective plane by its size. A projective plane of order n is a projective plane with the properties that each line contains $n+1$ points and each point is contained in $n+1$ lines. The next lemma also follows directly from the structure of projective planes.

Lemma 1.1.2. *A projective plane of order n has n^2+n+1 lines and n^2+n+1. points*

Proof. Let x be a point of a projective plane of order n. If we pick any other point p then there is a line containing x and p by the second property of projective planes. Therefore the collection of $n+1$ lines passing through x must contain every point of the plane. Furthermore, p must lie on exactly one line through x or there would be more than one line containing x and p contradicting the uniqueness requirement. Thus, each of the n points other than x on the $n+1$ lines containing x is a distinct point of the plane. Remembering to count x as well, this gives $n(n+1)+1 = n^2+n+1$ points of the plane. An analogous argument to this one proves that there are also n^2+n+1 lines in the plane. □

The expression n^2+n+1 arises frequently in this context so we denote $N = n^2+n+1$ to simplify future equations. Since $N \geq 4$ in order to satisfy the last axiom of projective planes, the smallest projective plane has order 2. This plane is unique up to isomorphism and it is commonly called the Fano plane after Gino Fano. The Fano Plane arises frequently in matroid theory and is shown in Figure 1.2.

We can use the properties we have discussed so far to show a method for creating projective planes from finite fields. Let p be a prime and k be a positive integer. We can construct a projective plane of order p^k by using the finite field $GF(p^k)$. Let $\mathbb{F} = GF(p^k)$ and $n = p^k$, then consider the vector space $\mathbb{F}^3$. We define the points of a plane to be the 1-dimensional subspaces of $\mathbb{F}^3$ and lines to be the 2-dimensional subspaces. It remains to show that this collection of lines and points satisfies the axioms of projective planes.

First, consider a pair of distinct lines. They must intersect in a 1-dimensional subspace (a point) because a 3-dimensional space such as $\mathbb{F}^3$ does not contain two disjoint 2-dimensional subspaces. If the lines intersect in a space with dimension 2 then the lines are not distinct. It is also straightforward to see that the second requirement of projective planes holds; a distinct pair of points define a unique line by simply taking the closure of the union of the two 1-dimensional spaces.

The final condition is met by noting that for any field $\mathbb{F}$, the space $\mathbb{F}^3$ contains the four distinct points containing $(1,0,0),(0,1,0),(0,0,1)$ and $(1,1,1)$ which form a quadrangle in the plane.

Having shown that this does in fact give us a projective plane we consider the number of points in this plane. Each of the non-zero vectors of $\mathbb{F}^3$ is part of a single 1-dimensional subspace and each of these spaces contains the linear multiples of a single vector. Therefore each 1-dimensional space contains $n-1$ non-zero vectors and the set of 1-dimensional spaces partitions the set of non-zero vectors of $\mathbb{F}^3$. There are n^3-1 non-zero vectors in $\mathbb{F}^3$ so the number of 1-dimensional subspaces is given by

$$\frac{n^3-1}{n-1} = n^2+n+1.$$

Thus there are n^2+n+1 points in the plane and, by Lemma 1.1.2, this projective plane has order $n = p^k$. We call this plane $PG(2,n)$.

This construction method gives us an infinite number of projective planes to study and also brings us to one of the most important open questions of combinatorics.

Open Problem 1.1.3. *Does a projective plane of order n exist where n is not a prime power?*

That is not to say that every finite projective plane is isomorphic to $PG(2,n)$ for some n. Every projective plane which is derived from a finite field is Desarguesian, meaning that Desargues' Theorem holds in all of these planes. It has been shown that there are 3 non-Desarguesian projective planes of order 9 which are not isomorphic to each other or to PG(2,9) [7]. No projective planes of orders which are not prime powers are currently known however.

This is not due to lack of trying on behalf of mathematicians. In the 20th century many people attempted to answer this question and drew conclusions about particular orders for which a projective plane certainly cannot exist. The earliest related work was done by Tarry in 1900 [19]. A *Latin square of order n* is an $n \times n$ array containing the numbers $\{1,2,\ldots,n\}$ such that no row or column contains any number more than once. If A and B are Latin squares such that $A = a_{i,j}$ and $B = b_{i,j}$ for $1 \leq i,j \leq n$ then A and B are *orthogonal* if the n^2 ordered pairs $(a_{i,j}, b_{i,j})$ are all distinct. Tarry enumerated, by hand, the Latin squares of order 6 and found that no pair of these were orthogonal. The origin of this work was to investigate Euler's thirty six officers problem [5], but it would turn out to have implications for projective planes as well. Bose's result of 1930 [2] states that if a projective plane of order n exists then so do $n-1$ pairwise orthogonal Latin squares of order n. In conjunction with Tarry's enumeration this was the first proof that no projective plane of order 6 exists. If a projective plane of order 6 existed then there would have to be a set of 5 pairwise orthogonal Latin squares when in fact Tarry's work showed there was not even a single pair which are orthogonal.

The next breakthrough in proving the non existence of projective planes came from Bruck and Ryser in 1949 [3] and confirmed the result that the projective plane of order 6 does not exist.

Theorem 1.1.4. *(Bruck-Ryser) If $n = 1,2$ mod 4 and n is not the sum of two squares then no projective plane of order n exists.*

This ruled out projective planes of order n where $n = 6, 14, 21, 22, \ldots$ and it remains the only collection of orders for which it is known that no projective plane exists. Unfortunately the discovery of this result did not resolve the next smallest plane for which existence was not yet determined, the plane of order 10. Though $10 = 2$ (mod 4), it is also the sum of two squares ($10 = 3^2 + 1^2$) and so the Bruck-Ryser Theorem does not apply.

It was an extensive computer search undertaken by Lam, Thiel and Swiercz [10] which eventually proved that no projective plan of order 10 could exist. This was done by applying principles of coding theory to the incidence matrix of the projective plane of order 10 which was assumed to exist. The incidence matrix is an $N \times N$ matrix where every row corresponds to a line of the plane and the columns are the points of the plane. The entries of the matrix are given by

$$A_{ij} = \begin{cases} 1 & \text{line } i \text{ contains point } j \\ 0 & \text{otherwise.} \end{cases}$$

The code space which the rows of this matrix generate over a binary field, contains vectors which each correspond to taking the symmetric difference of a collection of lines of the plane. These symmetric differences of lines are called *configurations* and they contain the points of the plane which are in an odd number of the lines in the configuration. The weight of a codeword in this space is equal to the number of non-zero entries it contains which is in turn equal to the number of points in the corresponding configuration. We define the weight enumerator polynomial for a code C as

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

where N is the length of the code and A_i is the number of codewords of weight i.

Some of the values of A_i were calculated from the structure of the plane. The 111 lines of the plane are the only configurations containing 11 points so $A_{11} = 111$. Similarly the empty codeword is the only configuration with no points, thus $A_0 = 1$. It was also determined that $A_i = 0$ for $i \in \{1,2,\ldots,10\}$ and for $i = 1,2 \pmod 4$. Since the plane contains the configuration of all the points, it was observed that $A_i = A_{111-i}$.

Determining the remaining A_i values required additional coding theory. We first define the dot product of two vectors. If $\mathbf{x} = (x_1,x_2,\ldots,x_n)$ and $\mathbf{y} = (y_1,y_2,\ldots,y_n)$ with $x_1,y_1,\ldots,x_n,y_n \in \mathbb{F}$ then the dot product of $\mathbf{x}$ and $\mathbf{y}$ is given by

$$\mathbf{x}\cdot\mathbf{y} = x_1y_1 + x_2y_2 + \cdots + x_ny_n.$$

We say two vectors $\mathbf{x}$ and $\mathbf{y}$ are *orthogonal* if $\mathbf{x}\cdot\mathbf{y} = 0$. For a code C which is a subspace of $\mathbb{F}^k$ the *orthogonal code* consists of all vectors which are orthogonal to every vector in C and is defined by

$$C^{\perp} = \{\mathbf{x} \in \mathbb{F}^k \mid \forall \mathbf{y} \in C,\ \mathbf{x}\cdot\mathbf{y} = 0\}.$$

It can be shown that if C is the code space generated by the incidence matrix of the projective plane of order 10, then the orthogonal code $C^{\perp}$ is a subset of C consisting of the vectors of C with even weight. This means that $(A_i)_{C^{\perp}} = (A_i)_C$ when i is even and $(A_i)_{C^{\perp}} = 0$ when i is odd. The MacWilliams identity provides a relationship between the weight enumerator of a code and the weight enumerator of the orthogonal code which allowed the A_i coefficients to be solved against each other.

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

The resulting system of equations is underdetermined, but can be calculated once the values A_{12},A_{15} and A_{16} are known. These variables were chosen as smaller configurations require less computation to investigate. The first value solved was A_{15}, shown to be 0 by Macwilliams, Sloane and Thompson [12]. Next, A_{12} was also shown to be 0 by Lam, Thiel and Swiercz [9] who went on to finish work started by Carter [4] which showed $A_{16} = 0$ [8]. This revealed the values of the remaining A_i coefficients and in particular $A_{19} = 24,675$. With evidence that a configuration containing 19 elements must exist in the code space, a final search was conducted to try and complete an 111×111 matrix with entries which fulfill the requirements of an incidence matrix for a projective plane of order 10. This was the most time consuming part of the search, but it was completed in 1989 and found no viable incidence matrices thus proving there is no projective plane of order 10.

We might hope that a similar line of reasoning could apply to the projective plane of order 12. The overall idea of systematically testing for valid incidence matrices for such a plane is reasonable, but computationally it is made more difficult by the fact that the incidence matrix for a projective plane of order 12 would contain just over twice as many entries as the incidence matrix for a projective plane of order 10. In addition, the methods used to reduce the scope of the search for the plane of order 10 do not all apply here because of the difference in structure of the plane. Notably, the binary code generated from the plane does not contain its orthogonal code (though from [1, 4.6.2] we will see that the ternary field is a better choice). We instead need to consider which projective planes do have this property and find some way of preventing the search space from becoming unfeasibly large.

This is where we turn our focus to matroid theory. If the bounds of coding theory are stretched by this computational method of determining the existence of planes then perhaps matroids can offer a theoretical approach. We start the same way as the coding theorists, with an incidence matrix for the projective plane of order n which is assumed to exist. We also consider the vector space C generated by the rows of the matrix, but then use these vectors as a chain-group representation for a matroid M [20]. The *support* of a vector is the set of columns with a non-zero entry in that vector. The minimal supports of vectors in C are cocircuits of M which gives us the relationship between the code and the matroid. The dual of a matroid is also easily defined as it simply has $C^{\perp}$ as its chain-group representation. Therefore the minimal supports in $C^{\perp}$ are cocircuits of M^* and circuits of M. We use this to show a connection between projective planes and ISD matroids. A similar relationship between projective planes and self-dual codes has been noted before (see [6]), but here we present the proof in a matroid context.

Lemma 1.1.5. *Let M be a matroid. If $M\backslash e = (M/e)^*$ then M is ISD.*

Proof. Let $N = M\backslash e$ so that we get the following relationships.

$$N = M\backslash e \leftarrow M \rightarrow M/e = N^*$$

First, consider a circuit C of M that does not contain e. When e is deleted from M it does not affect C which remains a circuit in N. Thus C is a cocircuit of N^* and furthermore when we consider coextending by e again C is unaffected. Therefore C is a cocircuit of M.

Next, consider a circuit C of M that contains e. By properties of circuits, $C-e$ is a circuit of $M/e = N^*$ and so it is a cocircuit of N. Now either $C-e$ or C is a cocircuit of M and we will show that it must be C which is the cocircuit. Suppose to the contrary that $C-e$ is a cocircuit of M. This implies $C-e$ is a cocircuit of $M/e = N^*$ and a circuit of N. This leads to the contradictory result that $C-e$ is a circuit of M when it is also a proper subset of the circuit $C \subseteq M$. Therefore it is not possible for $C-e$ to be a cocircuit of M and instead C must be a cocircuit of M.

Having shown that all circuits of M are cocircuits we need to show that the cocircuits are all circuits or equivalently that all circuits of M^* are cocircuits of M^*. We can see that by taking the dual of N and N^* we get $N^* = (M\backslash e)^* = M^*/e$ and $N = (N^*)^* = (M/e)^* = M^*\backslash e$. Thus we have the same relationship between M^*, N and N^* as M, N and N^*.

$$N = M^*\backslash e \leftarrow M^* \rightarrow M^*/e = N^*$$

This means the same arguments, showing that circuits of M are cocircuits of M, apply to M^*. Therefore every cocircuit of M is a circuit of M and M is ISD. □

Theorem 1.1.6. *Let n be divisible by some prime p but not by p^2. If a projective plane of order n exists let C be the code generated by the incidence matrix of the plane over $GF(p)$ and let N be the matroid which has C as a chain-group. Then there exists an ISD $GF(p)$-representable matroid M with $N = M\backslash e$ for some $e \in E(M)$.*

Proof. A projective plane of order n is equivalent to a $(n^2+n+1, n+1, 1)$ design of order n. By [1, 4.6.2], if n is once divisible by p then the code generated by the incidence matrix of the projective plane over $GF(p)$ has the following properties:

1. $C^{\perp} \subseteq C$
2. $\dim(C) = \dfrac{n^2+n+2}{2}$

We let N be the matroid which has C as a chain-group representation. The supports of the minimal vectors of $C^{\perp}$ are the circuits of N and $C^{\perp} \subseteq C$ so if they are not minimal supports in C then there must be a cocircuit C^* properly contained in the circuit. It is possible to take a linear combination of the vectors corresponding to C and C^* to cancel any entry which is part of both C and C^*. The resulting vector has smaller support than C and is still in $C^{\perp}$. Therefore we can repeat this technique using this vector in place of the the vector for C until we reach a vector which has minimal support and corresponds to a cocircuit. Therefore every vector $\mathbf{x}$ in $C^{\perp}$ is the sum of vectors which have a support contained the support of $\mathbf{x}$ and therefore every circuit is the union of cocircuits.

Now we know that every circuit of N is a union of circuits of N^* which implies that N^* is a quotient of N by [16, 7.3.9]. From the dimension of C and the fact that $\dim(C) + \dim(C^{\perp}) = n^2+n+1$ we can deduce that $r(N) = r(N^*)+1$. Therefore we can obtain N^* by extending N by a single element and then contracting this new element.

We can also find a way of expressing N and N^* with matrices. If A is a basis for the code C then it the matrix with A as its rows is a representation for N over $GF(p)$. Similarly, a basis for $C^{\perp}$, A^*, can be used in a matrix representation for N^* and has one less row. Let $\mathbf{x}$ be any vector in $C - C^{\perp}$ and consider the representation A' for the matroid M defined below.

$$A' = \left[\begin{array}{c|c} & 0 \\ & 0 \\ A^* & \vdots \\ & 0 \\ \hline \mathbf{x} & 1 \end{array}\right]$$

Deleting the last column must give a representation for the matroid N and contracting the last column results in the matroid N^*. The matroid M is $GF(p)$ representable and, by Lemma 1.1.5, M is ISD. □

The converse of of this Theorem is not true since there are ISD matroids with 6 elements such as $U_{3,6}$ and R_6 and no projective plane with 5 elements. However it does give a necessary condition for the existence of projective planes. This means if the projective plane of order 12 exists, which is the next smallest whose existence is unknown, then so does a specific ISD matroid which is representable over $GF(3)$ and has 158 elements and rank 79.

1.2 Thesis Overview

The remainder of thesis focuses on ISD matroids. Knowing that projective planes are related to ISD matroids with a single element deleted or contracted, inspired more investigation into the minors of ISD matroids. One of our aims was to learn more about the substructures of these highly structured matroids. We conjecture that there is not a lot of structure from ISD matroids preserved by minor operations.

Conjecture 1.2.1. *Every matroid is a minor of an ISD matroid.*

This is supported by Chapter 2 which contains the following theorem.

Theorem 1.2.2. *Every sparse paving matroid is a minor of an ISD sparse paving matroid.*

This proves the conjecture for a large class of matroids. It has conjectured by Mayhew, Newman, Welsh and Whittle that asymptotically almost all matroids are sparse paving [14]. This chapter also provides an example of a non-representable ISD matroid, the existence of which is necessary if we expect non-representable matroids to be minors of ISD matroids.

Chapter 3 provides further evidence for Conjecture 1.2.1.

Theorem 1.2.3. *Every representable matroid is a minor of an ISD representable matroid.*

In this chapter we also make another conjecture, this one specific to representable matroids.

Conjecture 1.2.4. *Every $\mathbb{F}$-representable matroid is a minor of an ISD $\mathbb{F}$-representable matroid for all fields $\mathbb{F}$.*

We prove this conjecture for fields of characteristic 2, algebraically closed fields, and $\mathbb{F} = GF(p)$ for primes p equivalent to 3 modulo 4.

Chapter 4 extends a result of Lindström which says that there are no ISD matroids which are simple and regular. We prove the following strengthening of this result.

Theorem 1.2.5. *If a matroid is simple and regular, then it cannot be obtained by contraction from an ISD matroid.*

In Chapter 5 we explore the overlap in the classes of frame matroids and ISD matroids which leads to the theorem below.

Theorem 1.2.6. *Let M be a frame matroid. If M is ISD and 3-connected, then it is a swirl.*

Chapter 6 is concerned with the axiomatisability of ISD matroids and self-dual matroids. A sentence in MS_0 which characterises ISD matroids is presented as well as a proof that there is no sentence which is satisfied if and only if a matroid is self-dual.

Finally, Chapter 7 is a summary chapter containing a collection of conjectures relating to the material of this thesis and the progress we have made toward each of them.

Chapter 2

Sparse Paving Matroids

A matroid M with rank r is *paving* if every circuit of the matroid has rank at least $r-1$. If both M and its dual are paving then we say M is *sparse paving*. A *non-basis* is an r-element set of a matroid which is not a basis and we use this to give an equivalent definition of sparse paving matroids. The matroid M is sparse paving if M is paving and whenever X,Y are distinct non-bases of M, $|X \cap Y| < r(M)-1$. Since M has no circuits with rank less than $r-1$ a non-basis of M must be a circuit hyperplane.

The Vámos matroid V_8 is a well known sparse paving matroid consisting of 8 elements and 5 circuit hyperplanes. It is an example of one of the smallest non-representable matroids as every matroid with 7 or fewer elements is representable over some field [16, 6.4.10]. If we denote the groundset $\{a,b,c,d,e,f,g,h\}$ then the circuit hyperplanes of V_8 are $\{\{a,b,c,d\},\{e,f,g,h\},\{a,b,g,h\},\{c,d,e,f\},$ $\{a,b,e,f\}\}$. These are equivalent to the edges of a diamond graph if we label each vertex with two elements of the matroid, as shown in Figure 2.1.

