UiT The Arctic University of Norway

Department of Mathematics and Statistics

Codes, matroids and derived matroids

Teodor Dahl Knutsen

Master's thesis in Mathematics MAT-3900, May 2023

Contents

1 Introduction **1**

2 Codes **4**
2.1 Generator matrices and parity-check matrices 5
2.2 Hamming codes 5
2.3 Distances and weights 5
2.4 Dual codes 10
2.5 Shortening and puncturing 11

3 Matroids **13**
3.1 Axioms of matroids 13
3.2 Vector matroids 15
3.3 Graphical matroids 16
3.4 Uniform matroids 17
3.5 Dual matroids 17
3.6 Connectedness and sums of matroids 18
3.7 Minors 19
3.8 Connection to codes 20
3.9 Hamming distance for matroids 21

4 Derived matroids **24**
4.1 Binary matroids 24
4.2 Representable matroids 25
4.3 Combinatorial derived matroids 27
4.4 Redundancy 33
4.5 Fast matroids 36
4.6 Combinatorial derived matroids of fast matroids 39
4.7 Extending the definition to a finite graded lattice 46
4.8 Derived matroid of q-matroids 49
4.9 Extended Longyear derived matroid 51

5 Implemented software **54**
5.1 Calculation of Betti-numbers for matroids 56

6 Final overview **60**

Bibliography **I**

A Alternative proof of Proposition 4.44 for uniform matroids **IV**

B The resolutions of elongations of combinatorial derived matroids of several uniform matroids **V**

C Circuits of a derived non-fast matroid **X**

List of Figures, Tables and Algorithms

Fig. 1 Incidence matrices of graphs 16
Fig. 2 Illustration of uniform matroids 17
Fig. 3 Connected graphs where the associated matroid is not connected 19
Fig. 4 Vámos matroid 21
Tab. 1 Number of circuits of a given size in $\delta_{FJK}M$ for the given matroid 28
Fig. 5 Sh(4) and a graph that contracts to Sh(4) 31
Alg. 1 Computation of bases of combinatorial derived matroid 55

1 Introduction

The theory of error-correcting codes over finite fields $\mathbb{F}_q$ has been developed gradually over the last 7-8 decades. The idea is to represent information in such a way that if it is sent over a noisy channel and only slightly corrupted, it shall nevertheless be possible to retrieve the correct information (with high probability). An important subclass of codes is linear codes; concretely one represents the information in question as a $\mathbb{F}_q$-linear subspace C of a large ambient space $\mathbb{F}_q^n$. It turns out that many of the most important properties of linear codes, like their tolerance for errors under transmission, are only dependent on a certain underlying combinatorial structure. This structure is the matroid, M_C.

The theory of matroids has been developed in parallel, introduced in the 1930's by H. Whitney, and has been applied in many areas outside coding theory, including topics as different as greedy algorithms and tropical geometry. There are also many matroids which do not come from codes. The connection between linear codes and matroids has been investigated more recently, and in particular during the two most recent decades. The dominant part of this activity has been to use matroid invariants to describe and analyze error-correcting codes, but to some extent one has also used concepts from coding (and graph) theory to describe properties of matroids.

In Sections 2 and 3 of this thesis we describe basic theory and important properties of error-correcting codes and matroids, and the most important elements in the connection between them. Some of the definitions are included because of their usefulness in later sections. A partial goal is to demonstrate how some invariants originally defined for linear codes, can also be defined for matroids associated to these codes, and in addition to matroids in general (including those which are represented by no linear codes at all). This sets the stage for the remaining part of the thesis, where a main point is to define derived matroids of given matroids, regardless of which codes they represent, or if they represent any code at all.

Section 4 is the heart of this thesis. There we treat the issue of derived matroids. In a (usual) matroid the study of dependent sets, or dependencies, is a central question. With derived matroids one studies "dependencies of dependencies." Derived matroids have quite recently turned out to be a useful tool within

computer science, in particular within private information retrieval [FK21]. We have therefore chosen to study this topic more closely.

Derived matroids were first defined by Longyear [Lon80] in 1979, but only for binary matroids M, that is matroids associated to binary codes/matrices. The definition of the matroid derived from M was such that the derived matroid δM was independent of the associated codes in case there were many such codes associated to M.

In 2019 Oxley and Wang [OW19] defined derived matroids $\delta M[A]$ derived from the pair (M, A), where M is a matroid associated to a matrix A, that defines a linear code C_A over any given finite field $\mathbb{F}_q$. The difference from Longyear is that the matroid M does not have to be binary, and that the result depends not only on the matroid, but also on the representation. Independently of this work, Jurrius and Pellikaan [JP15] defined a derived code, which is dual to the construction by Oxley and Wang.

In 2022, however, Freij-Hollanti, Jurrius, and Kuznetsova [FJK23] were able to define a derived matroid δM for any matroid, regardless of whether it comes from a code/matrix or not, and independent of what code it may come from if it comes from several ones. Their definition, although quite different from Oxley and Wang's definition, quite often, but far from always, gives the same result δM. One of the current issues of derived matroids ala FJK has been to determine the ranks of the derived matroid. In Subsections 4.3-4.6 we first present the construction and results by FJK, and then, as a piece of independent research, we prove general properties of δM, and in addition we define a large class of matroids M, which we denote by fast matroids. For these fast matroids we find that the rank of δM is the corank of M. In Example 4.11 we give an example of a non-fast matroid, where $r(\delta M)$ is different from the corank of M. This settles a difficult problem of whether the rank of δM always is equal to the corank of M. Also the rest of the thesis (Sections 4.7-5) is new and original research.

In Section 4, we also define derived matroids of finite graded lattices and of q-matroids. In addition we extend Longyear's definition of derived matroids of binary matroids, to a definition valid for all matroids. We show that the outcome of this is not always equal to the δM obtained from FJK.

In Appendix B we list free resolutions of Stanley-Reisner rings of derived ma-

troids δM for M various uniform matroids. These resolutions determine properties of these derived matroids, inspired by properties of linear codes, that is: their generalized weights.

In Section 5 we explain how we were able to perform these and other calculations for determining (properties of) derived matroids. This was done using a software library that was developed alongside this thesis, and is available at `https://github.com/teo8192/matroid-rs`. The fast matroids defined in Section 4 have been given their name because there are particularly fast algorithms to determine their properties. The main result that illustrates this, is Theorem 4.47, which shows that dependent sets for a derived matroid of a fast matroid, has a particularly simple form.

The initial interest for the main contributions of this thesis was sparked by the question of whether it was possible to simplify the construction of the combinatorial derived matroid, and the computation of them.

2 Codes

Information needs to be transmitted through both space and time; both noisy mediums. Deep space transmissions may be corrupted by radiation, electric signals may be disturbed by noise and a movie on a disc may suffer scratches. We still want to be able to get the information that is transmitted, even if it is corrupted. The goal of coding theory is precisely this. Information is encoded in such a way that even if parts of the encoded message are corrupted, it is still possible with a high probability to decode it back to the original information. But what is information?

We then need to start with the small building blocks of information, the symbols it consists of.

Definition 2.1. *An alphabet A of cardinality q is a finite set of symbols.*

Every message in our code will be sequences of symbols from the alphabet A, and the code is called a q-ary code. One type of codes are block codes, where all sequences of symbols in the code have the same length n. More formally, a block code C is a subset of A^n. For notation, for a sequence of symbols $\mathbf{x} \in A^n$, let x_i denote the i-th symbol in the sequence.

Some specific alphabets are more interesting than others, and we will focus on codes that use a finite field $\mathbb{F}_q$ as the alphabet. In this case $\mathbb{F}_q^n$ is a vector space, and we may have the code as a subspace of $\mathbb{F}_q^n$. Such codes are called linear codes.

Definition 2.2. *Let $C \leq \mathbb{F}_q^n$ be a linear code.*

- *The* word-length *n of the code is the dimension of the space that the code is embedded in.*
- *The dimension k of the code is $k = \dim_{\mathbb{F}_q}(C)$.*
- *The cardinality m of the code is $m = q^k$.*

Example 2.3. *Consider the subspace $C = \langle 1110000, 0011001, 10000011, 0100101 \rangle \subseteq \mathbb{F}_2^7$ (let the bitstrings be vectors in $\mathbb{F}_2^7$, and not two-bit numbers). These four vectors are linearly independent, and we get that the dimension of C is $k = 4$. From this, we can calculate that the cardinality of C is $m = 2^4 = 16$.*

2.1 Generator matrices and parity-check matrices

For any vector space, there is a basis for this vector space. If we let this basis be the rows of a matrix G, then the row-space of this matrix is the vector space itself. A matrix G such that its row-space is a linear code C is called a generator matrix of C. This generator matrix is not unique, since we may choose any matrix such that its row-space is C.

Associated to every linear code there is also a parity check matrix H. The row-space of the parity check matrix is the orthogonal space of the code, so in the same way that the generator matrix is not unique, the parity check matrix is not unique. We can use this parity check matrix to define the code,

$$C = \{\mathbf{x} | \mathbf{x} \in \mathbb{F}_q^n, H\mathbf{x} = \mathbf{0}\}.$$

If the generator matrix is of the form $G = [I|A]$, then a parity check matrix can be found as $H = [-A^\top|I]$, see [Hil86, Theorem 7.6].

2.2 Hamming codes

Hamming codes are a family of linear codes, originally invented to correct errors caused by punch card readers. One example where a hamming code is traditionally used today is in ECC memory, where a binary $\mathrm{Ham}(7, 4)$ is commonly used. There are q-ary hamming codes, but throughout this thesis binary Hamming codes will be used in examples, so these are the ones that will be defined.

To construct a binary Hamming code, choose a positive integer $r \geq 2$. Now construct a parity-check matrix by letting the columns be all non-zero elements of $\mathbb{F}_2^r$. This is the parity check matrix for a code with $n = 2^r - 1$ and $k = 2^r - r - 1$, and denote this code as $\mathrm{Ham}(n, k)$.

2.3 Distances and weights

When a code-word is corrupted, some symbols are changed. We then want a way to measure how different two sequences of symbols are. For this we may use the Hamming distance.

Definition 2.4. *The* Hamming distance *between two sequences of symbols* $\mathbf{x}$ *and* $\mathbf{y}$ *is*

$$d_H(\mathbf{x}, \mathbf{y}) = |\{i | x_i \neq y_i\}|.$$

This distance has some immediate properties:

$$\begin{aligned} d(\mathbf{x}, \mathbf{y}) &= 0 \Leftrightarrow \mathbf{x} = \mathbf{y} \\ d(\mathbf{x}, \mathbf{y}) &= d(\mathbf{y}, \mathbf{x}) \\ d(\mathbf{x}, \mathbf{z}) &\leq d(\mathbf{x}, \mathbf{y}) + d(\mathbf{y}, \mathbf{z}) \end{aligned}$$

This makes this a metric, and with this we have a metric space.

Example 2.5. *Let* $\mathbf{x} =$ `e2czRzQzZw` *and* $\mathbf{y} =$ `F2cZRqQOZw`*. Their Hamming distance is* $d_H(\mathbf{x}, \mathbf{y}) = |\{1, 4, 6, 8\}| = 4$.

Now consider the code C *from Example 2.3. Let* $\mathbf{a} = 1101001$, $\mathbf{b} = 0110011$ *and* $\mathbf{c} = 0010110$*. Observe that* $\mathbf{a}, \mathbf{b}, \mathbf{c} \in C$*. The distances between these vectors are:* $d(\mathbf{a}, \mathbf{b}) = 4, d(\mathbf{a}, \mathbf{c}) = 7, d(\mathbf{b}, \mathbf{c}) = 4$*. This also illustrates the triangle inequality, since* $d(\mathbf{a}, \mathbf{c}) = 7 \leq d(\mathbf{a}, \mathbf{b}) + d(\mathbf{b}, \mathbf{c}) = 8$.

Equipped with the Hamming distance, we may define the minimum distance of a code. The minimum distance of a code is the smallest number of symbols that can be changed in some code-word to get another code-word.

Definition 2.6. *The* minimum distance *of a code* C *is*

$$d(C) = \min_{\mathbf{x}, \mathbf{y} \in C} d_H(\mathbf{x}, \mathbf{y}).$$

For any element in $\mathbb{F}_q^n$, it is interesting to look at the symbols that are non-zero. This is called the support of the element.