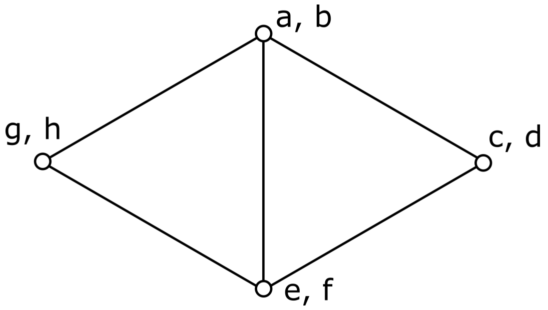

Figure 2.1: A diamond graph of the dependence in V_8.

Next we will demonstrate a method for adding elements to a sparse paving matroid to construct an ISD sparse paving matroid. First, we will investigate how a sparse paving matroid M behaves under deletion and contraction. Let $\mathscr{C}_H$ denote the set of circuit hyperplanes of M and let e be an element of $E(M)$. The set of circuit hyperplanes of M/e is given by $\{C-e \mid e \in C,\, C \in \mathscr{C}_H\}$ and the set of circuit hyperplanes of $M\backslash e$ is $\{C \mid e \notin C,\, C \in \mathscr{C}_H\}$. Thus when e is contracted from M the new circuit hyperplanes correspond to the circuit hyperplanes of M which contain e and when e is deleted they correspond to the circuit hyperplanes which do not contain e. This is promising when it comes to extending and coextending a sparse paving matroid because both operations can be used to generate new circuit hyperplanes.

Lemma 2.1.1. *A sparse paving matroid M is ISD if the complement of every circuit hyperplane is a circuit hyperplane.*

Proof. A matroid is ISD if the complement of every basis is another basis. This must mean the bases are in complementary pairs and the complement of non-bases are also non-bases. In a sparse paving matroid all non-bases are circuit hyperplane so if M is ISD then the complements of circuit hyperplanes are circuit hyperplanes. □

The Vámos matroid already contains four circuit hyperplanes which are in complementary pairs, but the complement of $\{a,b,e,f\}$ is not a circuit hyperplane so the Vámos matroid is not ISD.

To create an ISD matroid, first we coextend the Vámos matroid by two new elements i and j. Whenever we coextend, the new elements must be added to all of the current circuit hyperplanes or the cardinality of these circuits will be less than the rank of the matroid, thus causing the matroid to no longer be sparse paving. Currently the circuit hyperplanes of this matroid are as follows:

$$\{\{a,b,c,d,i,j\},\{e,f,g,h,i,j\},\{a,b,g,h,i,j\},\{c,d,e,f,i,j\},\{a,b,e,f,i,j\}\}.$$

We now make a free extension by adding the element k in such a way that it does not occur in any circuit hyperplanes. At this point the new matroid has eleven elements and has rank six. By adding a final element l and five new circuit hyperplanes, which are the complements of the existing circuit hyperplanes, we create an ISD sparse paving matroid. The set of circuit hyperplanes for this matroid is

$\{\{a,b,c,d,i,j\},\{e,f,g,h,i,j\},\{a,b,g,h,i,j\},\{c,d,e,f,i,j\},\{a,b,e,f,i,j\},$
$\{e,f,g,h,k,l\},\{a,b,c,d,k,l\},\{c,d,e,f,k,l\},\{a,b,f,g,k,l\},\{c,d,f,g,k,l\}\}.$

To confirm that this collection of circuit hyperplanes constitutes a sparse paving matroid we need only check that no pair of distinct circuit hyperplanes intersect in five points. This is easily verified by inspecting the list of circuit hyperplanes or we can use our construction method to convince us of this. The intersection of two distinct circuit hyperplanes from the Vámos matroid contained at most two points, because the Vámos matroid is sparse paving. Elements i and j were added to all of these circuit hyperplanes so the resulting intersections of two distinct circuit hyperplanes is at most four. The five circuit hyperplanes which were chosen as the complements of the first five have the same size of intersection as their counterparts so any pair has at most four elements in common. It only remains to verify that taking one circuit hyperplane extended from the original circuit hyperplanes and one of the complements does not lead to a pair of circuit hyperplanes with an intersection of five elements. This is not hard to check since circuit hyperplanes based on the original set all contain elements i and j, whereas circuit hyperplanes from the set of complements all contain k and l and therefore there are at least two elements which are different between the two. Thus the matroid we have defined is an ISD sparse paving matroid with V_8 as the minor obtained by deleting k and l, and contracting i and j.

Next, we refine this method so it will apply to any sparse paving matroid. This means that for a given sparse paving matroid M we can always find an ISD sparse paving matroid which contains M as a minor. This is demonstrated in the following theorem, a restatement of Theorem 1.2.2 with a bound on the size of N.

Theorem 2.1.2. *Let M be a sparse paving matroid with $r(M) = r$ and $|E(M)| = n$. Then there exists an ISD sparse paving matroid N such that M is a minor of N and $|E(N)| \leq n + |n-2r| + 4$.*

Proof. To prove this claim we shall construct an ISD sparse paving matroid with M as a minor. First we are looking to extend M or M^* until we reach a matroid M' where $r(M') = \frac{1}{2}|E(M')|$ or equivalently $r(M') = r^*(M')$. To achieve this we simply freely extend or freely coextend M to reach this equality. A free extension consists of adding a new element to the ground set which is not contained in any circuit hyperplanes and it increases $r^*(M)$ by one. A free coextension adds a new element to every circuit hyperplane and increases $r(M)$ by one. The number of elements we need to add is the difference between $r(M)$ and $r^*(M)$ which is $|n-2r|$.

Once we have generated M' there are two possibilities. The first is that M' contains a pair of complementary hyperplanes and the second is that M' contains no pairs of complementary circuit hyperplanes. If the first case occurs, then we simply add two elements so that the new matroid M'' falls into the second category. First we coextend M' by the element x which is added to every circuit hyperplane. Then we extend by the element y freely so it does not occur in any circuit hyperplanes. Now the matroid M'' cannot contain a pair of complementary circuit hyperplanes because none of them contain y and $r(M'') = r^*(M'')$. We will let M'' be the new M'.

Now there are no pairs of complementary circuit hyperplanes in M'. Let $\mathscr{C}_H$ denote the set of circuit hyperplanes of M'. We define a new matroid N with ground set $E(M') \cup \{x,y\}$ and circuit hyperplanes $\{C \cup x \mid C \in \mathscr{C}_H\} \cup \{(E(M')-C) \cup y \mid C \in \mathscr{C}_H\}$. This is obtained from M' by a free coextension by x and a specific extension by y so $M' = N\backslash y/x$ and $r(N) = r(M')+1$.

In order for N to be sparse paving (and therefore a matroid) the intersection of a pair of distinct circuit hyperplanes must contain fewer than $r(M')$ elements. A pair of circuit hyperplanes C_1, C_2 containing x directly corresponds to a pair of circuit hyperplanes of M' which had pairwise intersection strictly smaller than $r(M')-1$. Therefore $|C_1 \cap C_2| \leq r(M')-1$ when allowing for the additional common element x. Similarly, being the complement of the set of circuit hyperplanes containing x, the set of circuit hyperplanes containing y also has pairwise intersection less than $r(M')$. Having ruled out the other two possibilities, if we suppose a pair of circuit hyperplanes of N intersect in $r(M')$ elements then one must contain x, C_x, and one must contain y, C_y. These circuit hyperplanes already differ in the elements x and y, so they intersect in all the other elements. This means $E(N)-C_y$ is a circuit hyperplane and $(E(N)-C_y) \cap C_x = x$. Thus $(E(N)-C_y)-x$ and $C_x - x$ are complementary circuit hyperplanes of M' which contradicts our evaluation of M'. Therefore N is an ISD sparse paving matroid containing M as a minor.

The number of elements in M' is $n+|n-2r|$ and requires 2 or 4 elements more to reach N depending on whether M' contains complementary circuit hyperplanes. Thus, $|E(N)| \leq n+|n-2r|+4$. □

2.2 A Minimal Non-Representable ISD Matroid

When we extended the Vámos matroid to an ISD sparse paving matroid earlier we found a 12-element ISD matroid which is non-representable. We now show that there is a non-representable ISD matroid on 10 elements by choosing a different non-representable matroid to extend.

Proposition 2.2.1. *The smallest ISD non-representable matroid has 10 elements.*

Proof. Let M be the sparse paving matroid with ground set $\{a,b,c,d,e,f,g,h\}$ and circuit hyperplanes $\{\{a,b,c,h\}$, $\{a,c,d,g\}$, $\{c,d,e,h\}$, $\{b,d,e,f\}$, $\{b,d,g,h\}$, $\{b,c,f,g\}$, $\{a,b,e,g\}$, $\{a,d,f,h\}\}$. We will show that M is non-representable. Note that M can be derived from the matroid N presented in Figure 2.2 by letting the sets $\{a,c,e,f\}$ and $\{b,d,e,f\}$ be bases rather than circuits as they are shown in N. In the figure, line segments with the same markings have the same length.

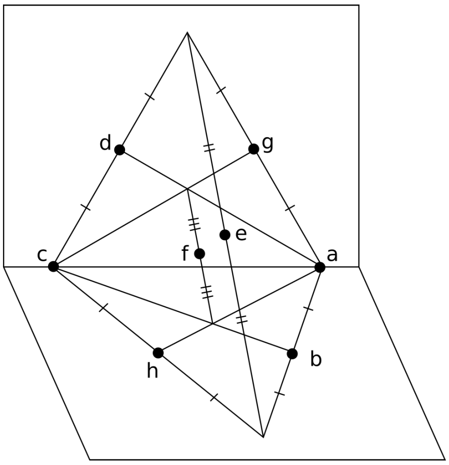

Figure 2.2: A picture of matroid N in Euclidean space.

Suppose that M does have a matrix representation A. We can use row operations to transform A into a matrix that starts with a rank four identity matrix where the identity consists of any basis for M. This means we only need to work with the remaining 16 entries of the matrix. When we discard the identity we can label the rows of the remaining part of the matrix with the elements forming the identity; here we have chosen the basis $\{a,b,c,d\}$. If we denote the row labels X and the column labels Y then a set $Z \in E(M)$, with size equal to the rank of the matroid, is dependent if and only if the square submatrix spanned by $(X-Z)\times(Y\cap Z)$ has determinant zero.

First we look at 1×1 submatrices. The circuit hyperplanes $\{a,b,c,h\}$ and $\{a,c,d,g\}$ both induce 1×1 matrices with determinant zero. Thus, there are two zero entries in the matrix and the other entries are non-zero. This is shown in the leftmost matrix in Figure 2.3.

$$\begin{array}{c c} & \begin{array}{cccc} e & f & g & h \end{array} \\ \begin{array}{c} a \\ b \\ c \\ d \end{array} & \begin{pmatrix} * & * & * & * \\ * & * & 0 & * \\ * & * & * & * \\ * & * & * & 0 \end{pmatrix} \end{array} \quad \begin{array}{c c} & \begin{array}{cccc} e & f & g & h \end{array} \\ \begin{array}{c} a \\ b \\ c \\ d \end{array} & \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & x_1 & 0 & x_2 \\ 1 & x_3 & x_4 & x_5 \\ 1 & x_6 & x_7 & 0 \end{pmatrix} \end{array} \quad \begin{array}{c c} & \begin{array}{cccc} e & f & g & h \end{array} \\ \begin{array}{c} a \\ b \\ c \\ d \end{array} & \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & \alpha^{-1} & 0 & 1 \\ 1 & 1 & \alpha & \alpha \\ 1 & \alpha & \alpha & 0 \end{pmatrix} \end{array}$$

Figure 2.3: The construction of a representation of M

Now we can scale the rows and columns of the matrix to guarantee seven entries which are 1. As we know that the entries are non-zero it is simply a matter of multiplying the appropriate row or column by a scalar. We then label the remaining entries with x_i values as shown in the middle matrix of Figure 2.3.

We can determine these x_i values using the other circuit hyperplanes of M. Below, we list the circuit hyperplanes along with the submatrix must have determinant zero and what that tells us about the x_i entries.

$$\{c,d,e,h\} \quad \rightarrow \quad \begin{vmatrix} 1 & 1 \\ 1 & x_2 \end{vmatrix} = 0 \quad \rightarrow \quad x_2 = 1$$

$$\{b,d,e,f\} \quad \rightarrow \quad \begin{vmatrix} 1 & 1 \\ 1 & x_3 \end{vmatrix} = 0 \quad \rightarrow \quad x_3 = 1$$

$$\{b,d,g,h\} \quad \rightarrow \quad \begin{vmatrix} 1 & 1 \\ x_4 & x_5 \end{vmatrix} = 0 \quad \rightarrow \quad x_4 = x_5$$

$$\{b,c,f,g\} \quad \rightarrow \quad \begin{vmatrix} 1 & 1 \\ x_6 & x_7 \end{vmatrix} = 0 \quad \rightarrow \quad x_6 = x_7$$

$$\{a,b,e,g\} \quad \rightarrow \quad \begin{vmatrix} 1 & x_4 \\ 1 & x_7 \end{vmatrix} = 0 \quad \rightarrow \quad x_4 = x_7$$

$$\{a,d,f,h\} \quad \rightarrow \quad \begin{vmatrix} x_1 & x_2 \\ x_3 & x_5 \end{vmatrix} = \begin{vmatrix} x_1 & 1 \\ 1 & x_5 \end{vmatrix} = 0 \quad \rightarrow \quad x_1 = \frac{1}{x_5}$$

If we let x_4 be α then the rest of the matrix is resolved as in the final matrix of Figure 2.3. However this also implies that $\{e,f,g,h\}$ is dependent in M as the determinant of the entire matrix is 0. This is a contradiction, since $\{e,f,g,h\}$ is not a circuit hyperplane of the sparse paving matroid it must be a basis and A does not represent M. Hence, M is non-representable.

We chose M specifically because it does not have any complementary circuit hyperplanes and has $r(M) = \frac{1}{2}E(M)$. This means that we can find an ISD sparse paving matroid with M as a minor by adding two elements using the method shown in Theorem 2.1.2. This matroid is non-representable and has 10 elements. The circuit hyperplanes of the matroid are shown below.

$$\begin{gathered}\{\{a,b,c,h,i\},\{a,c,d,g,i\},\{c,d,e,h,i\},\{b,d,e,f,i\},\{b,d,g,h,i\},\{b,c,f,g,i\},\\ \{a,b,e,g,i\},\{a,d,f,h,i\},\{d,e,f,g,j\},\{b,e,f,h,j\},\{a,b,f,g,j\},\{a,c,g,h,j\},\\ \{a,c,e,f,j\},\{a,d,e,h,j\},\{c,d,f,h,j\},\{b,c,e,g,j\}\}\end{gathered}$$

Now we need to verify that there are no non-representable ISD matroids on 8 or fewer elements. Since every matroid with less than 8 elements is representable we only need to consider matroids with 8 elements.

A computer was used to generate all matroids with 8 elements and they were each tested to see if they were ISD. The result was that there are 17 ISD matroids on 8 elements. Ten are sparse paving matroids and of the remaining seven, only two are simple. We give representations for these 12 matroids in Figure 2.4. The other five matroids must be representable because if we keep one element from each parallel class then this simplification of the matroid has fewer than 8 elements. Thus it must be representable and by duplicating the appropriate columns of the representation we can find a representation for the original matroid. For this reason we do not provide representations for the non-simple ISD matroids on 8 elements. □

$$\overset{\mathbb{R}}{\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 2 & 3 & 4 \\ 0 & 0 & 1 & 0 & 1 & 3 & 4 & 2 \\ 0 & 0 & 0 & 1 & 1 & 4 & 2 & 3 \end{bmatrix}} \quad \overset{\mathbb{R}}{\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 2 & 3 & 4 \\ 0 & 0 & 1 & 0 & 1 & 3 & 4 & 5 \\ 0 & 0 & 0 & 1 & 0 & 1 & 5 & 6 \end{bmatrix}}$$

$$\overset{\mathbb{R}}{\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 2 & 3 & 1 \\ 0 & 0 & 1 & 0 & 1 & 3 & 6 & 3 \\ 0 & 0 & 0 & 1 & 0 & 1 & 3 & 3 \end{bmatrix}} \quad \overset{\mathbb{R}}{\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 2 & 0 \\ 0 & 1 & 0 & 0 & 1 & 2 & 6 & 4 \\ 0 & 0 & 1 & 0 & 1 & 0 & 4 & 8 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}}$$

$$\overset{\mathbb{R}}{\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 6 & 3 & 2 \\ 0 & 0 & 1 & 0 & 1 & 3 & 3 & 1 \\ 0 & 0 & 0 & 1 & 1 & 2 & 1 & 2 \end{bmatrix}} \quad \overset{\mathbb{R}}{\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 3 & 4 & 1 \\ 0 & 0 & 1 & 0 & 1 & 4 & 5 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}}$$

$$\overset{\mathbb{R}}{\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 3 & 2 \\ 0 & 0 & 1 & 0 & 1 & 3 & 1 & 2 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 2 \end{bmatrix}} \quad \overset{GF(4)}{\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & a & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & a & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}}$$

$$\overset{GF(3)}{\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 2 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 2 \end{bmatrix}} \quad \overset{GF(2)}{\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}}$$

$$\overset{\mathbb{R}}{\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 2 \\ 0 & 0 & 1 & 0 & 1 & 3 & 4 & 0 \\ 0 & 0 & 0 & 1 & 1 & 5 & 6 & 0 \end{bmatrix}} \quad \overset{\mathbb{R}}{\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 2 \\ 0 & 0 & 1 & 0 & 1 & 1 & 2 & 0 \\ 0 & 0 & 0 & 1 & 1 & 2 & 0 & 0 \end{bmatrix}}$$

Figure 2.4: Representations of the 12 simple ISD matroids with 8 elements.

Chapter 3

Representable Matroids

3.1 Introduction

A representable matroid M has the property that there is a mapping between the elements of $E(M)$ and a collection of vectors such that a $X \subseteq E(M)$ is independent if and only if the corresponding vectors are. As a result we can represent M with a matrix where the columns are vectors with the same dependence structure as the elements of the ground set of M. On the other hand, we can also consider the vector space generated by the rows of the matrix. This is called a chain-group representation and was introduced by Tutte in [20]. We use these chain-groups to prove Theorem 1.2.3 which we restate here.

Theorem 3.1.1. *If M is a representable matroid then it is a minor of an ISD representable matroid.*

We also propose the following conjecture.

Conjecture 3.1.2. *If M is a matroid which is representable over a field $\mathbb{F}$, then there exists an ISD matroid N such that N is representable over $\mathbb{F}$, and M is a minor of N.*

We prove this conjecture in the cases where $\mathbb{F}$ is a field of characteristic 2, $\mathbb{F}$ is an algebraically closed field such as $\mathbb{C}$, or $\mathbb{F} = GF(p)$ for a prime $p = 3$ (mod 4). These proofs are found in the sections 3.3, 3.4 and 3.5 following the number theory introduced in 3.2 which is required to prove these results. Theorem 3.1.1 is a direct result of these theorems.