Definition 2.7. *The* support *of an element* $\mathbf{w} \in \mathbb{F}_q^n$ *is*

$$\text{supp}(\mathbf{w}) = \{i | w_i \neq 0\}.$$

Example 2.8. *Let* $\mathbf{a}, \mathbf{b}, \mathbf{c}$ *be as in example Example 2.5. The supports for these are:*

$$\begin{aligned}\text{supp}(\mathbf{a}) &= \{1, 2, 4, 7\} \\ \text{supp}(\mathbf{b}) &= \{2, 3, 6, 7\} \\ \text{supp}(\mathbf{c}) &= \{3, 5, 6\}\end{aligned}$$

Using the support of an element, we may then define the weight of an element, which is the number of non-zero symbols in the element.

Definition 2.9. *The* weight *of an element* $\mathbf{w} \in \mathbb{F}_q^n$ *is*

$$w(\mathbf{w}) = |\text{supp}(\mathbf{w})|.$$

Example 2.10 (Continuation of Example 2.8)**.** *To illustrate this, consider the vectors* $\mathbf{a}, \mathbf{b}, \mathbf{c}$*. We get that* $w(\mathbf{a}) = 4$*,* $w(\mathbf{b}) = 4$ *and* $w(\mathbf{c}) = 3$*.*

The support function can be extended to be a function on subsets of $\mathbb{F}_q^n$.

Definition 2.11. *Let* $L \subseteq \mathbb{F}_q^n$ *be a subset. Then the* support *of* L *is*

$$\text{supp}(L) = \bigcup_{\mathbf{w} \in L} \text{supp}(\mathbf{w}),$$

and the weight *of* L *is*

$$w(L) = |\text{supp}(L)|.$$

The weight function and the minimum distance of a code are closely related. In fact, the former may be used to calculate the latter.

Proposition 2.12. *Let* $C \leq \mathbb{F}_q^n$ *be a linear code. Then*

$$d(C) = \min_{\mathbf{w} \in C, \mathbf{w} \neq \mathbf{0}} w(\mathbf{w}).$$

Proof. We have that

$$d(C) = \min_{\mathbf{x}, \mathbf{y} \in C, \mathbf{x} \neq \mathbf{y}} d(\mathbf{x}, \mathbf{y}).$$

By the properties of the distance metric, we have that $d(\mathbf{x}, \mathbf{y}) = d(\mathbf{0}, \mathbf{x} - \mathbf{y})$. But the distance of a code-word to zero is the number of symbols in the code-word that is different from zero, which is the weight of the code-word. Since any code-word may be written as the difference of two code-words, and that the difference of two unique code-words are always a non-zero code-word, we have that the sets $\{\mathbf{x} - \mathbf{y} | \mathbf{x}, \mathbf{y} \in C, \mathbf{x} \neq \mathbf{y}\}$ and $\{\mathbf{w} | \mathbf{w} \in C, \mathbf{w} \neq \mathbf{0}\}$ are equal. We thus get that

$$d(C) = \min_{\mathbf{w} \in C, \mathbf{w} \neq \mathbf{0}} w(\mathbf{w}).$$

□

Example 2.13. *Let us calculate the minimum distance of the Hamming code* $C = \mathrm{Ham}(7, 4)$ *over* $\mathbb{F}_2$ *with the generator matrix*

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

The elements of this code are all linear combinations of the rows, and the code-words and their weights are:

$\mathbf{w}$	$w(\mathbf{w})$
$(0,0,0,0,0,0,0)$	0
$(1,0,0,0,0,1,1)$	3
$(0,1,0,0,1,0,1)$	3
$(1,1,0,0,1,1,0)$	4
$(0,0,1,0,1,1,0)$	3
$(1,0,1,0,1,0,1)$	4
$(0,1,1,0,0,1,1)$	4
$(1,1,1,0,0,0,0)$	3
$(0,0,0,1,1,1,1)$	4
$(1,0,0,1,1,0,0)$	3
$(0,1,0,1,0,1,0)$	3

$$\begin{array}{ll} (1,1,0,1,0,0,1) & 4 \\ (0,0,1,1,0,0,1) & 3 \\ (1,0,1,1,0,1,0) & 4 \\ (0,1,1,1,1,0,0) & 4 \\ (1,1,1,1,1,1,1) & 7 \end{array}$$

We can see that the smallest weight a non-zero codeword can have is 3*, and thus we have the minimum distance* $d(C) = 3$*. In fact, the minimum distance for all Hamming codes are* 3*.*

Observe that for any $\mathbf{x} \in C$, we have that $\text{supp}(\mathbf{x}) = \text{supp}(\langle \mathbf{x} \rangle)$. This means that the weight of any code-word is the same as the weight of the span of this code-word. We can also, for any one-dimensional subspace of C, find a codeword such that its span is this subspace. From this we may generalize the minimum distance of a code, by saying that it is the minimum weight of any one-dimensional subspace of the code. But then we can generalize this even further.

Definition 2.14. *Let* C *be a* k*-dimensional linear code. Then the* i*-th generalized hamming weight* d_i *is*

$$d_i = \min_{L \subseteq C, \dim L = i} w(L).$$

As we see, d_1 is the minimum weight of a one-dimensional subspace of the code, so this is the same as the minimum distance of the code.

Example 2.15 (Continuation of Example 2.13)**.** *As mentioned,* $d(C) = d_1$ *is the minimum distance of the code, and this is* 3*. Of the* 35 *two-dimensional subspaces of the code, the smallest weight of any of them is* 5*, so* $d_2 = 5$*. To find* d_3*, we need to look at the* 15 *subspaces of dimension* 3*, and there the smallest weight is* 6*. Finally, the entire code is a subspace of dimension* 4*, and its weight is* 7*, and we get that* $d_4 = 7$*.*

If we look at this example, we can see that these generalized hamming distances are strictly increasing;

$$1 \leq 3 < 5 < 6 < 7 \leq 7.$$

It turns out that this is true in general.