3.2 Quadratic Residues

An element a of a finite field $\mathbb{F}$ is a *quadratic residue* if there exists b in $\mathbb{F}$ such that

$$a = b^2.$$

The remaining elements of $\mathbb{F}$, which do not have this property, are called *quadratic nonresidues*. We will abbreviate these terms and say that every element of a finite field $\mathbb{F}$ is a residue or a nonresidue.

First we consider finite fields of characteristic 2. The following proposition is of use to us in this case.

Proposition 3.2.1. *(Frobenius Endomorphism) If $\mathbb{F}$ is a finite field with characteristic p then the map*

$$\begin{aligned} \phi &: \mathbb{F} \to \mathbb{F} \\ \phi(a) &= a^p \end{aligned}$$

is an automorphism.

Proof. Under this mapping, the fact that $\phi(a)\phi(b) = \phi(ab)$ is trivial; by the commutativity of multiplication, $x^p y^p = (xy)^p$. In order to show that $\phi(a) + \phi(b) = \phi(a+b)$ we will use the formula for binomial expansion and observe that in a field of characteristic p all but the first and last terms are equal to 0.

$$\begin{aligned} \phi(x+y) &= (x+y)^p \\ &= \sum_{i=0}^{p} \binom{p}{i} x^{p-i} y^i \\ &= x^p + y^p = \phi(x) + \phi(y) \end{aligned}$$ □

It is then clear that if $\mathbb{F}$ is a field of characteristic 2, the mapping of $a \mapsto a^2$ is onto and therefore every element of $\mathbb{F}$ is a residue.

The situation is slightly more complicated in fields that do not have characteristic 2. When p is an odd prime the only element of $\mathbb{Z}_p$ which is its own additive inverse is 0. Therefore, if we consider the multiplicative group $\mathbb{Z}_p^*$ and the fact that

$$a^2 \equiv (-a)^2 \mod \text{p},$$

the mapping $\phi : a \to a^2$ is a two to one mapping for $a \in \mathbb{Z}_p^*$. Thus, $\mathbb{Z}_p^*$ contains $\frac{p-1}{2}$ residues and the same number of nonresidues. Let R be the set of residues of $\mathbb{Z}_p^*$ and N be the set of nonresidues. Next we will present some well known properties of R and N. In the following lemma we use notation for multiplying a set of elements of a field each by a single element. If x is an element of a field and Y is a set of elements of the field then we define $xY = \{xy \mid y \in Y\}$.

Lemma 3.2.2. *Let p be an odd prime and R and N be the set of residues and nonresidues of $\mathbb{Z}_p^*$ respectively. If $r_1, r_2 \in R$ and $n_1, n_2 \in N$ then r_1r_2, $n_1n_2 \in R$ and $r_1n_1 \in N$. Moreover, $r_1R = R, r_1N = N, n_1R = N$ and $n_1N = R$.*

Proof. If $r_1, r_2 \in R$ then

$$r_1r_2 \equiv a^2b^2 \equiv (ab)^2 \mod p$$

for some $a, b \in \mathbb{Z}_p^*$ and therefore $r_1r_2 \in R$. The mapping $x \mapsto r_1x$ is an injective function in the field so the set $\{r_1a \mid a \in R\}$ is a subset of R which is equal in cardinality to R. This means that the multiples of r_1 with elements of R form the entire set R, $r_1R = R$. Therefore the other multiples of r_1 must elements of N and hence $r_1n_1 \in N$ and $r_1N = N$. By the same argument, the multiples of n_1 with elements of R make up the set N so n_1n_2 must be an element of R, $n_1N = R$ and $n_1R = N$. □

Lemma 3.2.3. *Let p be an odd prime, then for any $n \in N$ there exist $a, b \in R$ such that $a + b = n$.*

Proof. Only half of the elements of $\mathbb{Z}_p^*$ are residues and it is always the case that 1 is a residue. Choose $c \in N$ such that c has the smallest value (when comparing numbers as integers) of all numbers in N. Therefore the elements $c - 1$ and 1 are in R. From Lemma 3.2.2 we have $\{cr \mid r \in R\} = N$ and therefore there exists $d \in R$ such that $n = cd$. Now we can write

$$(c-1)d + d = cd = n$$

and $a = (c-1)d$ and $b = d$ satisfy the statement of the lemma. □

Next we introduce a theorem known as 'Fermat's Little Theorem' as it will be used in the final proposition of this section.

Theorem 3.2.4. *(Fermat's Little Theorem) Let p be a prime number and let $a \in \mathbb{Z}_p^*$. Then*

$$a^{p-1} \equiv 1 \mod p.$$

Proof. Consider $\mathbb{Z}_p^* = \{1, 2, \dots, p-1\}$. If we multiply each of these elements by a we get $\{a, 2a, \dots, (p-1)a\} = \mathbb{Z}_p^*$ as multiplication by a is injective. The product of each of these sets must be equivalent modulo p so

$$\begin{aligned} 1 \cdot 2 \cdot \ \cdots \ \cdot (p-1) &\equiv a \cdot 2a \cdot \ \cdots \ \cdot (p-1)a \mod p \\ &\equiv 1 \cdot 2 \cdot \ \cdots \ \cdot (p-1) \cdot a^{p-1}. \end{aligned}$$

Multiplying each side of the equivalence by the inverses of the elements of $\mathbb{Z}_p^*$ gives the desired result. □

The final result we need from number theory is given by the following proposition.

Proposition 3.2.5. *If p is a prime and $p \equiv 3$ (mod 4) then the additive inverse of any residue of $\mathbb{Z}_p^*$ is a nonresidue.*

Proof. Rearranging Fermat's Little Theorem gives

$$a^{p-1} - 1 \equiv 0 \mod p$$

and when p is an odd prime this can be factorised to

$$(a^{(p-1)/2} - 1)(a^{(p-1)/2} + 1) \equiv 0 \mod p.$$

Each of the $p-1$ elements of $\mathbb{Z}_p^*$ is a solution to $a^{p-1} \equiv 1$ (mod p) but each is also a solution to one of

$$a^{(p-1)/2} \equiv 1 \mod p \qquad \text{or} \qquad a^{(p-1)/2} \equiv -1 \mod p$$

If we consider a residue $a \in \mathbb{Z}_p^*$ then $a \equiv b^2$ (mod p) for some $b \in \mathbb{Z}_p^*$. Therefore $a^{(p-1)/2} \equiv b^{p-1} \equiv 1 \mod p$ and the residues of $\mathbb{Z}_p^*$ satisfy $a^{(p-1)/2} \equiv 1 \mod p$. The degree of this polynomial is equal to the number of residues in the field which leaves the $(p-1)/2$ nonresidues of the field as solutions to $a^{(p-1)/2} \equiv -1 \bmod p$. If $p = 3 \bmod 4$ then $(p-1)/2$ is odd and since $p-1 \equiv -1 \bmod p$, we have

$$(p-1)^{(p-1)/2} \equiv -1 \mod p.$$

Therefore $p-1$ is a nonresidue, $p-1 \in N$. Whenever $a \in R$ then $-a \equiv a(p-1) \in N$ by Lemma 3.2.2. Therefore the inverse of a residue element is a nonresidue. □

This result is the only one which requires that $p \equiv 3$ (mod 4). Primes of the form $p \equiv 1$ (mod 4) have the contrasting property that the inverse of a residue is a residue and the inverse of a nonresidue is a nonresidue. It is for this reason that only the fields $GF(p)$ where $p \equiv 3$ (mod 4) are suitable in the construction given in section 3.5.

3.3 Fields of Characteristic 2

Extending a binary code by vectors from the orthogonal code is a technique used by MacWilliams and Sloane in [13] which inspired this method of finding ISD representable matroids. However, having established Proposition 3.2.1, there is no reason not to consider all fields with characteristic 2. In the remainder of this section we will use $\mathbb{F}$ to refer a field of characteristic 2.

In order to prove Conjecture 3.1.2 holds over $\mathbb{F}$ we give a method of constructing an ISD matroid N that has M as a minor. If M is a matroid which is representable over $\mathbb{F}$ we can consider the chain-group representation of M as a code C which is generated by the rows of a matrix representation of M. Recall from Chapter 1, that the orthogonal code $C^{\perp}$ consists of all codewords which are orthogonal to every vector in C using the dot product as a bilinear form. Tutte proved that $C^{\perp}$ is the chain-group for M^* [20] so we can ensure that M is ISD if $C = C^{\perp}$. We don't necessarily need such a strong result to show M is ISD since C and $C^{\perp}$ can represent the same matroid without being equal. An example of when $C \neq C^{\perp}$ but M is ISD is shown in Figure 3.1. The two matrices are generators a pair of codes which are orthogonal and both represent the ISD matroid R_6 (see Figure 1.1) over $GF(3)$, but are not equal.

For our purposes, it is easier ignore these types of inequivalent chain-groups and find matroids where $C = C^{\perp}$ instead. First we find a matroid where $C \subseteq C^{\perp}$ and

$$A_1 = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 2 \\ 0 & 1 & 0 & 2 & 1 & 2 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \quad A_2 = \begin{bmatrix} 2 & 1 & 0 & 1 & 0 & 0 \\ 2 & 2 & 2 & 0 & 1 & 0 \\ 1 & 1 & 2 & 0 & 0 & 1 \end{bmatrix}$$

Figure 3.1: Two representations for R_6.

then we can raise the dimension of the code until $\dim(C) = \dim(C^{\perp})$ using matroid extensions and coextensions. If at each step we preserve the fact that $C \subseteq C^{\perp}$ then it must reach some point when $C = C^{\perp}$ and the new matroid is ISD. We achieve this process by finding a matrix representation for a matroid where each row is orthogonal to every row of the matrix which implies $C \subseteq C^{\perp}$. Then we add vectors from $C^{\perp}$ to C while ensuring they are a coextension to the matroid and that the new codewords $\mathbf{x}$ are *self-orthogonal*, that is, $\mathbf{x} \cdot \mathbf{x} = 0$.

Lemma 3.3.1. *Let X be a collection of vectors $\{\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n\}$ such that $\boldsymbol{x}_i \cdot \boldsymbol{x}_j = 0$ for all $i, j \in \{1, 2, \ldots, n\}$. Then the code C generated by X is a subset of its orthogonal code $C^{\perp}$.*

Proof. Every codeword in C is a linear combination of vectors in X. For any $\mathbf{c} \in C$ we will show that $\mathbf{c}$ is in $C^{\perp}$ as well. For any $\mathbf{d}$ in C we get

$$\begin{aligned} \mathbf{c} \cdot \mathbf{d} &= (c_1 \mathbf{x}_1 + \cdots + c_n \mathbf{x}_n) \cdot (d_1 \mathbf{x}_1 + \cdots + d_n \mathbf{x}_n) \\ &= \sum_{1 \le i,j \le n} c_i d_i (\mathbf{x}_i \cdot \mathbf{x}_j) \\ &= \sum_{1 \le i,j \le n} c_i d_i (0) \\ &= 0 \end{aligned}$$

Therefore $\mathbf{c}$ is orthogonal to every codeword of C so $\mathbf{c} \in C^{\perp}$. Thus, $C \subseteq C^{\perp}$. □

Proposition 3.3.2. *If M is a matroid representable over a field $\mathbb{F}$ of characteristic 2 then there exists a matroid M_0 such that M_0 has a matrix representation over $\mathbb{F}$ where every row of the matrix is orthogonal to every other and M is a deletion minor of M_0. Additionally, if $r(M) = r$ then it is possible to find M_0 such that $|E(M_0)| \le |E(M)| + 2r - 1$.*

Proof. Let A be a matrix which represents M over $\mathbb{F}$. We let $r(M) = r$ so that A has r rows. We will add extra columns in order to find a matrix where every row is orthogonal to every row in the matrix. Lemma 3.3.1 indicates that this is enough to cause the chain-group C to fulfill $C \subset C^{\perp}$.

The first set of columns which need to be added will ensure that every row is orthogonal to the other rows, but not necessarily itself. This will increase M by at most $r-1$ new elements. We add the columns one at a time and let the rows of the current matrix be denoted $\mathbf{a}_i$ for $i \in \{1,2,\dots,r\}$. When we add the ith of these $r-1$ new columns we want to make row i orthogonal with every other row. This is done by adding a column consisting of $i-1$ zero entries followed by a 1 in row i. For $i < j \leq r$ the jth entry is given by $-\mathbf{a}_i \cdot \mathbf{a}_j$. The zero entries ensure that the ith row remains orthogonal with the previous rows which was established by adding the previous columns. The choice of the entries after the 1 make the row orthogonal with those which come after it.

After completing this process the only non-orthogonal vectors are due to vectors which are not self-orthogonal, meaning the dot product of the vector with itself is not zero. By adding at most r new columns, one for each row, we can resolve this issue. If $-\mathbf{a}_i \cdot \mathbf{a}_i \neq 0$ then we choose b_i such that $b_i^2 = -\mathbf{a}_i \cdot \mathbf{a}_i$ add a new column with b_i as its ith entry and zeros elsewhere. It is possible to find b_i because every element is a quadratic residue and this new addition to each row makes every row vector self-orthogonal. This construction of A_0 is shown below.

$$A_0 = \left[\begin{array}{c|cccc|ccccc}
 & 1 & 0 & \cdots & 0 & b_1 & 0 & \cdots & 0 & 0 \\
 & a_{1,2} & 1 & & 0 & 0 & b_2 & & 0 & 0 \\
A & \vdots & & \ddots & \vdots & \vdots & & \ddots & & \vdots \\
 & a_{1,r-1} & a_{2,r-1} & & 1 & 0 & 0 & & b_{r-1} & 0 \\
 & a_{1,r} & a_{2,r} & \cdots & a_{r-1,r} & 0 & 0 & \cdots & 0 & b_r
\end{array}\right]$$

The maximum number of new columns required to generate M_0 from M is $2r-1$ so $E(M_0) \leq E(M) + 2r - 1$. □

Now we know we can always extend a matroid over $\mathbb{F}$ to one where the chain-group C has the property $C \subseteq C^{\perp}$. We now introduce the idea of a coset which will be useful in continuing with these $\mathbb{F}$-representable matroids.

Definition 3.3.3. *If C is a subspace of $C^{\perp}$ then the coset of a vector $\mathbf{x}$ in $C^{\perp}$ is* *given by*

$$[\mathbf{x}] = \{\mathbf{x}+\mathbf{y} \mid \mathbf{y} \in C\}$$

Vectors $\mathbf{x}$ *and* $\mathbf{y}$ *in* $C^{\perp}$ *are in the same coset if* $\mathbf{x}-\mathbf{y} \in C$.

Theorem 3.3.4. *Let M be an $\mathbb{F}$-representable matroid where $\mathbb{F}$ is a field of characteristic 2. Let C denote a chain-group representation of M. If $C \subseteq C^{\perp}$ then M is a minor of an $\mathbb{F}$-representable ISD matroid N. If $r(M) = r$ it is possible to find N such that $|E(N)| \leq 2|E(M)| - 2r + 2$.*

Proof. We will find a way of repeatedly coextending a matroid until it is ISD, but the coextension choice will depend on the parity of the ground set. We will start with a matroid M_0 and find matroids M_i with associated chain-groups C_i and matrices A_i.

We will show that for each M_i it is possible to add a new row vector from the orthogonal space which is not self-orthogonal. Then we add a new column to this matrix made up of zero entries except for the last which is chosen such that the last row is self-orthogonal. The construction is shown in Figure 3.2 in the case that $\mathbf{x} \in C_i^{\perp}$ and $a^2 = -\mathbf{x}\cdot\mathbf{x} \neq 0$. We know that a is guaranteed to exist since every element is a residue.

$$A_{i+1} = \left[\begin{array}{c|c} & 0 \\ & 0 \\ A_i & \vdots \\ & 0 \\ \hline \mathbf{x} & a \end{array}\right]$$

Figure 3.2: Construction of A_{i+1} from A_i

Next we show that this process is possible for any matroid starting with $C \subseteq C^{\perp}$. First we make the following claim.

Claim. If every vector in $C_i^{\perp} - C_i$ is self-orthogonal and C_i has even length then $\mathbf{1} \in C_i$.

This is because if $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ and $\mathbf{x}\cdot\mathbf{x} = 0$ then $x_1^2 + x_2^2 + \cdots + x_n^2 = 0$. From Proposition 3.2.1 we can deduce that $\mathbf{x}\cdot\mathbf{1} = x_1 + x_2 + \cdots + x_2 = 0$ and thus $\mathbf{1}$ is orthogonal to every vector in $C^{\perp}$. Hence, $\mathbf{1} \in (C^{\perp})^{\perp} = C$.

We will use this to address, initially, the case when M_i has an even number of elements, $C_i \subseteq C_i^{\perp}$ and $\mathbf{1} \notin C$. There must be some vector $\mathbf{x}$ in $C_i^{\perp}$ which is not self-orthogonal and we can simply add this as a new row with $a = \mathbf{x} \cdot \mathbf{x}$ as an additional entry and zeros elsewhere in the column as in Figure 3.2.

Next, if M_i has an odd number of elements and $C_i \subseteq C_i^{\perp}$ then it is not possible for $\mathbf{1}$ to be in C because it is not self-orthogonal. Therefore there are certainly vectors in $C_i^{\perp} - C_i$ which are not self-orthogonal, but we also have to be careful not to introduce the vector $\mathbf{1}$ into C_{i+1}. We will consider the difference in dimension between C_i and $C_i^{\perp}$.

If $\dim(C_i) = \dim(C_i^{\perp}) - 1$ then a single vector $\mathbf{x} \in C_i^{\perp} - C_i$ along with C generates the space $C_i^{\perp}$. In this case it does not matter if we end up with $\mathbf{1}$ in C_{i+1} because $r(M_{i+1}) = r^*(M_{i+1})$ and we do not need to coextend further.

If $\dim(C_i) < \dim(C_i^{\perp}) - 1$ then $C_i^{\perp} - C_i$ contains at least two vectors which are not in the same coset and at least one which is not self-orthogonal. We will show there are at least two which are not self-orthogonal. Assume that only one of the vectors, $\mathbf{x}$, is not self-orthogonal and that another, $\mathbf{y}$, has $\mathbf{y} \cdot \mathbf{y} = 0$. Then let $\mathbf{z} = \mathbf{x} + \mathbf{y}$ so that

$$\begin{aligned} \mathbf{z} \cdot \mathbf{z} &= (\mathbf{x} + \mathbf{y}) \cdot (\mathbf{x} + \mathbf{y}) \\ &= \mathbf{x} \cdot \mathbf{x} + 2(\mathbf{x} \cdot \mathbf{y}) + \mathbf{y} \cdot \mathbf{y} \\ &= \mathbf{x} \cdot \mathbf{x} \neq 0 \end{aligned}$$

Therefore there is another vector $\mathbf{z} \in C_i^{\perp} - C$ which is not self-orthogonal or in the same coset as $\mathbf{x}$. Thus, there is a choice of vectors to add to C_i and we can choose one such that $\mathbf{1}$ is not in C_{i+1}.