Theorem 2.16. *Let C be a k-dimensional linear code, and $d_1, \ldots, d_k$ be its generalized hamming weights. Then*

$$1 \leq d_1 < d_2 < \ldots < d_k \leq n.$$

Proof. See [Wei91, p. 1412]. □

2.4 Dual codes

We now want to look at the dual code, but to do this we first need an inner product. So let $\langle \cdot, \cdot \rangle$ be the standard dot product on $\mathbb{F}_q^n$. We can the define the orthogonal space of a subspace in this vector space.

Definition 2.17. *Let $L \subseteq \mathbb{F}_q^n$ be a subspace. Then the* orthogonal space *of L is*

$$L^\perp = \{\mathbf{w} \in \mathbb{F}_q^n | \langle \mathbf{w}, \mathbf{v} \rangle = 0 \text{ for all } \mathbf{v} \in L\}.$$

The dual code C^* of a linear code C is defined as the orthogonal complement of the code, $C^* = C^\perp$. Since C^* is still a subspace of $\mathbb{F}_q^n$, it is a linear code with word-length n, and since it is the orthogonal complement of C, we have that $\dim C^* = n - k$. The parity-check matrix of C is a generator matrix of C^*, and for the dual code the generator matrix of C acts as a parity check matrix, so their roles reverse.

But the minimum distance d^* of the dual code is not trivially found from n, k, d nor q for C. The dual code still has hamming weights, and also generalized hamming weights d_i^* since it is a linear code. With this we can formulate the Wei-duality theorem.

Theorem 2.18 (Wei-duality theorem)**.** *Let C be a k-dimensional linear code in $\mathbb{F}_q^n$, and C^* its dual code. Then*

$$\{d_i | 1 \leq i \leq k\} = \{1, 2, \ldots, n\} \backslash \{n + 1 - d_i^* | 1 \leq i \leq n - k\}$$

Proof. See [Wei91, p. 1413]. □

One consequence of this theorem is that if we know all the generalized hamming weights of a code, we easily find the generalized hamming weights of its dual code.

Example 2.19 (Continuation of Example 2.15)**.** *We want to calculate the generalized hamming weights of a* $\mathrm{Ham}(7,4)^*$ *code. We already have the weights of a* $\mathrm{Ham}(7,4)$ *code, the set* $\{3,5,6,7\}$*. Using the Wei-duality theorem, we get that*

$$\begin{aligned}\{1,2,3,4,5,6,7\}\backslash\{n+1-d_i^*|1\leq i\leq 3\} &= \{3,5,6,7\}\\ &\Downarrow\\ \{n+1-d_i^*|1\leq i\leq 3\} &= \{1,2,4\}\\ &\Downarrow\\ \{d_i^*|1\leq i\leq 3\} &= \{4,6,7\},\end{aligned}$$

so the generalized hamming weights are $d_1^*=4$*,* $d_2^*=6$ *and* $d_3^*=7$*.*

2.5 Shortening and puncturing

Another construction to get codes from other codes is shortening and puncturing. Shortening a code can be useful if we want a code with a specific length and minimum distance, and already know a code of greater length and the same minimum distance.

Let C be a linear code of dimension k in $\mathbb{F}_q^n$, and fix a coordinate position $1\leq j\leq n$. We now select all codewords in C where the j-th coordinate is 0, and remove the j-th coordinate from all codewords. Let this new code be C', called a shortened code of C. We see that C' has a shorter length, namely $n-1$, and at most as many codewords as C, but the minimum distance is greater than or equal to the minimum distance of C. If C has a parity-check matrix H, then we see that we get a parity-check matrix for C' by deleting the j'th column of H. More generally, we can shorten to a subset X (where X is a subset of the column-labels of the generator matrix for the code),

$$C(X)=\{\mathbf{x}\in C|\,\mathrm{supp}(\mathbf{x})\subseteq X\}.$$

If we remove one column of the generator matrix for a linear code C, we

are puncturing the code. The code that is generated by this matrix is called a punctured code of C. This punctured code has length $n-1$, dimension either k or $k-1$, and minimum distance at most the minimum distance of C. If E is the set of column labels of G, and $X \subseteq E$, let $C|_{E\setminus X}$ be a punctured code of C that is generated by G', where G' is obtained from G by removing the columns that are labeled by X.

By the construction, we can see that $C(X) = ((C^*)|_{E\setminus X})^*$. Note that we have the exact sequence

$$0 \to C(X) \to C \to C|_{E\setminus X} \to 0. \tag{2.20}$$

3 Matroids

Matroids are an abstraction of the concept of independence in finite sets. One concrete example of where they show up is with finite sets of vectors. If the dimension of the span of these vectors is equal to the number of vectors, then the vectors are independent, and otherwise they are dependent. We may thus think of an independent set as a set of vectors where they all "point in different directions".

Another place where they show up is in graph theory. We may look at a set of edges in a graph, and ask if they form a spanning tree/forest. If they do, then the edges are independent, and otherwise they are dependent. So dependence in this sense means that the edges contains a cycle in the graph.

For notation, a subset $A = 1234 \subseteq \{1, \ldots, n\}$ will be an abbreviation for $A = \{1, 2, 3, 4\}$ when $n \leq 9$.

3.1 Axioms of matroids

There are several cryptomorphic sets of axioms that are used to define matroids. By being cryptomorphic, we mean that each set of axioms implies the other sets of axioms.

One set of axioms are based on the independent sets of a matroid.

Definition 3.1. *A matroid $M = (E, \mathcal{I})$ is a pair of a set E and a family $\mathcal{I}$ of subsets of E where $\mathcal{I}$ is the independent sets and satisfies the following axioms;*

(I1) $\emptyset \in \mathcal{I}$.

(I2) If $I' \subseteq I$ *and* $I \in \mathcal{I}$, *then* $I' \in \mathcal{I}$.

(I3) If $I, I' \in \mathcal{I}$ *and* $|I'| < |I|$, *then there exists an* $x \in I \backslash I'$ *such that* $I' \cup \{x\} \in \mathcal{I}$.

Another way of defining matroids is based on the rank function of the matroid.

Definition 3.2. *A set E with a rank function $r : E \to \mathbb{N}$ satisfying the following axioms is a matroid.*

(R1) If $X \subseteq E$, *then* $0 \leq r(X) \leq |X|$.

(R2) If $X \subseteq Y \subseteq E$, *then* $r(X) \leq r(Y)$.

(R3) If X and Y are subsets of E, then

$$r(X \cup Y) + r(X \cap Y) \leq r(X) + r(Y).$$

One way to recover the rank function from the independent sets is to define the rank function as

$$r(X) = \max\{|I| : I \subseteq X, I \in \mathcal{I}\}$$

A third way of defining matroids is based on the circuits of the matroid.

Definition 3.3. *A set E with a family $\mathcal{C}$ of subsets of E satisfying the following axioms is the circuits of a matroid.*

(C1) $\emptyset \notin \mathcal{C}$.

(C2) If $C, C' \in \mathcal{C}$ and $C' \subseteq C$, then $C' = C$.

(C3) If $C_1, C_2 \in \mathcal{C}$ and $C_1 \cap C_2 \neq \emptyset$, then for $x \in C_1 \cap C_2$, there exists an $C_3 \subseteq C_1 \cup C_2 \backslash \{x\}$ such that $C_3 \in \mathcal{C}$

One way to get the circuits of a matroid from the rank function is to define the circuits as

$$\mathcal{C} = \min\{C \subseteq E : r(C) = r(C\backslash\{x\}), \forall x \in C\}$$

We may also define a matroid by looking at its bases.

Definition 3.4. *A set E with a family $\mathcal{B}$ of subsets of E satisfying the following axioms is the bases of a matroid.*

(B1) $\mathcal{B} \neq \emptyset$.

(B2) If $B_1, B_2 \in \mathcal{B}$ and $x \in B_1 \backslash B_2$, there exists an element $y \in B_2 \backslash B_1$ such that $(B_1 \backslash \{x\}) \cup \{y\} \in \mathcal{B}$.

We may recover the bases from the circuits by defining the bases as

$$\mathcal{B} = \max\{X \subseteq E | C \not\subseteq X, \forall C \in \mathcal{C}\}.$$

We may also get the independent sets from the bases by defining the independent sets as

$$\mathcal{I} = \{I \subseteq B : B \in \mathcal{B}\}.$$

From how the rank function is derived from the independent sets, and how the independent sets are derived from the bases, we can see that

$$r(X) = \max\{|X \cap B||B \in \mathcal{B}\}.$$

For more details on the proofs of the cryptomorphism of these axioms, see [Oxl92].

Related to the rank function is the nullity function, defined on a subset $X \subseteq E$ as

$$n(X) = |X| - r(X).$$

3.2 Vector matroids

Given any matrix A, there is a matroid that is associated to this matrix.

Proposition 3.5. *Let E be a set of column labels of an $n \times m$ matrix A over a field $\mathbb{F}$. Let $\mathcal{I}$ be the set of subsets X of E such that the multiset of columns labeled by X is linearly independent in the vector space $\mathbb{F}^m$. Then $(E, \mathcal{I})$ is a matroid.*

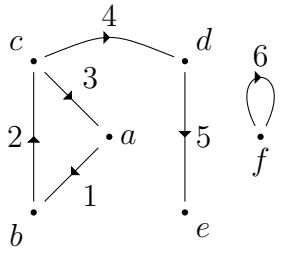
Proof. See [Oxl92, Prop 1.1.1]. □

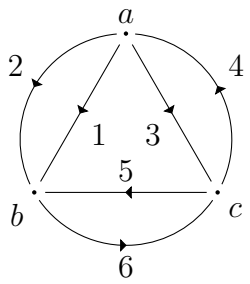
Definition 3.6. *Given a matrix A, the vector matroid $M[A]$ is the matroid $(E, \mathcal{I})$ from the previous proposition.*

Example 3.7. *Let us calculate the bases of the vector matroid $M[A]$ given the matrix*

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

over $\mathbb{F}_2$. Let the label i refer to the i'th column of A, so we get the ground set $E = \{1, 2, 3, 4, 5, 6\}$. Observe that this matrix has rank 2, so the bases are subsets of E of cardinality 2. There are 15 such subsets, but some of them are linearly





$$\begin{array}{c} \\ a \\ b \\ c \\ d \\ e \\ f \end{array} \begin{array}{c} \begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \end{array} \\ \begin{pmatrix} 1 & 0 & -1 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \end{array}$$

(a)

$$\begin{array}{c} \\ a \\ b \\ c \end{array} \begin{array}{c} \begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \end{array} \\ \begin{pmatrix} 1 & 1 & 1 & -1 & 0 & 0 \\ -1 & -1 & 0 & 0 & -1 & 1 \\ 0 & 0 & -1 & 1 & 1 & -1 \end{pmatrix} \end{array}$$

(b)

Figure 1: Two graphs and their incidence matrices. The directions of their edges have been chosen arbitrarily.

dependent. We can see that the three sets $\{1,2\}$*,* $\{3,4\}$ *and* $\{5,6\}$ *are dependent, but the rest are independent. We therefore get the bases*

$$\begin{aligned}\mathcal{B} = \{&\{1,3\},\{1,4\},\{1,5\},\{1,6\},\{2,3\},\{2,4\},\\ &\{2,5\},\{2,6\},\{3,5\},\{3,6\},\{4,5\},\{4,6\}\}.\end{aligned}$$

3.3 Graphical matroids

If we have a multigraph $G = (V, E)$, this induces a matroid. This matroid is on the set of edges of G, and a subset of edges is dependent if they contain a cycle. If we choose some arbitrary direction to the edges, we can create a vector matroid from this graph. In fact, every graphic matroid is representable over every field, see [Oxl92, Proposition 5.1.2]. If $D(G)$ is our directed graph, then let $A_{D(G)} = [a_{i,j}]$ be the incidence matrix of $D(G)$. This is the matrix whose rows are indexed by

(a) The two circuits 134 and 245 in $U_{2,5}$. (b) The circuits 1234, 5678 and 1256 in $U_{3,8}$.

Figure 2: Illustration of two uniform matroids. The elements will generally be labelled starting with 1 in the top left and increasing along the row, until the last element in the bottom right is labelled n.

vertices and columns are indexed by edges,

$$a_{i,j} = \begin{cases} 1, & \text{if vertex } i \text{ is the tail of a non-loop edge } j, \\ -1, & \text{if vertex } i \text{ is the head of a non-loop edge } j, \\ 0, & \text{otherwise.} \end{cases}$$

Some graphs an their incidence matrices are shown in Figure 1.