We have now shown how this sequence of coextensions can be repeated until we reach a matroid with rank equal to its corank. We also need to show that it is possible to start this process. If $|E(M)|$ is even and its chain-group contains the vector $\mathbf{1}$ then it is necessary to let M_0 be equal to M with a loop as an extra element. This corresponds to an extra column of 0s in the chain-group and so C is still a subset of $C^{\perp}$. If M is not in the previous case then $M_0 = M$ and M is a contraction minor of an $\mathbb{F}$-representable ISD matroid.

We have given the construction for the matroid sequence and verified that it is possible to construct so it only remains to prove that this gives us an $\mathbb{F}$-representable ISD matroid which contains M as a minor.

Each matroid in the sequence is a coextension of the last which can be observed by noting that if the element corresponding to the last column of A_{i+1} is contracted then A_i is obtained. Therefore M_0 is a contraction minor of M_i for all i and M is either equal to M_0 or a single element deletion of M_0.

The method of coextending the A_i matrices ensured that every row was orthogonal to every other row so, by Lemma 3.3.1, $C_i \subseteq C_i^{\perp}$. The difference between the rank and corank decreases for each subsequent matroid so eventually they must be equal, at which point $C_i = C_i^{\perp}$. This means that $N = M_i$ is ISD and must be $\mathbb{F}$-representable because A_i is a representation for N over $\mathbb{F}$. The number of coextentions required to reach N is equal to $r^*(M) - r(M) = |E(M)| - 2r$, except it may take two additional elements to compensate for the chain-group of M containing $\mathbf{1}$. Therefore if N is found using this method then $|E(N)| \leq 2|E(M)| - 2r + 2$. □

3.4 Algebraically closed Fields

As we observed in the last section, adding new elements to matroids while trying to preserve self-orthogonality of the chain-group and increase the rank is partly dependent on the quadratic residues in the field. In an algebraically closed field $\mathbb{F}$ we generally do not use the term quadratic residue, but it remains the case that if $a \in \mathbb{F}$ then $a = b^2$ for some $b \in \mathbb{F}$. For that reason, we will say that every element of $\mathbb{F}$ is a residue when $\mathbb{F}$ is algebraically closed to be consistent with our other terminology.

If we look back to the proof of Proposition 3.3.2, it does not require anything from the field other than that every element is a residue. Therefore we can restate the proposition in terms of algebraically closed fields.

Proposition 3.4.1. *If M is a matroid representable over a field $\mathbb{F}$ which is algebraically closed then there exists a matroid M_0 such that M_0 has a matrix representation over $\mathbb{F}$ where every row of the matrix is orthogonal to every other and M is a deletion minor of M_0. Additionally, if $r(M) = r$ then it is possible to find M_0 such that $|E(M_0)| \leq |E(M)| + 2r - 1$.*

The related theorem for algebraically closed fields does not follow as directly, but the proof of Theorem 3.3.4 can be adapted. We also note here that the field should not have characteristic 2 in order for the following proof to work. Every field of characteristic 2 is already addressed in Theorem 3.3.4 so no results are lost by only considering those fields with other characteristics in the next theorem.

Theorem 3.4.2. *Let M be an $\mathbb{F}$-representable matroid where $\mathbb{F}$ is an algebraically closed field and char$(\mathbb{F}) \neq 2$. Let C denote a chain-group representation of M. If $C \subseteq C^{\perp}$ then M is a minor of an $\mathbb{F}$-representable ISD matroid. In addition, it is possible to find N such that $|E(N)| = 2|E(M)| - 2r(M)$.*

Proof. We follow the same method used in the proof of Theorem 3.3.4. Let $M_0 = M$ and we will construct a sequence of matroids M_i with matrix representation A_i and chain-group C_i. The method for finding A_{i+1} from A_i is again to append a new row from C_i with a new column which makes the row self-orthogonal. This is shown back in Figure 3.2.

If $\dim(C_i) < \dim(C_i^{\perp}) - 1$ then $C_i^{\perp} - C_i$ contains at least two vectors $\mathbf{x}$, $\mathbf{y}$ from different cosets. If either of these are not self-orthogonal then it can be used as the additional row. If neither are then $\mathbf{x} \cdot \mathbf{x} = 0$ and $\mathbf{y} \cdot \mathbf{y} = 0$ so we let $\mathbf{z} = \mathbf{x} + \mathbf{y}$ so that

$$\begin{aligned} \mathbf{z} \cdot \mathbf{z} &= (\mathbf{x}+\mathbf{y}) \cdot (\mathbf{x}+\mathbf{y}) \\ &= \mathbf{x} \cdot \mathbf{x} + 2(\mathbf{x} \cdot \mathbf{y}) + \mathbf{y} \cdot \mathbf{y} \\ &= 2(\mathbf{x} \cdot \mathbf{y}) \neq 0 \end{aligned}$$

It is here that we require that the characteristic of $\mathbb{F}$ is not 2 so that $2(\mathbf{x} \cdot \mathbf{y}) \neq 0$. This means that $\mathbf{z}$ is not self-orthogonal and we can use it as our new row in A_{i+1}.

If, instead, $\dim(C_i) < \dim(C_i^{\perp}) - 1$, then we note that there is only one coset in $C_i^{\perp}$ other than C_i. We take any vector $\mathbf{x}$ from the coset to append to C_i and add a column which makes the vector self-orthogonal. Then $C_{i+1} \subseteq C_{i+1}^{\perp}$ and $\dim(C_{i+1}) = \dim(C_{i+1}^{\perp})$ implies that M_{i+1} is ISD and therefore it cannot contain any loops. This ensures that the last entry in the last column is non-zero.

This proves that it is always possible to coextend M_i in such a way that M_{i+1} has $C_{i+1} \subseteq C_{i+1}^{\perp}$ and at some point we reach an ISD matroid. Therefore M is a contraction minor of an $\mathbb{F}$-representable ISD matroid N. The number of coextentions required is equal to $r^*(M) - r(M) = |E(M)| - 2r$. Therefore if N is found using this method then $|E(N)| = 2|E(M)| - 2r$. □

Using the results on fields of characteristic 2 and algebraically closed fields we can prove Theorem 3.1.1 which we restate here with an explicit bound on the size of the ISD matroid.

Theorem 3.4.3. *If M is a representable matroid then it is a minor of an ISD representable matroid N. Furthermore, if $|E(M)| = n$ and $r(M) = r$ then it is possible to find N such that $|E(N)| \leq 2n+2r$*

Proof. If M is representable over a field $\mathbb{F}$ then it is also representable over the algebraic closure of $\mathbb{F}$ which we will denote $\mathbb{F}'$. This field must have characteristic 2 or be an algebraically closed field that does not have characteristic 2. Therefore by Proposition 3.3.2 and Theorem 3.3.4 or by Proposition 3.4.1 and Theorem 3.4.2 M is a minor of an ISD $\mathbb{F}'$-representable matroid. The bound on the size of N is worse by two elements for the fields of characteristic 2 so that is the bound we use here. It takes at most $2r-1$ elements to extend an arbitrary $\mathbb{F}'$-representable matroid to a matroid M' where the chain-group C is a subset of $C^{\perp}$. It then takes no more than $r^*(M') - r(M') + 2 = n+1$ elements to produce an ISD matroid N. Hence, $|E(N)| \leq 2n+2r$. □

3.5 GF(p) for p=3 (mod 4)

In this section we give a constructive proof that if M is a matroid which is representable over $GF(p)$ where p is a prime and $p = 3 \pmod 4$ then there exists an ISD matroid N which is representable over the same field and contains M as a minor. First, however, it is necessary to apply the theory of residues and nonresidues to a vector space. Recall that we denote the set of residues of a field R, and the set of nonresidues N. The results of Lemmas 3.2.2 and 3.2.3 and Proposition 3.2.5 will be important in this section. Namely, that R and N are invariant under multiplication by elements of R and will be mapped to each other if multiplied by an element of N. Any element of N is the sum of two elements in R and, lastly, the the inverse of a residue is a nonresidue.

Lemma 3.5.1. *Let $\mathbf{x}$ and $\mathbf{y}$ be orthogonal, linearly independent vectors of $GF(p)^n$ for a prime p. If $\mathbf{x} \cdot \mathbf{x} \equiv a \in R$ and $\mathbf{y} \cdot \mathbf{y} \equiv b \in R$ then there is a vector $\mathbf{z}$ which is a linear combination of $\mathbf{x}$ and $\mathbf{y}$ and has $\mathbf{z} \cdot \mathbf{z} \in N$.*

Proof. Let $\mathbf{z} = c\mathbf{x} + d\mathbf{y}$ where $c, d \in GF(p)$ and then

$$\begin{aligned}\mathbf{z}\cdot\mathbf{z} &= (c\mathbf{x}+d\mathbf{y})\cdot(c\mathbf{x}+d\mathbf{y})\\ &= c^2(\mathbf{x}\cdot\mathbf{x}) + 2cd(\mathbf{x}\cdot\mathbf{y}) + d^2(\mathbf{y}\cdot\mathbf{y})\\ &= c^2(\mathbf{x}\cdot\mathbf{x}) + 2cd(0) + d^2(\mathbf{y}\cdot\mathbf{y})\\ &= c^2a + d^2b.\end{aligned}$$

Depending on the choice of c and d, c^2 and d^2 can take any value from R and therefore so can c^2a and d^2b, by Lemma 3.2.2. Lemma 3.2.3 asserts that we can choose c and d so that $c^2a + d^2b \in N$. □

Lemma 3.5.2. *Let* $\mathbf{x}$ *and* $\mathbf{y}$ *be orthogonal, linearly independent vectors of* $GF(p)^n$ *for a prime* $p = 3$ *(mod 4). If* $\mathbf{x}\cdot\mathbf{x} \equiv a \in R$ *and* $\mathbf{y}\cdot\mathbf{y} \equiv b \in N$ *then there is a vector* $\mathbf{z}$ *which is a linear combination of* $\mathbf{x}$ *and* $\mathbf{y}$ *and has* $\mathbf{z}\cdot\mathbf{z} \equiv 0$.

Proof. The proof follows the same reasoning as the proof for Lemma 3.5.1, but note that here $b \in N$. Using the same choice of $\mathbf{z} = c\mathbf{x} + d\mathbf{y}$ we again have $\mathbf{z}\cdot\mathbf{z} = c^2a + d^2b$. By Lemma 3.2.2, $c^2a \in R$ and so $-c^2a \in N$ by Proposition 3.2.5. Again using Lemma 3.2.2, d^2b can take any value in N so we let $d^2b = -c^2a$. Thus we can find a vector $\mathbf{z}$ such that $\mathbf{z}\cdot\mathbf{z} = 0$. □

As we saw in the previous section, a matroid is ISD if a chain-group representation C of the matroid is a equal to its orthogonal code $C^{\perp}$. We will again be constructing a matroid with this property and we will continue to use the same bilinear form, the dot product.

Theorem 3.5.3. *Let* M *be a matroid representable over* $GF(p)$ *for some prime* $p \equiv 3$ *(mod 4). Then there exists an ISD matroid* N *such that* N *is representable over* $GF(p)$ *and* M *is a minor of* N*. Furthermore, if* $|E(M)| = n$ *and* $r(M) = r$ *then it is possible to find the matroid* N *such that* $|E(N)| \leq 4n + 6r - 6$.

Proof. We will again be working with the code space corresponding to a matroid. First we need to extend M to a matroid where $C \subseteq C^{\perp}$ and we will then extend and coextend this matroid until $\dim(C) = \dim(C^{\perp})$ while retaining the property that $C \subseteq C^{\perp}$. At this point the new matroid will have $C = C^{\perp}$ so it must be an ISD matroid.

Starting with M we will show it is always possible to find an extension M_0 of M with a code space $C \subseteq C^{\perp}$. We simply need to ensure that the chosen generator for C, which is the matrix representation of M_0, contains vectors which are orthogonal to every other vector in the generator (Lemma 3.3.1). This can be accomplished by adding no more than $3r-1$ new elements to M where $r = r(M)$. The first $r-1$ of these columns start with $i-1$ zero entries followed by a one in the ith row for $i \in \{1,2,\dots,r-1\}$. The remaining $r-i$ entries are chosen so that each vector after the ith row is orthogonal to the ith one.

$$\left[\begin{array}{c|cccc|cccccccc}
 & 1 & 0 & \cdots & 0 & b_{1,1} & b_{1,2} & 0 & 0 & \cdots & \cdots & 0 & 0 \\
 & a_{1,2} & 1 & & 0 & 0 & 0 & b_{2,1} & b_{2,2} & & & 0 & 0 \\
A & \vdots & & \ddots & \vdots & \vdots & \vdots & & & & \ddots & \vdots & \vdots \\
 & a_{1,r-1} & a_{2,r-1} & & 1 & 0 & 0 & 0 & 0 & & \ddots & 0 & 0 \\
 & a_{1,r} & a_{2,r} & \cdots & a_{r-1,r} & 0 & 0 & 0 & 0 & \cdots & \cdots & b_{r,1} & b_{r,2}
\end{array}\right]$$

At most $2r$ more elements are needed to ensure that each vector is self-orthogonal in M'. If $\mathbf{x}$ is a vector of M extended by $r-1$ elements and $\mathbf{x}\cdot\mathbf{x} = a$ then adding the element b as an additional entry to $\mathbf{x}$ means $(\mathbf{x},b)\cdot(\mathbf{x},b) = a+b^2$. Therefore additional entries can only change $\mathbf{x}\cdot\mathbf{x}$ by adding a value of $GF(p)$ which is a residue. For each vector $\mathbf{x}$ of the generator matrix $\mathbf{x}\cdot\mathbf{x}$ is 0, a nonresidue or a residue. By Lemma 3.2.3 and Proposition 3.2.5 these vectors can be made self-orthogonal by adding 0, 1 or 2 entries respectively.

Now we can let M_0 be a matroid constructed from M in this way so M is a minor of M_0 and the chain-group representation of M_0 contains vectors which are orthogonal to all of the vectors in the chain-group. Let the code space corresponding to the chain-group be denoted C_0 and then we have $C_0 \subseteq C_0^{\perp}$. Next we begin an inductive process; if $\dim(C_i) = \dim(C_i^{\perp})$ then M_i is ISD, but if not then $\dim(C_i) < \dim(C_i^{\perp})$ and we can find a matroid M_{i+1} with code space C_{i+1} such that the difference in dimension between C_{i+1} and $C_{i+1}^{\perp}$ is one less than between C_i and $C_i^{\perp}$.

There are two distinct cases to consider: First, when $\dim(C_i^{\perp}) - \dim(C_i) > 1$ and second, when $\dim(C_i^{\perp}) - \dim(C_i) = 1$. We will use A_i to denote a matrix representation for M_i which is also a generator for C_i.

1. If M_i has a chain-group C_i with the property $\dim(C_i^{\perp}) - \dim(C_i) > 1$ then a generator for $C_i^{\perp}$ contains at least 2 vectors which are not in C_i. If there is

any vector $\mathbf{x}_n$ in $C_i^{\perp} - C_i$ with $\mathbf{x}_n \cdot \mathbf{x}_n = a \in N$ then $-a \in R$, by Lemma 3.2.5, and we can define A_{i+1} as shown below where $b^2 = -a$.

$$A_{i+1} = \left[\begin{array}{c|c} & 0 \\ & 0 \\ A_i & \vdots \\ & 0 \\ \hline \mathbf{x}_n & b \end{array}\right]$$

If, on the other hand, $C_i^{\perp}$ does not contain any vectors $\mathbf{x}$ with $\mathbf{x} \cdot \mathbf{x} \in N$, then $\mathbf{x} \cdot \mathbf{x} = 0$ or $r \in R$ for all $\mathbf{x} \in C_i^{\perp}$.

Suppose that all of the vectors in $C_i^{\perp} - C_i$ have the property $\mathbf{x} \cdot \mathbf{x} \in R$. Let $\mathbf{x}_r$ be one of these vectors and consider the vector space generated by C_i and $\mathbf{x}_r$ which we will denote $C_i \cup \mathbf{x}_r$. Having one additional generating vector, $\dim(C_i \cup \mathbf{x}_r) = \dim(C_i) + 1$ and therefore $\dim((C_i \cup \mathbf{x}_r)^{\perp}) = \dim(C_i^{\perp}) - 1$. Since $\mathbf{x}_r$ is in $C_i^{\perp}$ we know that $C_i \subseteq (C_i \cup \mathbf{x}_r)^{\perp}$ and the dimension of $(C_i \cup \mathbf{x}_r)^{\perp}$ is larger than that of C_i so $(C_i \cup \mathbf{x}_r)^{\perp} - C_i$ is non-empty. Let $\mathbf{y}_r$ be a vector in $(C_i \cup \mathbf{x}_r)^{\perp} - C_i$ and by assumption $\mathbf{y}_r \cdot \mathbf{y}_r \in R$. Now, however we have $\mathbf{x}_r, \mathbf{y}_r \in C_i^{\perp}$ which are orthogonal and linearly independent so by Lemma 3.5.1 there exists $\mathbf{z}$ in $C_i^{\perp}$ which is a linear combination of $\mathbf{x}_r$ and $\mathbf{y}_r$ and $\mathbf{z} \cdot \mathbf{z} \in N$. This contradicts our assumption and therefore if $C_i^{\perp}$ does not contain any vectors $\mathbf{x}$ with $\mathbf{x} \cdot \mathbf{x} \in N$ it must contain a vector $\mathbf{x}_0$ with the property that $\mathbf{x}_0 \cdot \mathbf{x}_0 = 0$.