3.4 Uniform matroids

Uniform matroids are particularly simple in their construction[1]. The uniform matroid $U_{k,n}$ is a matroid of rank k on a ground set of n elements. The bases of this matroid are all subsets of the ground set of size k. This immediately gives an explicit rank function for this matroid:

$$r(X) = \min\{|X|, k\}.$$

Figure 2 shows two uniform matroids.

3.5 Dual matroids

One interesting thing about matroids is that they have duals. These duals are an abstraction of both the orthogonality of vector spaces and planar duals of plane graphs. The following theorem is useful for the definition of the dual of a matroid.

[1]But this does not mean that they necessarily are simple!

Theorem 3.8. *Let M be a matroid and $\mathcal{B}^*(M)$ be $\{E(M)\backslash B | B \in \mathcal{B}(M)\}$. Then $\mathcal{B}^*(M)$ is the set of bases of a matroid on $E(M)$.*

Proof. See [Oxl92, Theorem 2.1.1]. □

This matroid with bases $\mathcal{B}^*(M)$ on the ground set $E(M)$ is called the *dual* of the matroid M and is denoted by M^*. In general, the asterisk $*$ is used for denoting association to the dual. Thus r^* would be the rank function of the dual matroid, also called the corank of the matroid. From how the dual matroid is defined, it is clear that

$$r(M) + r^*(M) = |E(M)|.$$

Example 3.9 (Continuation of Example 3.7)**.** *We want to calculate the bases of the dual matroid $M[A]^*$. Immediately we can see that this dual matroid is a matroid of rank* 4*. Since we already have the set of bases for $M[A]$, it is quite easy to calculate $\mathcal{B}^*$.*

$$\begin{aligned}\mathcal{B}^* = \{&\{2,4,5,6\},\{2,3,5,6\},\{2,3,4,6\},\{2,3,4,5\},\{1,4,5,6\},\{1,3,5,6\},\\ &\{1,3,4,6\},\{1,3,4,5\},\{1,2,4,6\},\{1,2,4,5\},\{1,2,3,6\}\{1,2,3,5\}\}.\end{aligned}$$

We can have an even more explicit formulation of the corank function.

Proposition 3.10. *For all subsets $X \subseteq E(M)$,*

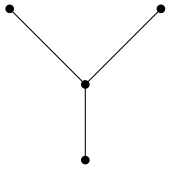
$$r^*(X) = |X| - r(E(M)) + r(E(M)\backslash X).$$

Proof. See [Oxl92, Proposition 2.1.9]. □

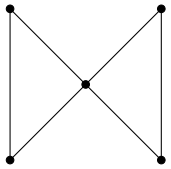
3.6 Connectedness and sums of matroids

Definition 3.11. *A matroid M is connected if and only if for all distinct pairs $e, f \in E(M)$, there is at least one circuit $C \in \mathcal{C}(M)$ such that $e, f \in C$.*

If we have a graphical matroid, the notion of connectedness in a graph and in the matroid is not the same. This is illustrated in Figure 3.



(a) Here we have the matroid $M = U_{3,3} = U_{1,1} \oplus U_{1,1} \oplus U_{1,1}$.



(b) Here we have the matroid $M = U_{2,3} \oplus U_{2,3}$.

Figure 3: Two connected graphs where the associated matroid is not connected.

Definition 3.12. *The sum of two matroids $M = M_1 \oplus M_2$ has the ground set as the disjoint union of the ground sets of the two matroids, $E = E(M_1) \sqcup E(M_2)$, and independent sets $\mathcal{I} = \{I_1 \sqcup I_2 | I_1 \in \mathcal{I}(M_1), I_2 \in \mathcal{I}(M_2)\}$.*

Proposition 3.13. *Let $M = M_1 \oplus M_2$ be the sum of two matroids. Then $(E, \mathcal{I})$ from the previous definition is a matroid.*

Proof. See [Oxl92, Proposition 4.2.12]. □

3.7 Minors

Definition 3.14. *The deletion $M\backslash X$ of a matroid M by a set $X \subseteq E(M)$ is the matroid on the ground set $E(M)\backslash X$ having independent sets $\mathcal{I}(M\backslash X) = \{I \subseteq E(M)\backslash X : I \in \mathcal{I}(M)\}$.*

The deletion of a set X is also called the restriction to the set $E(M)\backslash X$. It is easy to see that $M\backslash X = (E(M)\backslash X, \mathcal{I}(M\backslash X))$ is a matroid, and that the circuits of this matroid are

$$\mathcal{C}(M\backslash X) = \{C \subseteq E(M)\backslash X : C \in \mathcal{C}(M)\}.$$

Definition 3.15. *The contraction of X from M is the matroid*

$$M/X = (M^*\backslash X)^*$$

We can immediately see that M/X is a matroid, since both deletion and taking the dual yields matroids. Now we can find the circuits of a contracted matroid.

Proposition 3.16. *The circuits of M/X are*

$$\mathcal{C}(M/X) = \min\{C\backslash X : C \in \mathcal{C}(M), C\backslash X \neq \emptyset\}.$$

Proof. See [Oxl92, Proposition 3.1.11]. □

Proposition 3.17. *Doing contractions and deletions commute. Therefore we may write $M\backslash X/Y$ for a matroid contracted by elements of a set Y and deleted by elements of the set X in some order, where X and Y are disjoint subsets of $E(M)$.*

Proof. See [Oxl92, Proposition 3.1.26(iii)]. □

Definition 3.18. *A* minor *M' of a matroid M is a matroid such that there exists $X, Y \subseteq E(M)$ such that $M' = M\backslash X/Y$.*

3.8 Connection to codes

For any code C we naturally get a matroid associated with its generator matrix, the vector matroid earlier mentioned. Denote by M_C the matroid associated with the generator matrix G. This matroid is independent of the choice of the generator matrix. A result from linear algebra gives that if two matrices A and B are row equivalent, then a set of column vectors of A is linearly independent if and only if the set of corresponding columns of B are linearly independent. We also have that for two matrices G and G' that have the same row-space, they are row equivalent. Hence we can see that the choice of a generator matrix is independent of the matroid associated with a linear code.