Next we want to find a vector $\mathbf{y}_r$ in $C_i^{\perp} - (C_i \cup \mathbf{x}_0)^{\perp}$ with $\mathbf{y}_r \cdot \mathbf{y}_r \in R$. Note that $\mathbf{x}_0$ is in $(C_i \cup \mathbf{x}_0)^{\perp}$, and $C_i^{\perp}$ is larger in dimension than $(C_i \cup \mathbf{x}_0)^{\perp}$, so $C_i^{\perp}$ must contain a vector which is linearly independent of $C_i \cup \mathbf{x}_0$. Let $\mathbf{z}$ be such a vector and if $\mathbf{z} \cdot \mathbf{z} \in R$ then we can simply let $\mathbf{y}_r = \mathbf{z}$. If not, then $\mathbf{z} \cdot \mathbf{z} = 0$ and as $\mathbf{z}$ is not orthogonal to $\mathbf{x}_0$ we can let $\mathbf{y}_r = \mathbf{x}_0 + \mathbf{z}$. We are valid in choosing $\mathbf{y}_r$ this way as

$$\begin{aligned} \mathbf{y}_r \cdot \mathbf{y}_r &= (\mathbf{x}_0 + \mathbf{z}) \cdot (\mathbf{x}_0 + \mathbf{z}) \\ &= \mathbf{x}_0 \cdot \mathbf{x}_0 + 2(\mathbf{x}_0 \cdot \mathbf{z}) + \mathbf{z} \cdot \mathbf{z} \\ &= 2(\mathbf{x}_0 \cdot \mathbf{z}) \neq 0 \end{aligned}$$

and we know that $\mathbf{y}_r \cdot \mathbf{y}_r$ is not a nonresidue. Now we have vectors $\mathbf{x}_0$ and

$\mathbf{y}_r$ from $C_i^{\perp}$ such that

$$\begin{aligned}\mathbf{x}_0 \cdot \mathbf{y}_r &= \mathbf{x}_0 \cdot (\mathbf{x}_0 + \mathbf{z}) \\ &= \mathbf{x}_0 \cdot \mathbf{x}_0 + \mathbf{x}_0 \cdot \mathbf{z} \\ &= \mathbf{x}_0 \cdot \mathbf{z} \neq 0\end{aligned}$$

and we will use them to form A_{i+1} as shown below.

$$A_{i+1} = \left[\begin{array}{c|ccc} A_i & & \mathbf{0} & \\ \hline \mathbf{x}_0 & a & b & c \\ \mathbf{y}_r & d & e & 0 \end{array}\right]$$

In order to have $C_{i+1} \subseteq (C_{i+1})^{\perp}$ we need the rows of M_{i+1} to be orthogonal to each other and themselves. This means we need to find $a, b, c, d, e \in GF(p)$ with the properties:

(a) $a^2 + b^2 + c^2 \equiv -(\mathbf{x}_0 \cdot \mathbf{x}_0) \equiv 0$

(b) $d^2 + e^2 \equiv -(\mathbf{y}_r \cdot \mathbf{y}_r) \in N$

(c) $ad + be \equiv -(\mathbf{x}_0 \cdot \mathbf{y}_r) \not\equiv 0$

First, we are able to choose d and e which fulfill (b) by Lemma 3.2.3. Next we choose $\alpha, \beta, \gamma \neq 0$ which have the same properties as a, b, c in (a). Let α be any value, then $-\alpha^2 \in N$ by Proposition 3.2.5 and we can choose β and γ such that $\beta^2 + \gamma^2 \equiv -\alpha^2$ by Lemma 3.2.3. Now we want to ensure that $\alpha d + \beta e \not\equiv 0$ by permuting the labels on α, β and γ. This is certainly possible as α, β and γ are not all equal so permuting them will change the value of $\alpha d + \beta e$. Now we consider the effect of scaling the newly labeled α, β, γ by $k \neq 0$.

$$\begin{aligned}(k\alpha)^2 + (k\beta)^2 + (k\gamma)^2 &\equiv k^2\alpha^2 + k^2\beta^2 + k^2\gamma^2 \\ &\equiv k^2(\alpha^2 + \beta^2 + \gamma^2) \equiv 0\end{aligned}$$

Therefore $k\alpha$, $k\beta$ and $k\gamma$ also fulfill condition (a) and furthermore

$$k\alpha d + k\beta e \equiv k(\alpha d + \beta e).$$

Therefore by choosing the correct value for k we can get $k\alpha$, $k\beta$, d and e to satisfy condition (c) due to the fact multiplication is injective and $\alpha d + \beta e \not\equiv$

0. Thus let a, b and c equal $k\alpha$, $k\beta$ and $k\gamma$ respectively and we can construct the matrix above with the required conditions.

It must be possible to construct A_{i+1} by one of the methods shown above. Care was taken to ensure that there are non-zero entries in the new columns of the matrix and that the additional vectors are orthogonal to every other vector. Therefore these new matroids are formed by a single coextension, or two coextensions and an extension and $C_{i+1} \subseteq C_{i+1}^{\perp}$. A coextension raises the dimension of C_i by one and an extension raises the dimension of $C_i^{\perp}$ by one so in both of these methods above the dimension of C_i is increased by one with respect to $C_i^{\perp}$.

2. The second case occurs when $\dim(C_i^{\perp}) - \dim(C_i) = 1$. As $C_i \subseteq C_i^{\perp}$, the vector corresponding to each cocircuit is in $C_i^{\perp}$. This implies that every cocircuit is the union of circuits because if we repeated cancel entries of the vector corresponding to a cocircuit C with vectors corresponding to circuits which are subsets of C then we must reach a vector with minimal support, which is another circuit. Therefore the cocircuit is covered by circuits.

   Every circuit of M_i^* is a union of circuits of M_i which implies that M_i is a quotient of M_i^* by [16, 7.3.9]. There are only two cosets in $C_i^{\perp}$ including C_i. Take any vector $\mathbf{x}$ in $C_i^{\perp} - C_i$ and we generate A_{i+1} as follows

$$A_{i+1} = \left[\begin{array}{c|c} & 0 \\ & 0 \\ A_i & \vdots \\ & 0 \\ \hline \mathbf{x} & 1 \end{array}\right]$$

   Deleting the last column results in a matrix representation for M_i^* and contracting the last column gives the matrix A_i, a representation for M_i. By Lemma 1.1.5 M_{i+1} is ISD.

Thus, M is a minor of M_0 and M_0 is a minor of an ISD matroid $N = M_n$ for some n.

Finally, we prove that if M has n elements and rank r then the matroid N has no more than $4n + 6r - 6$ elements. As mentioned earlier, it takes a maximum of $3r - 1$ elements to extend M to M_0 so $E(M_0) \leq n + 3r - 1$. We can also deduce that $r(M_0) = r$ so $r^*(M_0) = (n+3r-1) - r = n+2r-1$. Thus, the difference in the rank and the corank of M_0 is $n+r-1$ which indicates that $N = M_{n+r-1}$ is ISD and requires at most three new elements for each step of the construction except for the last step which is guaranteed to take only one new element. Therefore $E(N) \leq n+3r-1+3(n+r-1)-2 = 4n+6r-6$. □

Chapter 4

Regular Matroids

4.1 Introduction

Regular matroids are a subset of the class of representable matroids. They are simply the class of matroids which are representable over every field, though there are several different characterisations. Some of these are presented here with more details given in [16].

Proposition 4.1.1. *The following statements are equivalent for a matroid M*

1. *M is regular.*
2. *M is representable over every field.*
3. *M is representable over GF(2) and GF(3).*
4. *M is representable by a totally unimodular matrix.*
5. *M is binary and orientable.*

Given the many ways in which they can be defined, it is not surprising that regular matroids have a number of unique properties and have been extensively studied. Of the results relating to regular matroids it is the following theorem of Lindström [11] which we will focus on in this chapter.

Theorem 4.1.2. *(Lindström) If a matroid M is simple and regular then it is not ISD.*

This is a fairly complete description of how the classes of ISD matroids and regular matroids intersect, but we extend this result further and here restate Theorem 1.2.5.

Theorem 4.1.3. *If a matroid is simple and regular, then it cannot be obtained by contraction from an ISD matroid.*

Before we can prove this theorem we give a property which is shared by matroids that can be generated by contracting ISD matroids.

Lemma 4.1.4. *If a matroid M is a contraction minor of an ISD matroid then every cocircuit of M is a union of circuits of M.*

Proof. If M is an ISD matroid then the set of circuits of M is exactly the set of cocircuits of M. If N is a contraction minor of M then there exists $X \subseteq E(M)$ such that $N = M/X$. A cocircuit of N is simply a cocircuit of M which has no intersection with X and as M is ISD it is also a circuit. A circuit of M with no intersection with X must be a union of circuits of N by [16, Exercise 2b pg. 105]. □

A *cycle* of a binary matroid is a union of circuits so we shall call matroids with the property that all cocircuits are unions of circuits *cyclic-cocircuit matroids*. All matroids which can be obtained by contracting ISD matroids are cyclic-cocircuit matroids, but it is not known whether the two classes are the same. We will in fact be proving the slightly stronger theorem from which Theorem 4.1.3 will directly follow.

Theorem 4.1.5. *If M is simple and regular then it is not a cyclic-cocircuit matroid.*

Before proving this theorem we will present the proof of Lindström's theorem and explain why it is not easily adapted to our proof. Then we will introduce concepts of connectivity and Seymour's decomposition theorem which together give us strong enough structural properties of regular matroids to prove Theorem 4.1.5.

4.2 Lindström's proof

Here we will outline Lindström's proof and show that the method he used is not likely to be useful in proving our extension. The way Lindström states his theorem is actually stronger than the way we phrased it earlier. He looks at connected, regular matroids and shows the only one which is ISD is $U_{1,2}$.

Theorem 4.2.1. *(Lindström) The uniform matroid $U_{1,2}$ is the only connected, regular ISD matroid.*

Proof. Let M be a connected, regular matroid. We will show that if C is a circuit of M then $|C| \leq 2$. Assume that C is a circuit containing more than two elements and let e and f be distinct elements of C. By [23, 5.1.1] there exists a cocircuit D such that $C \cap D = \{e, f\}$ and as M is ISD, D is also a circuit.

We now use circuits C and D to find a third circuit B which intersects the other two in the elements e and f. First, note that every circuit in M has even cardinality as they must intersect every cocircuit in an even number of elements and the circuits are cocircuits themselves. This means that M is bipartite and from this we can deduce that, being its own dual, M is Eulerian [22]. Therefore the entire groundset of M is a disjoint union of circuits. Now we take the symmetric difference of $E(M)$, C and D and note that $E(M) \triangle C \triangle D$ is a disjoint union of circuits and contains e and f. There must be a circuit B in $E(M) \triangle C \triangle D$ which contains the element e and since B cannot intersect either of the cocircuits C or D in a single element, it must contain f too. This gives us three circuits and cocircuits B, C and D, which each contain the elements e and f, but are otherwise disjoint.

Now we can use the orientability of regular matroids from [23, 10.4.3]. It states that we can label every element of the circuits and cocircuits of M with $+$ or $-$ to find a partition with the following property. If a circuit C has the partition $C = \{C^+, C^-\}$ and a cocircuit D has a partition $D = \{D^+, D^-\}$ then

$$|C^+ \cap D^+| + |C^- \cap D^-| = |C^+ \cap D^-| + |C^- \cap D^+|.$$

In addition we are allowed to choose the partitions in such a way that $C^+ = C$ and $C^- = \emptyset$ for one circuit or cocircuit; here we choose the circuit C. Next we consider e and f in the cocircuit D. As $e, f \in C^+$, they must each be in different parts of D to satisfy the equality above. By looking at the overlap of cocircuit D with circuit B we can similarly deduce that e and f have the same sign in the circuit B. Finally, we return to C, but this time as a cocircuit. The intersection with B forces e and f to be in different sets of the partition of cocircuit C.

This construction was not dependent on the choice of elements e and f, so by this same argument, any pair of elements of C should have different signs in the cocircuit C. This is a contradiction when $|C| > 2$ and therefore there cannot be any circuits with size greater than 2. As M is connected, this implies that every element is parallel with every other and the only ISD matroid of this type is $U_{1,2}$. □

The difficulty in applying this method to our theorem comes in finding B, C and D. This is because in a cyclic-cocircuit matroid it is not the case that circuits and cocircuits are equivalent.

Following Lindström's method we let M be a simple, regular cyclic-cocircuit matroid. If we assume C is a circuit which has more than two elements then we can still let $e, f \in C$ and use [23, 5.1.1] to find a cocircuit D where $C \cap D = \{e, f\}$. The difference here is that C is not guaranteed to be a cocircuit and D is a union of circuits, but it does not have to be a circuit itself. Therefore we are unable to continue the rest of the construction.

It is clear that we need to use something stronger than the methods used by Lindström. We find the strength we need in Seymour's decomposition theorem which we discuss in the next section.

4.3 Matroid connectivity

Connectivity in matroids is a way of generalising connectivity in graphs. We say a graph is *connected* if it consists of a single component in which any pair of vertices act as the endpoints of some path. This kind of connectivity does not directly apply to matroids. A graph G which is connected and a a graph H which is not connected can have the same graphic matroid. Instead we consider structures with a higher level of connectivity.

First, we review some terminology which will be useful when discussing graphic matroids. A matroid M is *graphic* if the groundset of M is equal to the edge set of a graph G and the set of circuits of M is in correspondence with the set of cycles of G. We can assume G is connected and we call a set of edges in G a *cut-set* if the graph acquired by deleting these edges from G is disconnected. A minimal set of edges with this property is a *bond* and the bonds of a graph are cocircuits of the graphic matroid.

Next, rather than only deleting edges, we give a way of describing graphs in which vertices have been removed. Let G be a graph and X be a set of vertices of G. Then $G-X$ is the graph obtained by deleting every vertex in X from G along with any edge which is incident with one of the deleted vertices. If G is connected, but $G-X$ is disconnected then we call X a *vertex cut* of G. The minimal number of vertices that must be removed from a connected graph in order for it to become disconnected is related to how connected the graph is. We say a graph G is *k-connected* if every vertex cut of G contains at least k vertices. We have to take care when it comes to complete graphs because they contain no vertex cuts as the graph will be empty before it becomes disconnected. It would not make sense for a finite graph to have infinite connectivity so we restrict the definition to exclude complete graphs. Another useful way of viewing connectivity is given by Menger's Theorem. Note that two paths are *internally disjoint* if the only vertices they have in common are the end points of the paths.

Theorem 4.3.1. *(Menger) A graph G is k-connected if and only if every pair of vertices are joined by k pair-wise internally disjoint paths.*

Thus, connectivity in graphs is related to how easily they can be disconnected by removing vertices. The analogue for matroids is defined by *separations*.

Definition 4.3.2. *Let M be a matroid and let $k \geq 1$ be an integer. A k-separation of M is a partition (X,Y) of $E(M)$ such that $|X|,|Y| \geq k$, and $r(X)+r(Y)-r(M) < k$.*

We say that a matroid is *n-connected*, if it has no *k-separation* for $k < n$. There is some equivalence between graph and matroid connectivity; If G is a connected graph with at least four edges then it is 3-connected if and only if $M(G)$ is 3-connected [16, 8.1.9]. Connectivity properties also behave well under duality. If a matroid is n-connected then so is its dual. Finally, to simplify the most common forms of connectivity, a 1-connected graph is often simply called connected. As previously mentioned, all matroids are 1-connected, so a connected matroid refers to 2-connectedness.

Here we introduce one final notion of connectivity in matroids. Whereas a 4-connected matroid has no 3-separations, an *internally 4-connected* matroid is permitted to have a 3-separation (X,Y) as long as $|X| = 3$ or $|Y| = 3$. A 3-separation of this kind does not provide a good method of decomposition, something we will revisit later.

The following proposition puts a lower bound on the number of elements in each circuit of a highly connected matroid.

Proposition 4.3.3. *Let M be an n-connected matroid. If $|E(M)| > 2(n-1)$ then every circuit in M contains at least n elements.*

Another concept associated with connectivity is matroid sums. These are operations which form larger matroids from smaller components. We will use Seymour's definition [18] for how 1-, 2- and 3-sums act on binary matroids.

Definition 4.3.4. *Let M_1 and M_2 be binary matroids where one of the following sets of conditions holds.*

1. *$E(M_1) \cap E(M_2) = \emptyset$ and $E(M_1), E(M_2) \neq \emptyset$.*
2. *$E(M_1) \cap E(M_2) = \{e\}$ where e is an element which is not a loop or coloop of M_1 or M_2 and $|E(M_1)|, |E(M_2)| \geq 3$.*
3. *$E(M_1) \cap E(M_2) = \{Z\}$ where Z is a 3 element circuit of M_1 and M_2 which contains no cocircuit of M_1 or M_2, and $|E(M_1)|, |E(M_2)| \geq 7$.*

Define a new matroid M by letting $E(M)$ be the symmetric difference of $E(M_1)$ and $E(M_2)$, and the set of cycles of M be the symmetric difference of cycles in M_1 and M_2. Then, depending on which properties are fulfilled above, M is a 1-, 2-, or 3-sum of M_1 and M_2 respectively. This is denoted

$$M = M_1 \oplus_i M_2 \qquad i \in \{1,2,3\}.$$

It is conventional to call a three element circuit of a matroid a *triangle* and these occur frequently when discussing 3-sums. Another convention we will use, in the case of 2-sums and 3-sums, is to call e and Z the *guts point* and the *guts line* respectively. They form the part of the matroid where M_1 and M_2 are joined and the degree of the sum indicates how strongly connected the resulting matroid is. If $M = M_1 \oplus_k M_2$ then $(E(M_1) \cap E(M), E(M_2) \cap E(M))$ is a k-separation of M. This also gives us a way of associating matroid sums with connectivity.

Proposition 4.3.5. *Let M be a binary matroid. For $n = 2,3$, M is n-connected if and only if*

$$M \neq M_1 \oplus_k M_2$$

for $k < n$. Similarly M is internally 4-connected if and only if

$$M \neq M_1 \oplus_k M_2$$

where $k = 1,2,3$.

We now have a way of describing matroids in terms of their connectivity and how easily they can be decomposed into smaller matroids. Restricted to regular matroids, Seymour's decomposition theorem gives a very good description of their structure. The theorem mentions the matroid R_{10}, for which a representation over $\mathbb{R}$ is given in Figure 4.1.

$$\begin{array}{cccccccccc}
a & b & c & d & e & f & g & h & i & j \\
\end{array}$$
$$\begin{bmatrix}
1 & 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 & 1 \\
0 & 1 & 0 & 0 & 0 & 1 & -1 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 1 & -1 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & -1 & 1 \\
0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & -1
\end{bmatrix}$$

Figure 4.1: A representation of R_{10} over $\mathbb{R}$

Theorem 4.3.6. *(Seymour) Every regular matroid M may be constructed by means of 1-, 2-, and 3-sums, starting with internally 4-connected matroids each isomorphic to a minor of M and each either graphic or cographic or isomorphic to R_{10}.*

This means internally 4-connected matroids which are graphic, cographic or isomorphic to R_{10} act as the smallest building blocks for all regular matroids. We can use Theorem 4.3.6 to break down matroids into their smallest parts which will be crucial in proving Theorem 4.1.5.

4.4 Proof of Theorem 4.1.5

In this section we show that the class of simple, regular matroids is disjoint from the class of cyclic-cocircuit matroids. We will prove Theorem 4.1.5 by using Seymour's decomposition theorem. By assuming that matroids with these properties exist and considering the connectivity of the resulting matroids we will arrive at a contradiction.

The smallest components of regular matroids, as demonstrated by the decomposition theorem, consist of graphic matroids, cographic matroids, and matroids isomorphic to R_{10}. For this reason we will first prove a number of propositions about how these three types of matroid behave with respect to being cyclic-cocircuit matroids.

Initially, we look at matroids which are already internally 4-connected and cannot be constructed with 1-, 2- and 3-sums.