There is a class of matroids called representable matroids. These are matroids M such that there exists a matrix A where $M \simeq M[A]$. We can see that the class of representable matroids over $\mathbb{F}_q$ are the matroids that comes from linear codes over $\mathbb{F}_q$. There are also matroids that are not representable, such as the Vámos matroid in Figure 4, and they have no natural connection to linear codes.

Another connection between codes and matroid is the notion of duality.

Proposition 3.19. *Let C be a linear code over $\mathbb{F}_q$, and M_C the matroid associated to this code. Then the dual of M_C is the matroid associated to the dual code C^*,*

$$M_{C^*} = M_C^*.$$

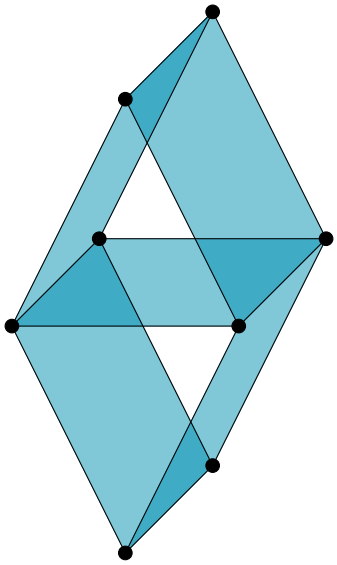


Figure 4: The Vámos matroid is a matroid of rank 4 on 8 elements. All sets of cardinality smaller than 4 are independent, and the only dependent sets of cardinality 4 are the ones that share a face in this figure, where the elements are represented as vertices.

Proof. See [Oxl92, Theorem 2.2.8]. □

There are also a connection between the minors of a matroid M_C, and shortened/punctured codes of C. If $X \subseteq E$, we have that $M_{C|_{E\backslash X}} = M\backslash X$, where deletion corresponds to puncturing. We can now also see that the shortening corresponds to contraction, $M_{C(X)} = M/(E\backslash X)$. Observe from Equation (2.20) that we can find the dimensions of the codes. In particular, we find that

$$\dim C(X) = \dim C - \dim C|_{E\backslash X} = r_{M_C}(E) - r_{M_C}(E\backslash X) = n^*_{M_C}(X). \tag{3.20}$$

3.9 Hamming distance for matroids

For a linear code C we know that a vector $\mathbf{w} = (w_1, \ldots, w_n)$ is a code-word if it is in the null space of the parity-check matrix H. This is equivalent to saying that $\sum \mathbf{C}_i w_i = \mathbf{0}$ where C_i are the columns of H. Now assume that $\mathbf{w}$ is a non-zero code-word of the smallest weight. By Proposition 2.12, this means that the weight of this code-word is the minimum distance of the code, and we have that

d_1 columns of H are linearly dependent. If we assume that we have a set of fewer than $d(C)$ columns of H that are linearly dependent, then we would have another code-word of smaller weight than $\mathbf{w}$, so we get

$$d(C) = d_1 = \min\{s | s \text{ columns of } H \text{ are linearly dependent}\}.$$

This can immediately be formulated in terms of the dual matroid, and at the same time generalized to higher weights

$$d_h = \min\{|X||X \subseteq E, r^*(X) \leq |X| - h\}.$$

Here r denotes the rank function of M_C and r^* the rank function of M_C^*. Moreover a subset $L \subseteq C$ is supported on X if and only if there are are least h relations between the columns of H supported on X. Now using Proposition 3.10, we get

$$\begin{aligned} d_h &= \min\{|X||X \subseteq E, r^*(X) \leq |X| - h\} \\ &= \min\{|X||X \subseteq E, |X| + r(E\backslash X) - r(E) \leq |X| - h\} \\ &= \min\{|X||X \subseteq E, r(E\backslash X) \leq r(E) - h\} \\ &= \min\{|E\backslash X||X \subseteq E, r(X) \leq r(E) - h\} \\ &= n - \max\{|X||X \subseteq E, r(X) \leq r(E) - h\} \end{aligned}$$

The previous paragraph was relating the minimum distance of a code to the matroid of the code. We now got a way of formulating this purely in matroid terms, so we can define the generalized hamming weights for a matroid (both representable and non-representable) as

Definition 3.21. *Given any matroid with rank function r and ground set E, the generalized hamming weights are*

$$d_h = n - \max\{|X||X \subseteq E, r(X) \leq r(E) - h\},$$

where $h \leq r(E)$.

Note that again using Proposition 3.10 with this definition, we get that

$$d_h = \min\{|X||X \subseteq E, r^*(X) \leq |X| - h\} = \min\{|X||X \subseteq E, n^*(X) \geq h\}$$

for all matroids.

Example 3.22. *We can now calculate the generalized hamming weights for the non-representable Vámos matroid, see Figure 4. The largest possible set of rank* 3 *in this matroid has cardinality* 4*, so we get that* $d_1 = 8 - 4 = 4$*. Since all sets of cardinality* 3 *or less are independent, every set* X *where* $|X| \geq 3$ *has that* $r(X) \geq 3$*. Therefore, the largest sets of rank at most* 2*,* 1 *and* 0 *are respectively sets of cardinality* 2*,* 1 *and* 0*. We therefore get that* $d_2 = 8-2 = 6$*,* $d_3 = 8-1 = 7$ *and* $d_4 = 8 - 0 = 8$*.*

With these generalized weights for matroids, we can get results analogous to Theorem 2.16 and Theorem 2.18 for matroids.