Proposition 4.4.1. *If M is a non-empty, simple, cyclic-cocircuit matroid, then M is not graphic.*

Proof. Assume M is a counterexample and let G be a graph such that $M = M(G)$. Since M is simple, G does not contain any loops. Let H be a connected component of G where H contains more than one vertex. Note that if there is no such H then G is trivial because it has no edges. Next we choose any vertex v of H. If we repeatedly delete edges incident with v then v is no longer connected to any other vertex. This means the set of edges adjacent to v forms a cut-set and there is a subset of these edges which forms a bond of the graph. This is a cocircuit of M which consists of edges adjacent to a single vertex of G. For this cocircuit to be a union of circuits, every one of the edges must be in a non-trivial parallel class, but this cannot happen if M is simple. Therefore our assumption that M is a counterexample was incorrect. □

Proposition 4.4.2. *If M is a non-empty 3-connected, regular, cyclic-cocircuit matroid then M is not cographic.*

Proof. Let G be a graph such that $M = M^*(G)$. Using properties of connectivity, when $M^*(G)$ is 3-connected it follows that $M(G)$ is 3-connected and therefore G is 3-connected. We can now apply Theorem 4.3.1 to G and thus every pair of vertices in G must be joined by 3 pair-wise internally disjoint paths. Take an edge e and let its incident vertices be denoted v and w. We can now choose two additional paths p_1, p_2 between v and w so that e, p_1 and p_2 are disjoint. This allows us to construct the cycles $p_1 \cup e$ and $p_2 \cup e$ which intersect in the edge e.

Suppose that $p_1 \cup e$ is a union of bonds of G. One of these bonds must contain e and that bond intersects with the cycle $p_2 \cup e$ in only the edge e. However, it is not possible that a circuit and a cocircuit intersect in exactly one element. Thus we have a contradiction and we have found a cycle of G which is not a union of bonds of G. This corresponds to a cocircuit of $M^*(G)$ which is not a union of circuits of $M^*(G)$ and therefore $M^*(G)$ is not a cyclic-cocircuit matroid. □

Proposition 4.4.3. *If M is a cyclic-cocircuit matroid then M is not isomorphic to R_{10}.*

Proof. Refer to the representation for R_{10} given in Figure 4.1. We can observe that the closure of $\{a,b,c,d\}$ contains g and h and forms a hyperplane. Therefore the complement $\{e,f,i,j\}$ is a cocircuit. However, looking at the elements $\{e,f,i,j\}$, f is the only one with an entry in the second row and i is the only element with an entry in the third row. Therefore neither f nor i are part of a dependent set contained in $\{e,f,i,j\}$. This means that $\{e,f,i,j\}$ is an example of a cocircuit which is not the union of circuits and R_{10} is not a cyclic-cocircuit matroid. □

It now follows from Theorem 4.3.6 and Propositions 4.4.1, 4.4.2 and 4.4.3 that if a regular matroid is internally 4-connected it cannot be cyclic circuit. Next we give a similar set of restrictions for the cases when a cyclic-cocircuit matroid M contains 2- or 3-sums. It may be that not every cocircuit in one of the internally 4-connected components of M is cyclic. This is the result of the weaker connectivity between the components and the way the matroid sums behave. In a 2-sum there is an element in each of the constituent matroids which is not part of M and in a 3-sum there is a triangle of each matroid which is not present in M.

Proposition 4.4.4. *Let M be a cyclic-cocircuit matroid. Let M_1 and M_2 be matroids such that*

$$M = M_1 \oplus_i M_2$$

for $i \in \{2,3\}$. If C^* is a cocircuit of M_1 and $C^* \subseteq E(M)$ then C^* is cyclic in M_1.

Proof. Let C^* be a cocircuit of M_1 such that $C^* \subseteq E(M)$. Then $E(M_1) - C^*$ is a hyperplane of M_1 which contains the guts point or line so $E(M) - C^*$ is a hyperplane of M and therefore C^* is cocircuit of M. As M is a cyclic-cocircuit matroid, C^* must be a cycle of M. This cycle does not intersect M_2 and it must be a symmetric difference of cycles of M_1 and M_2. In a 2-sum there is no cycle of M_2 such that the symmetric difference with a cycle from M_1 has no intersection with M_2 so C^* must simply be a cycle from M_1. In a 3-sum the only way a non-empty cycle of M_2 has a symmetric difference with a cycle of M_1 which does not contain any elements of M_2 is if the cycle from M_2 is $E(M_1) \cap E(M_2) = Z$ and the cycle from M_1 contains Z. Then the cycle C^* of M along with Z is a cycle in M_1 and by taking the symmetric difference of cycles $C^* \cup Z$ and Z we see that C^* is cyclic in M_1. □

We now show that even when not every cocircuit is required to be cyclic the components cannot be regular. First we consider components of a 2-sum.

Proposition 4.4.5. *Let M be an internally 4-connected, regular matroid with $|E(M)| \geq 4$. There is no element $e \in E(M)$ such that every cocircuit not containing e is a union of circuits.*

Proof. Assume the conclusion is false and let M be a counterexample. Since M is internally 4-connected and regular, M is graphic, cographic or isomorphic to R_{10} by Theorem 4.3.6.

If M is graphic and $M = M(G)$ then G can only have two vertices. If there are more than two vertices then at least one vertex v is not incident with the edge e. The set of edges incident with v contains a cocircuit which is not a union of circuits as none of these edges are in parallel pairs. If G has only two vertices then it consists of a single parallel class. This cannot form an internally 4-connected matroid as a 3-connected matroid with at least 4 elements does not contain any circuits of size 2 by Proposition 4.3.3.

If instead M is cographic with $M = M^*(G)$ then again G must contain the edge e and every cycle of the graph not containing e is a union of bonds. Consider an edge f which is distinct from e. Let the two vertices it is incident with be denoted v and w. As G is 3-connected, v and w have a further two pairwise edge disjoint paths between them by Menger's Theorem. At most, one of these paths contains e and the other path along with f forms a cycle not containing e. If this cycle were a union of bonds then one bond must contain f and would intersect the other cycle in exactly one element. This again contradicts the fact that a matroid cannot contain a circuit and a cocircuit which have one element in their intersection. Therefore there are no cographic matroids with the required properties.

Finally, it is straightforward to check that R_{10} is not a suitable choice for M. Each element in R_{10} is equivalent so if there were an element e with the desired properties then we can find an isomorphism which maps it to the element a given in the proof of Proposition 4.4.3. However, in that proof we give a cocircuit which is not cyclic and does not contain a. Therefore there is no element of R_{10} that can be labeled e such that every cocircuit which doesn't contain e is a union of circuits. □

Next we show that matroids which form a cyclic-cocircuit matroid after a 3-sum, cannot be regular.

Proposition 4.4.6. *Let M be a 3-connected, graphic or cographic matroid with $|E(M)| \geq 7$. There is no three element circuit $Z \in E(M)$ such that every cocircuit which is disjoint from Z is a union of circuits.*

Proof. As previously stated, we know that M is graphic, cographic or isomorphic to R_{10} by Theorem 4.3.6. In this case, however, R_{10} is not an option worth investigating as it does not contain a three element circuit. Instead we only need to prove that M cannot be graphic or cographic.

If M is graphic then $M = M(G)$ for some graph G and we know G contains the cycle Z. It is not possible for any of the edges in Z to be in a non-trivial parallel class. Any additional edge on this triangle brings the total number edges to at least four. This leads to a contradiction because Proposition 4.3.3 shows that a 3-connected matroid with at least four elements cannot have any parallel pairs.

We choose an edge e not contained in Z which we are guaranteed because M has at least 7 elements. Then there is a vertex v which is not incident with any edges of Z. The set of edges incident with v contains a cocircuit which is only the union of circuits if it is made up of parallel pairs. Again, Proposition 4.3.3 indicates this is not the case. Therefore M is not graphic.

This leaves the possibility that M is cographic. If this is the case then we should be able to find a graph G such that $M = M^*(G)$. Thus G should contain a three element bond Z and every cycle which does not contain any elements of Z should be a union of bonds. Again note that G contains no parallel pairs because it is 3-connected. Now we can apply Theorem 4.3.1. First take any edge $e \notin Z$ and denote its incident vertices v and w. There are three edge disjoint paths between v and w because G is 3-connected. One of these is e, one path p_1 might pass through two edges of Z, but at least one other path p_2 doesn't intersect Z. We can create a cycle $p_2 \cup e$ which is not the union of bonds since no bond will contain e or it will intersect the cycle $p_1 \cup e$ in exactly one element which is a contradiction. Therefore M is not cographic. □

One of the last results we introduce before putting everything together is to show that it is possible to isolate a graphic or cographic component of a matroid through a single separation.

Definition 4.4.7. *Let M be a binary matroid which is 3-connected. A leaf is a minimal set $X \in E(M)$ such that $|X| \geq 4$ and $(X, E(M) - X)$ is a 3-separation.*

Lemma 4.4.8. *If M is a binary matroid which is 3-connected, but not internally 4-connected, then M contains a pair of disjoint leaves.*

Proof. Let M be a binary matroid which is 3-connected and not internally 4-connected. Then there must be a partition (X,Y) of $E(M)$ which is a 3-separation with $|X|,|Y| \geq 4$. Each of X and Y is a leaf or contains a leaf of M. Therefore M contains two disjoint leaves, one which is a subset of X and one which is a subset of Y. □

Lemma 4.4.9. *Let M be a regular matroid and let X be a leaf of M. Then there exists a matroid M_1 such that $E(M_1) \cap E(M) = X$ and M_1 is graphic or cographic.*

Proof. Let X be a leaf of the matroid M. By [18, 2.9], there exist matroids M_1 and M_2 such that

$$M = M_1 \oplus_3 M_2$$

and $X = E(M_1) - E(M_2)$. Therefore $X = E(M_1) \cap E(M)$. Next we observe that if M_1 has a 2-separation it is due to parallel classes on the elements of the triangle $Z = E(M_1) \cap E(M_2)$ [18, 4.3]. However, we chose X to be minimal so any elements on the guts line of M must belong to M_2 so M_1 contains no parallel pairs and is 3-connected.

Now assume that M_1 is not graphic or cographic. By [18, 14.2], M_1 has a minor isomorphic to R_{10} or R_{12}. If M_1 has an R_{10} minor then M_1 itself is isomorphic to R_{10}, but this is a contradiction as M_1 would contain no triangles and could not be a component of a 3-sum. Therefore M_1 has a minor isomorphic to R_{12} and from [18, 9.2], we see that M_1 has an exact 3-separation (X',Y') with $|X'|,|Y'| \geq 6$. Without loss of generality we let $|Z \cap Y'| \geq 2$ so that X' is the part of the partition with minimal intersection with Z. Then $(X' - Z, E(M) - (X' - Z))$ is a 3-separation of M, but $|X' - Z| \geq 4$ and $X' - Z$ is properly contained in X which contradicts our choice of X as a leaf. Therefore M_1 must be graphic or cographic. □

Next we put together the results on internally 4-connected matroids so that we can turn to matroids with lower connectivity and prove the extension to Lindström's Theorem.

Proposition 4.4.10. *Let M be a simple, regular matroid which is a cyclic-cocircuit matroid. Then M is not internally 4-connected.*

Proof. If M is regular and internally 4-connected then it must be graphic, cographic or isomorphic to R_{10} by Theorem 4.3.6. Propositions 4.4.1, 4.4.2 and 4.4.3 prove these possibilities are not valid and thus M is not internally 4-connected. □

Proposition 4.4.11. *Let M be a simple, regular matroid which is cyclic-cocircuit. Then M is not 3-connected.*

Proof. Let us make the assumption that there exists a simple, regular matroid which is 3-connected in addition to being a cyclic-cocircuit matroid. Let M be a minimal example of such a matroid. We know M cannot be internally 4-connected from Proposition 4.4.10. Then, by Lemma 4.4.8 and Lemma 4.4.9, there exist matroids M_1, M_2 such that

$$M = M_1 \oplus_3 M_2$$

and M_1 is graphic or cographic. We will let Z denote the three element circuit in common between M_1 and M_2. Now we can look at the structure imposed on M_1 by M. Every cocircuit of M_1 which does not intersect Z must be a union of circuits of M_1, by Proposition 4.4.4. Applying Proposition 4.4.6 to M_1 results in a contradiction so our assumption was incorrect. □

Now we can prove the main theorem.

Proof of 4.1.5. Assume that M is a minimal counterexample and therefore it must be 2-connected. If M were not 2-connected then

$$M = M_1 \oplus_1 M_2$$

and both M_1 and M_2 would also be simple, regular and cyclic-cocircuit so M would not be minimal. We know that M is not 3-connected by Proposition 4.4.11. As M

is 2-connected, but not 3-connected we can find matroids M_1 and M_2 such that

$$M = M_1 \oplus_2 M_2$$

and $E(M_1) \cap E(M_2) = e$. We take M_1 to be as small as possible and prove that M_1 must be 3-connected. Assume for a contradiction that M_1 is not 3-connected, thus

$$M_1 = M_3 \oplus_2 M_4.$$

Without loss of generality we can let $e \notin E(M_3)$ and so there must be a separate decomposition of M such that $M = M_3 \oplus_2 M_5$ for some matroid M_5. This is a contradiction as $|E(M_3)| < |E(M_1)|$. Therefore M_1 must be 3-connected.

Propositions 4.4.4 and 4.4.5 prove that M_1 cannot be internally 4-connected. Therefore we can apply Lemma 4.4.8 which shows M_1 has 2 disjoint leaves, so there must be one which does not contain e. Therefore, by Lemma 4.4.9, we can find a sum,

$$M_1 = M_3 \oplus M_4,$$

where M_3 is graphic or cographic and does not contain e. Again we let Z denote the common ground set elements of M_3 and M_4.

For the 3-sum to be well defined $|E(M_3)| \geq 7$ and Proposition 4.4.4 says that every cocircuit of M_3 which does not intersect Z is the union of circuits. This is not possible as shown by Proposition 4.4.6 and therefore M is not a counterexample. □

Corollary 4.4.12. *If M is a cosimple, regular matroid then M cannot be obtained by deleting elements from an ISD matroid.*

Chapter 5

Frame Matroids

5.1 Biased Graphs and Frame Matroids

A biased graph Ω consists of a graph where some of the cycles in the graph are *balanced* cycles and the remainder are *unbalanced* cycles. In a biased graph we denote the set of balanced cycles B and we can describe the biased graph as the pair (G,B). The only restriction on the set of balanced cycles of a biased graph relates to theta subgraphs. A *theta subgraph*, pictured on the right of Figure 5.1, is a set of three internally disjoint paths between two vertices. By taking any pair of these paths we find that a theta subgraph contains three cycles and in a biased graph 0, 1 or 3 of these cycles can be balanced. That is, a theta subgraph cannot contain precisely two balanced cycles. We say a biased graph Ω is *balanced* when every cycle of Ω is balanced.

Whereas graphs give rise to graphic matroids, biased graphs generate frame matroids. Before we can describe these matroids we need to introduce the two remaining substructures of biased graphs which are shown in Figure 5.1. Pictured

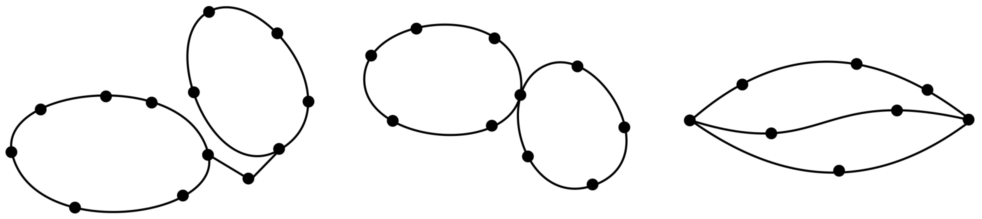

Figure 5.1: Handcuffs and a theta graph.

first is an example of *loose handcuffs*, a pair of cycles with a minimal path from one to the other. The second structure is a pair of cycles that share a single vertex and these are called *tight handcuffs*.

Now we can describe the frame matroid $M(\Omega)$ which is generated from the biased graph Ω. As in graphic matroids, the ground set of $M(\Omega)$ is given by the edges in Ω. The circuits of $M(\Omega)$ are the minimal sets of edges which form balanced cycles, loose handcuffs, tight handcuffs or theta graphs. This means that all balanced cycles are circuits and any of the three structures in Figure 5.1 which do not contain a balanced cycle are also circuits of $M(\Omega)$.

Another way of characterising frame matroids is given by Zaslavsky [24].

Proposition 5.1.1. *M is a frame matroid if and only if there exists a matroid N with a basis B such that $N \backslash B = M$ and for all $e \in E(M)$, the unique circuit contained in $B \cup e$ has at most 3 elements.*

The naming of frame matroids is made more apparent by this proposition. The basis B acts as a frame in the matroid N and every element of $E(N)$ lies on a line containing two elements of B. Therefore a frame matroid M is simply what remains of N when the basis B is deleted.

It is also useful, at this point, to mention the rank function of a frame matroid. The dependent sets of $M(\Omega)$ are those which contain a balanced cycle of Ω or one of the structures in Figure 5.1. Therefore the largest independent set in a component of Ω can be found by taking a maximal tree and one additional edge as long as together this set of edges does not contain a balanced cycle. Any larger set of edges must contain two distinct cycles and therefore must contain a pair of handcuffs or a theta graph and is not independent. However, in a balanced component there are no unbalanced cycles so the largest independent set is simply a maximal tree. Thus, in an unbalanced component of Ω the size of the largest independent set matches the number of vertices of the component, and in a balanced component the largest independent set is one smaller.

Proposition 5.1.2. *Let Ω be a biased graph. The rank of $M(\Omega)$ is equal to the number of vertices in Ω minus the number of balanced components.*

The rank of the matroid is decreased when the number of balanced components increases. Therefore a cocircuit C of $M(\Omega)$ corresponds to a minimal set of edges in Ω such that $\Omega - C$ contains one more balanced component than Ω.

We now introduce the class of matroids called swirls as described in [16, pg. 664]. A swirl of rank r contains elements in pairs $\{a_0, b_0, a_1, b_1, \ldots, a_{r-1}, b_{r-1}\}$. The non-spanning circuits are given by $\{a_i, b_i, z_{i+1}, z_{i+2}, \ldots, a_{i+k}, b_{i+k}\}$ where z is either a or b and $1 \leq k \leq r-2$ with subscripts calculated modulo r along with balanced r element cycles which intersect each pair $\{a_i, b_i\}$ in exactly one element.

We will investigate the form Ω can take if $M(\Omega)$ is ISD and come to the following result. This is a restatement of Theorem 1.2.6.

Theorem 5.1.3. *Let M be a frame matroid. If M is ISD and 3-connected, then it is a swirl.*

In this case, the graph G underlying Ω must be as shown in Figure 5.2. We will prove this in the next section.

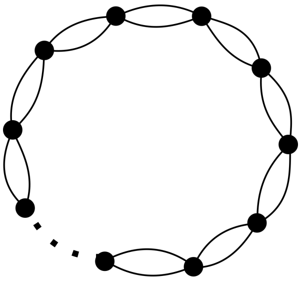

Figure 5.2: Structure for Ω when $M(\Omega)$ is ISD and 3-connected.

5.2 ISD Frame Matroids

In this section we characterise ISD frame matroids by identifying structures that do not occur in a biased graph Ω if $M(\Omega)$ is ISD. First, note that if Ω is a biased graph and X is a set of edges of Ω then we can define a new biased graph $\Omega - X$. If $\Omega = (G, B)$ then the graph underlying $\Omega - X$ is $G - X$ and the set of balanced cycles of $\Omega - X$ are the cycles in B which do not intersect X.

We want to restrict ourselves to matroids which are connected. Any ISD matroid which is not connected is the direct sum of two smaller ISD matroids so we only need to consider the connected components. This will ensure that Ω is also connected.

Now we will prove a simple lemma which will form the base of many proofs.

Lemma 5.2.1. *Let Ω be a connected biased graph such that $M(\Omega)$ is ISD and connected. If v is any vertex in Ω then the set of edges incident with v must contain a circuit of $M(\Omega)$.*

Proof. Let v be a vertex of Ω and E_v be the set of edges incident with v. As v becomes newly isolated in $\Omega - E_v$, it must be a balanced component of $\Omega - E_v$. If v was originally in an unbalanced component then v is a balanced component in $\Omega - E_v$ and if v was in a balanced component then all of the components that are generated in $\Omega - E_v$ are balanced. Either way there is an increase in balanced components and therefore $r(\Omega - E_v) < r(\Omega)$. Thus, Ω must contain a cocircuit $C \subseteq E_v$ and since $M(\Omega)$ is ISD, C is a circuit of $M(\Omega)$ contained in E_v. □

If $M(\Omega)$ is ISD then we already know that there are no loops in $M(\Omega)$ as no circuit intersects any cocircuit in a single element. A parallel pair in $M(\Omega)$ must also be a series pair in an ISD matroid, but the only connected matroid containing a parallel pair which is a series pair is $U_{1,2}$. Therefore, if $M(\Omega)$ is a connected ISD matroid other than $U_{1,2}$ then $M(\Omega)$ has no circuits of size one or two and in turn Ω has no balanced cycles of size one or two.

Lemma 5.2.2. *Let Ω be a biased graph where $M(\Omega)$ is ISD and connected, but not the uniform matroid $U_{1,2}$. If v is any vertex of Ω then the set of edges incident with v contains a pair of tight handcuffs or a theta subgraph.*

Proof. From Lemma 5.2.1 we know that every vertex v in Ω is incident with a circuit of $M(\Omega)$. As Ω contains no balanced cycles of size 2, the edges incident with v must contain every edge of one of the structures in Figure 5.1. This is only possible for a pair of tight handcuffs with 3 or 4 edges or a theta graph of 3 edges in parallel. □

The importance of this result is that since neither of these structures contains a balanced cycle, every vertex of Ω is incident with an unbalanced cycle of size two.

Corollary 5.2.3. *Let Ω be a biased graph where $M(\Omega)$ is ISD and connected, but not the uniform matroid $U_{1,2}$. If v is any vertex of Ω then v is incident with an unbalanced cycle.*

This is our most useful tool in proving the next results.

Lemma 5.2.4. *Let Ω be a biased graph such that $M(\Omega)$ is ISD and connected and Ω contains vertices v and w, and more than three edges which are incident with both v and w. Then $M(\Omega) = U_{2,4}$.*

Proof. Suppose that v and w are vertices of Ω and there are more than three edges incident with v and w. There are more than two edges so $M(\Omega)$ is not $U_{1,2}$ and Ω does not contain a balanced cycle. Therefore three of the edges between v and w form a theta subgraph θ which is a cocircuit of $M(\Omega)$. This means in the graph $\Omega - \theta$ there will be a balanced component since the rank of the matroid must be decreased by one. Since v and w had more than three incident edges, $\Omega - \theta$ is connected and therefore it has to be balanced. By Corollary 5.2.3 any vertex of Ω is incident with an unbalanced cycle and so if there are any vertices other than v and w they will be incident with an unbalanced cycle which remains in $\Omega - \theta$. This cannot happen if $\Omega - \theta$ is balanced so Ω and $\Omega - \theta$ only contain two vertices and a single edge incident with them. Any additional edges would create unbalanced loops or an unbalanced parallel pair. Therefore Ω contains the theta graph with one additional edge and $M(\Omega)$ is equal to $U_{2,4}$. □

Proposition 5.2.5. *If Ω is a biased graph and the associated frame matroid $M(\Omega)$ is ISD and connected, then every edge of Ω which is not a loop is in a nontrivial parallel class.*

Proof. In this proof we will use case analysis to show that if there is a pair of adjacent vertices with precisely one edge incident with both vertices then $M(\Omega)$ cannot be ISD. By considering all possible structures with an edge in a parallel class of size one we will show that this implies that the set of circuits and the set of cocircuits of $M(\Omega)$ are not equal and therefore the matroid is not ISD.

Assume that v, w and e exist in Ω where e is the only edge incident with both v and w. First, consider all possible paths from v to w. Each path must have an edge which is incident to v so we let the set of edges which are contained in a path from v to w and are incident with v be denoted W_v. Note that W_v is a cut-set of the biased graph as $\Omega - W_v$ does not contain a path from v to w and so v and w are in different components of $\Omega - W_v$. Furthermore W_v is a minimal cut-set of Ω as any vertex other than v which was on a path from v to w is part of the component containing w in $\Omega - W_v$. Therefore no subset of W_v is a cut-set and in particular, $W_v - e$ is not a cut-set. We also know that $\Omega - (W_v - e)$ is not balanced because there are unbalanced cycles incident with w by Corollary 5.2.3 and this implies that $W_v - e$ does not contain a cocircuit. As $M(\Omega)$ is ISD, $W_v - e$ does not contain a circuit and therefore W_v consists of at most one unbalanced cycle of size two along with single edges.

Next we examine all the possibilities and consider them in three separate cases; W_v contains an unbalanced two element cycle, W_v does not contain any cycles and v is incident with a theta graph, or W_v does not contain a cycle and v is not incident with a theta graph.

For the remainder of the proof, remember that w is incident with an unbalanced cycle by Corollary 5.2.3. We will also return to using E_v to denote all edges incident to v.

Case 1: W_v contains an unbalanced 2 element cycle.

When W_v contains a single cycle, $E_v - W_v$ must also contain a cycle by Lemma 5.2.2. Other than when $M(\Omega) = U_{2,4}$ no parallel classes with size greater than three exist in Ω by Lemma 5.2.4, and therefore the cycle in $E_v - W_v$ must come from one of the structures shown in Figure 5.3. Each of these options will imply the existence of a circuit which is not a cocircuit.

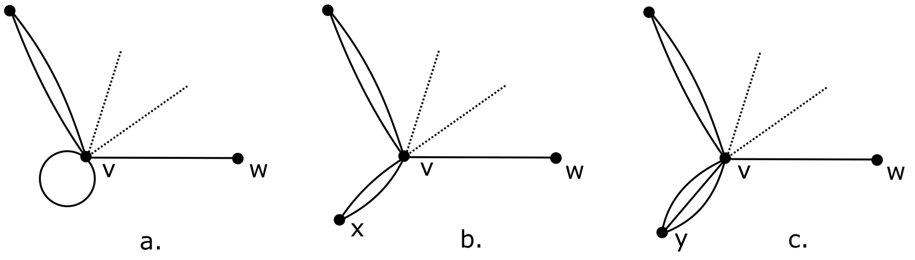

Figure 5.3: Case 1.

a. If v is incident with a loop then this loop along with the parallel pair in W_v form a circuit C. The set of edges in W_v is a bond so no proper subset of the edges is a cut-set and therefore the graph $\Omega - C$ is connected. Since w is incident with an unbalanced cycle, $\Omega - C$ is not balanced. This indicates that the rank of $M(\Omega - C)$ is not lower than the rank of $M(\Omega)$ and therefore C is not a cocircuit.

b. If $E_v - W_v$ has a parallel class of size two incident with v and x, then the handcuffs consisting of this pair of edges and the pair of edges in W_v is a circuit of

$M(\Omega)$. Both x and w must have a circuit incident to them by Corollary 5.2.3 and thus deleting the handcuffs at v does not increase the number of balanced components of the graph and this circuit is not a cocircuit.

c. If $E_v - W_v$ contains a theta subgraph incident to vertices v and y then the handcuffs created by taking two of the edges of the theta graph and the cycle from W_v are a circuit C. These edges are not a cut-set of the graph and, as w is incident to a circuit, $\Omega - C$ is not balanced. Therefore the handcuffs cannot be a cocircuit of $M(\Omega)$.

All of these options have circuits which are not cocircuits and are unsuitable for a graph where $M(\Omega)$ is ISD. Hence W_v cannot contain an unbalanced cycle.

Case 2: W_v does not contain a cycle and v is incident with a theta graph.

Next we consider the options for Ω given in Figure 5.4 where v and x are incident to a theta subgraph θ. In each of these cases θ is a circuit and therefore a cocircuit. In the subgraph $\Omega - \theta$ there are unbalanced cycles incident with w so in order for θ to be a cocircuit it must be x which is part of a balanced component. This balanced component in $\Omega - \theta$ cannot contain any vertices other than x as these vertices must be incident with unbalanced cycles in Ω by Corollary 5.2.3. Loops in Ω are never balanced so x is incident with exactly those three edges of θ.

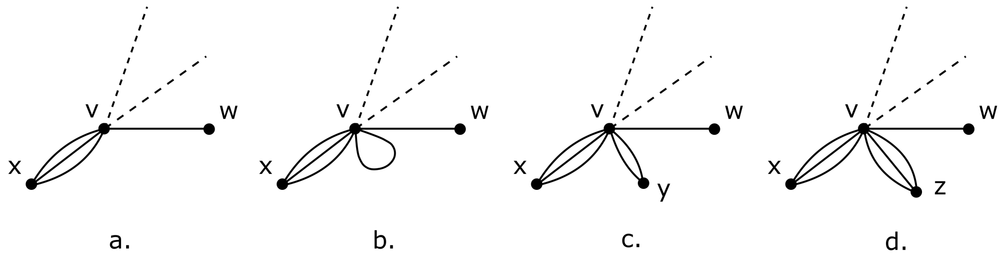

Figure 5.4: Case 2.

a. If v is not incident with any additional cycles then we consider the set of edges consisting of two of the edges incident with x and v as well as all the single edges incident with v. We find that this collection of edges C is a cocircuit. In the graph $\Omega - C$ there is a balanced component consisting of v and x joined by a single edge, but any proper subset of C does not create a balanced component when deleted from Ω as every vertex is incident with an unbalanced cycle.

Clearly, C is not a circuit of Ω because it is not a balanced cycle and it does not contain two cycles.

b. If v is incident with a loop then the loop along with two edges from the theta subgraph form a circuit C. The circuit is not a cocircuit, as there is a single component in $\Omega - C$ and there are unbalanced cycles incident with w so there are no new balanced components.

c. If v is incident with a parallel class of size two which is also incident with the vertex y then the parallel pair and two edges from the theta subgraph form a pair of tight handcuffs. There must be another unbalanced cycle which is incident with y by Lemma 5.2.2 and therefore the handcuffs cannot be a cocircuit because, when they are deleted from the graph, the cycles incident with w and y prevent either component from being balanced.

d. If v is incident to a second theta subgraph of edges also incident on z then the handcuffs formed by taking two edges of each of the theta graphs is a circuit of $M(\Omega)$. As in possibility b., deleting the handcuffs does not increase the number of balanced components in the graph as w is incident with unbalanced cycles. Hence, these handcuffs are a circuit, but not a cocircuit.

Again, in these four scenarios the collections of circuits and cocircuits of $M(\Omega)$ are not equal and if $M(\Omega)$ is ISD this cannot occur.

Case 3: W_v does not contain a cycle and v is not incident with a theta graph.

The final two options are pictured in Figure 5.5. If v is not incident with a theta graph then it must be incident with a pair of tight handcuffs with 3 or 4 elements. It is not possible for v to be incident with two loops because if $M(\Omega)$ contains a circuit with two elements it implies that $M(\Omega) = U_{1,2}$. This means that v must be incident to a pair of edges which are also incident with another vertex x. From Lemma 5.2.2 we see that x must be incident with another unbalanced cycle besides this parallel pair.

a. If E_v contains a loop then together the two cycles incident with v form a pair of tight handcuffs. If the handcuffs are deleted from Ω then no balanced components are formed because w and x are both incident with unbalanced cycles. Therefore the handcuffs are a circuit, but not a cocircuit.

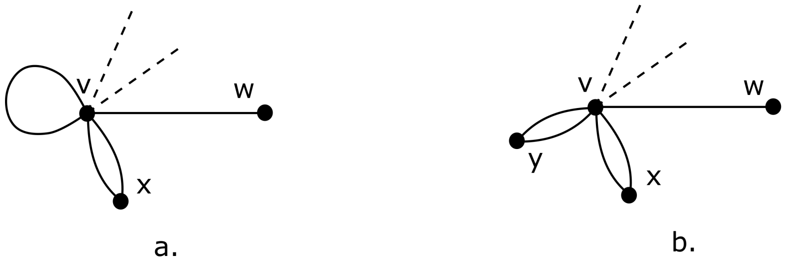

Figure 5.5: Case 3.

b. If E_v contains a second parallel pair which is also incident with y then the pair of parallel pairs form a circuit together. By Lemma 5.2.2, y is incident with another unbalanced cycle. Therefore if the handcuffs are deleted from Ω, every component is unbalanced because of the cycles incident with w, x and y. Hence, the handcuffs are not a cocircuit.

Both of these options in this final case have circuits which are not cocircuits. Thus there are no possibilities which do not result in a contradiction and Ω cannot contain any edges in non-trivial parallel classes. □

At this point it is clear that every edge in Ω must be a loop or in a parallel class of size two or three except for where $M(\Omega)$ is $U_{2,4}$. Next we wish to find a restriction on the number of neighbours each vertex can have.

Proposition 5.2.6. *Let Ω be a biased graph. If $M(\Omega)$ is ISD then no vertex in Ω has more than 2 neighbouring vertices.*

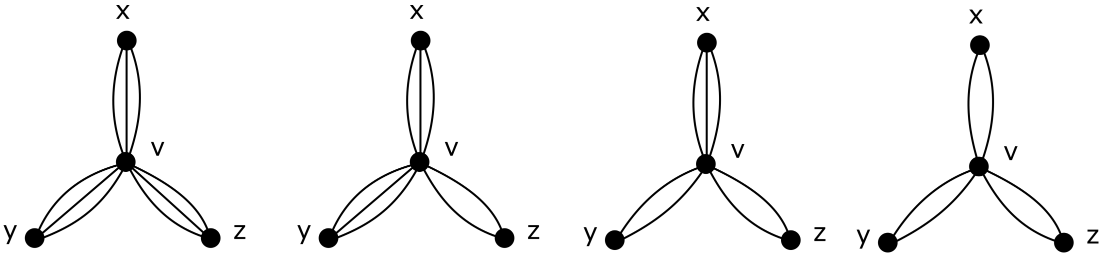

Figure 5.6: Vertex with 3 neighbours

Proof. If Ω contains four edges in parallel then $M(\Omega) = U_{2,4}$ by Lemma 5.2.4 and each vertex has a single neighbouring vertex. If Ω does not have a parallel class of size four then from Proposition 5.2.5 we know that if two vertices are adjacent then there are either two or three edges which are incident on both vertices. Thus if we assume that there is a vertex v in Ω which has at least 3 adjacent vertices we can deduce that there exist vertices x, y and z in one of the forms shown in Figure 5.6. Again we will show that these possibilities imply that the set of circuits and cocircuits of $M(\Omega)$ are not equal and therefore $M(\Omega)$ cannot be ISD.

a. If there are at least two theta subgraphs incident with v then a pair of edges from each of the two theta subgraphs forms a circuit C. The graph $\Omega - C$ contains a single component which is unbalanced by the third parallel class incident with v. Therefore C is a circuit and not a cocircuit.

b. If there are at least two parallel classes of size two incident with v then a pair of these parallel classes form a circuit C. Let v, y and z be the vertices which are incident with C. Then y and z must each be incident with another unbalanced cycle by Lemma 5.2.2. Since all components of $\Omega - C$ are unbalanced, it is not possible for the circuit C to be a cocircuit.

Each of these options implies that $M(\Omega)$ is not ISD so Ω must not contain any vertices which are adjacent to more than two neighbours. □

This is a strong restriction on the structure of Ω since it now must contain no diverging paths. We are almost ready to fully describe the graph G underlying Ω after first considering the biased graphs with 1 or 2 vertices which behave less consistently.

Proposition 5.2.7. *Let Ω be a biased graph where $M(\Omega)$ is the corresponding frame matroid and $M(\Omega)$ is ISD. If Ω is connected and has fewer than 3 vertices then the graph G which underlies Ω has one of the structures shown in Figure 5.7.*

Proof. If Ω has a single vertex then the only edges it can contain are unbalanced loops. If it has no loops then $M(\Omega)$ is the empty matroid. If it contains unbalanced loops then a pair of loops forms a two element circuit and $M(\Omega) = U_{1,2}$. If Ω has 2 vertices v and w, we now consider how many edges are incident with both vertices. It is not possible that there is a single edge between v and w, by Proposition 5.2.5. If Ω contains one balanced parallel pair between v and w then this also means $M(\Omega)$ is $U_{1,2}$ and there cannot be any additional edges on v or w or the balanced

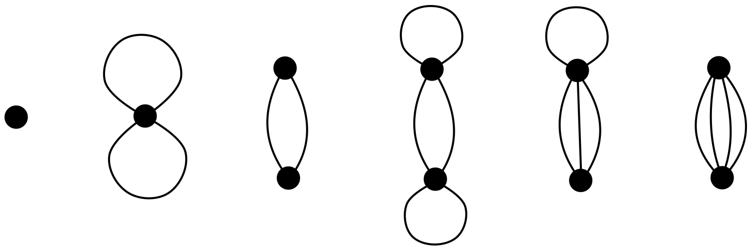

Figure 5.7: Biased graphs with 1 or 2 vertices

cycle would not be a cocircuit of $M(\Omega)$. If there is a parallel pair between v and w which is not balanced, then each of v and w must be incident with an unbalanced loop in order to fulfill Lemma 5.2.2 and $M(\Omega) = U_{2,4}$. If there is theta subgraph θ on the edges v and w containing no balanced cycles then exactly one of v or w should be incident with a loop. This is because $\Omega - \theta$ should contain precisely one more balanced component than Ω and this also has the frame matroid $U_{2,4}$. Finally, if there are 4 edges incident with both v and w then $M(\Omega) = U_{2,4}$ and Ω contains no other edges, by Lemma 5.2.4. □

Finally, we are ready to give the structure for a general biased graph which has an ISD frame matroid. We will first introduce some graph terminology that will be referred to in the proposition. A *doubled cycle* can be obtained by taking a cycle and adding another edge alongside each edge of the cycle so that every edge is in a parallel class of size two. This also called a $2C_k$ where k is the number of vertices in the doubled cycle. A similar concept can be applied to a path to generate a *doubled path* where every edge is in a parallel class of size two, but selecting one representative from each class results in a path.

Proposition 5.2.8. *Let $\Omega = (G,B)$ be a biased graph with more than two vertices such that $M(\Omega)$ is a connected ISD frame matroid. Then G is either a doubled cycle $2C_k$ or a doubled path with an additional edge at each of the two end vertices as shown in Figure 5.8.*

Proof. From Proposition 5.2.6, every vertex in Ω has one or two neighbours. Furthermore, there are no single edges in Ω by proposition 5.2.5. Either every vertex has two neighbours and the vertices form a cycle with parallel classes or there are two vertices with only one neighbour each and Ω has a path structure.

Considering the first of these options we will let Ω be a cycle where every edge

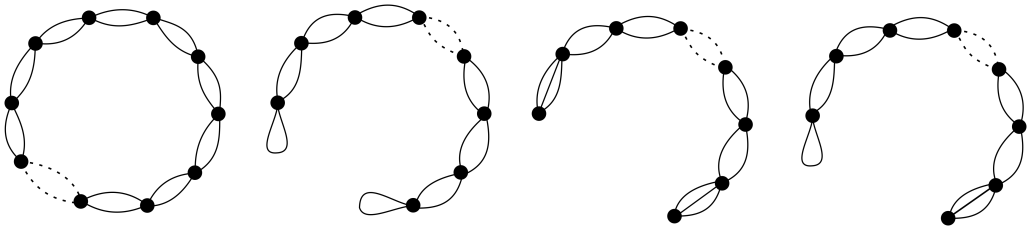

Figure 5.8: Biased Graphs of ISD Frame Matroids

is in a non-trivial parallel class. Suppose there is a parallel class with three edges between two vertices v and w of Ω so these edges produce a theta subgraph θ. In the graph $\Omega-\theta$ there is a single component because there is a path between v and w from the other part of the cycle. This path has parallel classes so $\Omega-\theta$ is not balanced and therefore θ is a circuit, but not a cocircuit. This is a contradiction if $M(\Omega)$ is ISD so every parallel class must have two edges. It remains to show that no vertex of Ω is incident with a loop. If it were, then the loop and a neighbouring parallel pair form a pair of tight handcuffs C. Again, because Ω is a cycle, $\Omega-C$ contains a single unbalanced component so C is a circuit which is not a cocircuit. Therefore there are no loops and Ω is a $2C_k$.

In the case where Ω contains vertices which do not have two neighbours then there must be two end vertices of the path which each have only one neighbour. These vertices must be incident with a circuit, by Lemma 5.2.2, so they are incident with at least three edges. If they are incident with four or more edges then they are incident with at least two loops or with a loop and a theta graph. Both of these scenarios are contradictory because if C is a pair of handcuffs consisting of two loops or of a loop and two edges of a theta graph then $\Omega-C$ does not contain a balanced component and C is not a cocircuit. Therefore the end vertices are incident to exactly three edges - either a loop and a parallel pair or a theta subgraph. Next we can assert that there are no loops incident with the vertices which have two neighbours. If there were, then the tight handcuffs C consisting of the loop with a pair of parallel edges are not a cocircuit, because $\Omega-C$ contains no balanced components.

Finally, there are no parallel classes of size at least three except the classes of size exactly three which may be incident with an end vertex. Assume there is a parallel class of size three or more which is not incident with an end vertex and let the circuit C be a pair of tight handcuffs containing two edges of this class and two edges of a neighbouring parallel class. There are at most two components in $\Omega - C$ and none of them are balanced because the end vertices are incident with unbalanced cycles. Hence C is not a circuit and there are no parallel classes of size three or greater which are not incident with the vertices with only one neighbour. Therefore the only possible structures for Ω are a doubled cycle or a doubled path where the end vertices are incident to three edges as pictured in Figure 5.8. □

The proof of Theorem 5.1.3 directly follows from this proposition.

Proof of 5.1.3. Let M be an ISD, 3-connected frame matroid. By Proposition 5.2.8, if $M = M(\Omega)$ then Ω is one of the biased graphs shown in Figure 5.8. Of these, the only structure which gives a 3-connected frame matroid is the doubled cycle. Therefore Ω must be a doubled cycle $2C_k$ and we can deduce from the set of non-spanning circuits of the frame matroid that $M(\Omega)$ is a swirl. □

5.3 Special Cases

Having found the possible structures for Ω where $M(\Omega)$ is an ISD frame matroid we next consider the more restricted classes of graphic matroids, signed graphic matroids and bicircular matroids. Graphic matroids are a subset of regular matroids so the first result is already given in Theorem 4.2.1 due to Lindström.

Proposition 5.3.1. *If G is a graph and the graphic matroid $M(G)$ is ISD and connected then $M(G)$ is $U_{1,2}$.*

Proof. Graphic matroids are equivalent to the matroids associated with a biased graph where every cycle is balanced. This means every cycle is a circuit and cocircuit of $M(G)$ and G cannot contain any loops. Proposition 5.2.5 means there are no single edges in G and if any edge is in a parallel pair then in addition this is a series pair. The only connected matroid with a parallel pair which is a series pair is $U_{1,2}$. □

Next we characterise the structure of signed graphs which have ISD signed graphic matroids. A signed graph is a graph where every edge is given a sign of $+$ or $-$ and the cycles of the graph with an even number of negative edges are balanced.

Proposition 5.3.2. *If Ω is a signed graph with more than two vertices and the signed graphic matroid $M(\Omega)$ is ISD and connected then Ω is a doubled cycle of even length $2C_{2k}$ or a doubled path with loops at the extremal vertices. In either structure the parallel pairs consist of one positive edge and one negative edge and the loops are negative.*

Proof. Let Ω be a signed graph such that the signed graphic matroid $M(\Omega)$ is ISD. We know that Ω has one of the structures from Figure 5.8 so assume that Ω is a doubled cycle. Every parallel pair of edges in Ω must be unbalanced and therefore must consist of one edge of each sign. Therefore it is possible to pick one edge from each pair in such a way that there is a large cycle C which has an even number of negative edges and is balanced. The complementary edges which remain in $\Omega - C$ should also be balanced so that C is a cocircuit. The complement of a balanced cycle in Ω is another balanced cycle so Ω has an even number of vertices and Ω is a $2C_{2k}$.

If instead Ω has two vertices each with only one neighbour then it must be a doubled path with two loops. By Proposition 5.2.8, Ω must have three edges incident with each terminal vertex. However, in a signed graph if there are three edges in parallel then there must be a pair of edges which form a balanced cycle. This cannot happen because except for when $M(\Omega) = U_{1,2}$ no connected ISD matroid contains a parallel pair. Therefore Ω contains no theta graphs and must be a doubled path with two loops.

In either case there can be no balanced cycles and therefore every cycle must contain an odd number of negative edges. This forces loops to be negative edges and parallel pairs to contain one positive and one negative edge. □

Bicircular graphs are simply frame matroids which have no balanced cycles so all the circuits of a bicircular matroid correspond to bicycles in the graph (Figure 5.1). In accordance, we also define a *free-swirl* which is a swirl without any of the non-spanning circuits which intersect one element of each of the pairs of elements in the ground set. This last proposition directly follows from Theorem 5.1.3 and the definition of bicircular matroids and free-swirls.

Proposition 5.3.3. *If M is an ISD, 3-connected, bicircular matroid then it is a free-swirl.*

Chapter 6

Axiomatisability

In [15], Mayhew, Newman and Whittle introduce a form of monadic second-order logic (MS_0) which can be used to characterise certain classes of matroids. In this chapter we define a sentence ψ in MS_0 such that a matroid M satisfies ψ if and only if M is ISD. We will also use methods from their paper to show that the class of self-dual matroids is not able to be characterised by a sentence in MS_0.

6.1 ISD matroids

Here we give a description of MS_0 and use it to find a sentence which is only satisfied by ISD matroids. In a sentence of MS_0 variables are interpreted as subsets of the ground set of a matroid. We use three predicates: $X_1 \subseteq X_2$ is true whenever X_1 is a subset of X_2; Ind(X_1) is true when X_1 is independent; and Sing(X_1) is true when $|X_1| = 1$. We also have access to the connectives $\{\neg, \wedge\}$ and since this set is functionally complete we will use $\vee, \rightarrow$ and $\leftrightarrow$ which can be expressed with $\neg$ and $\wedge$. Finally, the last item in the MS_0 toolkit is the existential quantifier $\exists$ and by pairing this with $\neg$ we can also use $\forall$.

We now put these together to find a sentence which describes ISD matroids. Such a sentence should assert that the complement of every basis is also a basis of the matroid so first we write predicates which describe bases and complements in MS_0.

A basis is a maximal independent set which we can establish in MS_0 as

$$\text{Basis}(X) = \text{Ind}(X) \wedge \forall X_1 (X \subseteq X_1 \rightarrow X_1 \subseteq X \vee \neg \text{Ind}(X_1)).$$

If two sets are complementary then every element is part of exactly one of them.

$$\text{Comp}(X,Y) = \forall X_1 (\text{Sing}(X_1) \rightarrow (X_1 \subseteq X \leftrightarrow \neg(X_1 \subseteq Y)))$$

We use these in the following sentence ψ. A matroid M satisfies ψ if and only if M is ISD.

$$\psi : \forall X (\text{Basis}(X) \leftrightarrow \forall Y (\text{Comp}(X,Y) \rightarrow \text{Basis}(Y)))$$

6.2 Self-dual Matroids

Unlike ISD matroids, the properties of self-dual matroids are not able to be captured by a sentence in MS_0. In order to prove this we will first define a notion of equivalence for matroids.

Definition 6.2.1. *Let M_1 and M_2 be matroids. Let $\mathscr{M}$ be the set of all matroids M' such that $E(M') \cap (E(M_1) \cup E(M_2)) = \emptyset$ and let $\mathscr{K}$ be the set of all k-variable sentences in MS_0. Then M_1 and M_2 are k-equivalent if, for all M' in $\mathscr{M}$ and for all ψ in $\mathscr{K}$, both, or neither, $M_1 \oplus M'$ and $M_2 \oplus M'$ satisfy ψ.*

It is not hard to show that this is an equivalence relation. The fact that k-equivalence is reflexive and symmetric follows directly from the definition. Next, suppose that M_1 and M_2 are k-equivalent and M_2 and M_3 are k-equivalent, but that M_1 and M_3 are not. Then there exists a k-variable sentence ψ and a matroid M' such that exactly one of $M_1 \oplus M'$ or $M_3 \oplus M'$ satisfies ψ. Relabeling does not affect whether a matroid satisfies a sentence in MS_0 so we relabel M_2, if necessary, to ensure that $|M_2 \cap M'| = \emptyset$. Now it implies that one of the pairs, M_1 and M_2, or M_2 and M_3, is not k-equivalent depending on whether or not $M_2 \oplus_2 M'$ satisfies ψ. This is a contradiction and therefore k-equivalence is an equivalence relation. Furthermore, there are a finite number of equivalence classes which is proved in [15].

Lemma 6.2.2. *Let k be a positive integer. There are a finite number of equivalence classes of matroids under the relation of k-equivalence.*

Next we use this result to prove that self-dual matroids are not axiomatisable in MS_0.

Theorem 6.2.3. *There is no sentence ψ in MS_0 such that a matroid is self-dual if and only if it satisfies ψ.*

Proof. Suppose instead that ψ is a sentence which describes self-dual matroids and that ψ has k variables. By Lemma 6.2.2, there are a finite number of equivalence classes for k-equivalence. Therefore if we consider the infinite family of matroids, $M(K_n)$ for $n \geq 5$, there must be two distinct matroids of this type which are k-equivalent. Thus, let M_1 and M_2 be k-equivalent where $M_1 = M(K_n)$, $M_2 = M(K_m)$ and $n < m$. Now we choose $M' \cong M_1^*$ such that $E(M') \cap (E(M_1) \cup E(M_2))$. Because M_1 and M_2 are k-equivalent, $M_1 \oplus M'$ is indistinguishable from $M_2 \oplus M'$ with respect to ψ. Note, however, that whereas $M_1 \oplus M' \cong M_1 \oplus M_1^*$ is self-dual, $M_2 \oplus M' \cong M_2 \oplus M_1^*$ is not self-dual because the largest connected minor of $M_2 \oplus M_1^*$ is isomorphic to M_2 and the largest connected minor of $(M_2 \oplus M_1^*)^*$ is isomorphic to M_2^*. Therefore ψ cannot accurately determine the class of self-dual matroids when it is satisfied by both, or neither of $M_1 \oplus M'$ and $M_2 \oplus M'$. Hence there is no sentence which characterises self-dual matroids. □

Chapter 7

Conjectures

We conclude this thesis by discussing a number of conjectures which have arisen.

Conjecture 7.1.1. *Every matroid is a minor of an ISD matroid.*

It makes sense to begin with the conjecture which was the first to be conceptualised. This conjecture motivated several chapters of the thesis which lead to a proof for two classes of matroids. Theorem 2.1.2 proves that all sparse paving matroids are minors of ISD sparse paving matroids and Theorem 3.4.3 shows that the conjecture holds for representable matroids.

The methods used for each of these classes do not seem to be able to be generalised to all matroids. It is also difficult to see how a counterexample could be constructed as it requires showing that the matroid is not a minor of any ISD matroid.

A related conjecture comes from taking this idea and putting a restriction on the type of ISD matroids we are interested in.

Conjecture 7.1.2. *Every $\mathbb{F}$-representable matroid is a minor of an ISD $\mathbb{F}$-representable matroid, for all fields $\mathbb{F}$.*

Chapter 3 addresses this question and proves, by means of Theorems 3.3.4, 3.4.2 and 3.5.3, that it is true when $\mathbb{F}$ is a field of characteristic 2, an algebraically closed field, or $GF(p)$ for a prime $p = 3$ (mod 4). These proofs all centre around chain-groups and the orthogonal vector space defined using the dot product as a bilinear form. It relies on finding vectors which are orthogonal and, in particular, vectors which are orthogonal to themselves. This does not occur in some fields such as

$\mathbb{R}$ which makes it unclear how one might going about proving this result for all fields.

In the cases when the previous conjectures are true it is possible to put an upper bound on how large the ISD matroid which contains any given matroid as a minor must be. This suggests the following conjecture.

Conjecture 7.1.3. *There exists c in $\mathbb{Z}$ such that for any matroid M there exists an ISD matroid N such that M is a minor of N and $|E(N)| \leq c|E(M)|$.*

Of course this can only be true if Conjecture 7.1.1 is also true.

Conjecture 7.1.4. *If M is a matroid and every cocircuit of M is a union of circuits there exists an ISD matroid N with $X \subseteq E(N)$ such that $M = N/X$.*

Another way of phrasing this is to say that we conjecture that the class of cyclic-cocircuit matroids is the same as the class of contraction minors of ISD matroids. We know that every contraction minor of an ISD matroid is a cyclic-cocircuit matroid, but it is not yet known whether the converse is true.

Lastly, we conjecture that there are far fewer ISD matroids than self-dual matroids for matroids with a large number of elements.

Conjecture 7.1.5. *Let S_n be the number of self-dual matroids on n-elements up to isomorphism. Let i_n be the number of ISD matroids on n-elements.*

$$\lim_{n\to\infty} \frac{i_n}{S_n} = 0$$

Bibliography

[1] ASSMUS, E. F., AND KEY, J. D. *Designs and Their Codes*. Cambridge University Press, Cambridge; New York, NY, USA, 1993.

[2] BOSE, R. C. On the application of the properties of galois fields to the problem of construction of hyper-graeco-latin squares. *Sankhyā: The Indian Journal of Statistics* (1938), 323–338.

[3] BRUCK, R. H., AND RYSER, H. J. The nonexistence of certain finite projective planes. *Canad. J. Math 1*, 191 (1949), 9.

[4] CARTER, J. L. *On the existence of a projective plane of order ten*. University of California, Berkeley, 1974.

[5] EULER, L. *Recherches sur une nouvelle espece de quarres magiques*. Zeeuwsch Genootschao, 1782.

[6] GLYNN, D. G. The construction of self-dual binary codes from projective of odd order. *Australasian Journal of Combinatorics 4* (1991), 277–284.

[7] LAM, C. W., KOLESOVA, G., AND THIEL, L. A computer search for finite projective planes of order 9. *Discrete Mathematics 92*, 1-3 (1991), 187–195.

[8] LAM, C. W., THIEL, L., AND SWIERCZ, S. The nonexistence of code words of weight 16 in a projective plane of order 10. *Journal of Combinatorial Theory, Series A 42*, 2 (1986), 207–214.

[9] LAM, C. W., THIEL, L., SWIERCZ, S., AND MCKAY, J. The nonexistence of ovals in a projective plane of order 10. *Discrete Mathematics 45*, 2-3 (1983), 319–321.

[10] LAM, C. W., THIEL, T., AND SWIERCZ, S. The non-existence of finite projective planes of order 10. *Canad. J. Math 41*, 6 (1989), 1117–1123.

[11] LINDSTRÖM, B. On Binary Identically Self-dual Matroids. *Eur. J. Comb. 5*, 1 (1984), 55–58.

[12] MACWILLIAMS, F., SLOANE, N., AND THOMPSON, J. G. On the existence of a projective plane of order 10. *Journal of Combinatorial Theory, Series A 14*, 1 (1973), 66–78.

[13] MACWILLIAMS, F. J., SLOANE, N. J., AND THOMPSON, J. G. Good self dual codes exist. *Discrete Mathematics 3*, 1-3 (1972), 153–162.

[14] MAYHEW, D., NEWMAN, M., WELSH, D., AND WHITTLE, G. On the asymptotic proportion of connected matroids. *European Journal of Combinatorics 32*, 6 (2011), 882–890.

[15] MAYHEW, D., NEWMAN, M., AND WHITTLE, G. Yes, the missing axiom of matroid theory is lost forever. *arXiv preprint arXiv:1412.8399* (2014).

[16] OXLEY, J. *Matroid theory, volume 21 of Oxford Graduate Texts in Mathematics*. Oxford University Press, Oxford, 2011.

[17] RAINS, E. M., AND SLOANE, N. J. A. Self-dual codes. *arXiv preprint math/0208001* (2002).

[18] SEYMOUR, P. D. Decomposition of regular matroids. *J. Comb. Theory, Ser. B 28*, 3 (1980), 305–359.

[19] TARRY, M. *Le Problème des 36 officiers...: Congrès de Paris 1900.* Secrétariat de l'Association française pour l'avancement des sciences, 1900.

[20] TUTTE, W. T. Lectures on matroids. *J. Res. Nat. Bur. Standards Sect. B 69*, 1-47 (1965), 468.

[21] VEBLEN, O. A system of axioms for geometry. *Transactions of the American Mathematical Society 5*, 3 (1904), 343–384.

[22] WELSH, D. J. Euler and bipartite matroids. *Journal of Combinatorial Theory 6*, 4 (1969), 375–377.

[23] WELSH, D. J. *Matroid theory.* Courier Corporation, 2010.

[24] ZASLAVSKY, T. Frame matroids and biased graphs. *European Journal of Combinatorics 15*, 3 (1994), 303–307.