Theorem 3.23. *Let* M *be a matroid. Then the generalized hamming weights are strictly increasing,*

$$1 \leq d_1 < d_2 < \cdots < d_{r(M)} \leq |E(M)|.$$

Proof. Let $1 < h \leq r(M)$, and let $X \in \{X \subseteq E | n^*(X) \geq h\}$ such that $d_h = |X|$. If we remove any single element from X, then the conullity will decrease by at most one, so therefore $n^*(X) = h$. This also implies that for $X' = X \backslash \{x\}, x \in X$ we have that $n^*(X') \geq h - 1$, and thus $d_{h-1} \leq |X'| = |X| - 1 < d_h$, yielding the result. □

Theorem 3.24. *Let* M *be a matroid with generalized hamming weights* d_i *and let* d_i^* *be the generalized hamming weights of* M^**. Then*

$$\{1, \cdots, |E(M)|\} \backslash \{d_i | 1 \leq i \leq r(M)\} = \{|E(M)| + 1 - d_i^* | 1 \leq i \leq r^*(M)\}.$$

Proof. See [Lar05, Proposisjon 5.18]. □

4 Derived matroids

This section will introduce several ways of creating a "derived matroid" from a given matroid. These are used for investigating "dependencies among dependencies", but have more potential applications such as in private information retrieval [FK21], and also checking the planarity of graphs [Lon80]. The derived matroid generally uses the circuits of the original matroid as a ground set, so the following terminology will be used when it might be ambiguous what matroid a circuit is a member of. 0-circuit will refer to a circuit in the original matroid M, 1-circuit will refer to a circuit in the derived matroid δM, and in general a k-circuit will be a circuit in the matroid $\delta^k M = \delta(\delta^{k-1}M)$.

Fundamental circuits are also utilized. Given a basis B of a matroid M, the fundamental circuit $C_{e,B}$ for an element $e \in E(M)\backslash B$ is the unique circuit $C \subseteq B \cup \{e\}$.

4.1 Binary matroids

The first to introduce the concept of derived matroids was Longyear [Lon80] for binary matroids. These were created to begin answering questions posed by Gian-Carlo Rota to investigate "dependencies among dependencies". One way of looking at the relation between the dependent sets is to look at the symmetric difference of them. The symmetric difference can be iterated, known as the Kirkhoff sum.

Definition 4.1. *The Kirkhoff sum of a set of sets is*

$$K(A) = \{e \in \text{supp}(A) | \#\{C | e \in C, C \in A\} \text{ is odd}\}$$

Definition 4.2. *A circuit basis for a binary matroid M is a minimal set of circuits $A \subseteq \mathcal{C}(M)$ such that for all $C \in \mathcal{C}(M)$ there exists $S \subseteq A$ such that $C = K(S)$.*

Using these circuit bases, we can create a derived matroid.

Definition 4.3. *Let M be a binary matroid. The Longyear derived matroid $\delta_L M$ is a matroid on the ground set $\mathcal{C}(M)$ with the bases being the circuit bases of M.*

Longyear further proved that $\delta_L M$ is a binary matroid.

We can see that any dependent set $A \subseteq E(\delta_L M)$ is a set such that there exists a non-empty set $S \subseteq A$ such that $K(S) = \emptyset$. If we were to use this property to define dependencies, we can extend the definition to all matroids. This idea is further explored in Section 4.9.

Longyear also noted that another extension of this to representable matroids over a field of characteristic p is to let the 1-circuits be the minimal sets of 0-circuits where each edge occurs in a multiple of p of the 0-circuits in the set. The problem is that there is not always a canonical choice of p, since some matroids can be represented over fields of different characteristics.

4.2 Representable matroids

Oxley and Wang [OW19] extended and generalized the concept of derived matroids to representable matroids. The idea is; for a given representation of a matroid, use the minimal elements of the null space of this matrix as columns in a new derived code, and have the derived matroid be the vector matroid of this new matrix.

Let M be a representable matroid, and $G \in \mathbb{F}_q^{k\times n}$ be some representation of this matroid. We have with this an associated code that is generated by the matrix G, and a parity-check matrix H. Associated with each circuit $C \in \mathcal{C}(M)$, we have a vector $\mathbf{q}_C = (q_1, \ldots, q_n) \in \mathbb{F}_q^n$ such that $H\mathbf{q}_C = \mathbf{0}$ and $q_i \neq 0 \Leftrightarrow i \in C$. We can then create a matrix $A = [\mathbf{q}_{C_1}, \ldots, \mathbf{q}_{C_{|\mathcal{C}(M)|}}]$, and let $\delta_{OW} M[G] = M[A]$.

Definition 4.4. *Given a representable matroid M with representation G, the Oxley-Wang derived matroid is the matroid $\delta_{OW} M[G]$. If the representation is clear from context, we will simply write $\delta_{OW} M$.*

By the construction, the Oxley-Wang derived matroid for a given representation is also a representable matroid. Also since taking linear combinations over $\mathbb{F}_2$ coincides with the Kirkhoff sum, we can see that the Oxley-Wang derived matroid is a generalization of the Longyear derived matroid.

Proposition 4.5. *Let M be a representable matroid with representation G. Then $\delta_{OW} M$ is a simple matroid of rank $|E(M)| - r(M)$. In particular, if B is a basis of M, then the set of fundamental circuits $\{C_{e,B} | e \in E(M)\backslash B\}$ is a basis of $\delta_{OW} M$.*

Proof. See [OW19, Lemma 3]. □

Definition 4.6. *The* simplification $\text{simplify}(M)$ *of a matroid* M *is obtained by deleting all loops and then deleting one element from each* 2*-element circuit until no parallel edges remain. The* cosimplification *arises from the dual of the simplified dual,* $\text{cosimplify}(M) = \text{simplify}(M^*)^*$.

Oxley and Wang proved further results such as that $U_{2,4}$ is the only matroid where $\delta_{OW}M = M$, cosimplification of a matroid does not change the derived matroid and that the only matroids that are not dependent on the representation are when they are representable over $\mathbb{F}_2$ or $\mathbb{F}_3$. We also have that the derived matroid of a sum of matroids is the sum of the derived matroids.

Example 4.7. *As an example, let us calculate the derived matroid of the matroid* M_C *associated with the generator matrix* G *of the linear code* $\text{Ham}(7,4)$ *over* $\mathbb{F}_2$. *With the following generator matrix*

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

we have the circuits $\mathcal{C} = \{2345, 1346, 1256, 1247, 1357, 2367, 4567\}$. *Using the corresponding circuit vectors as columns of a matrix, we get*

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

We now have that $\delta_{OW}M_C = M[A]$. *If we look at the row-echelon form of* A *(and*

remove zero-rows), we get

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

Observe that this is the parity-check matrix of a $\mathrm{Ham}(7,4)$ *code, so we have that* $\delta_{OW} M_C \simeq M_C^*$.

4.3 Combinatorial derived matroids

We now have a way of looking at dependencies among dependencies of binary matroids and representable matroids. However, for the representable matroids the derived matroid may be dependent on its representation, and what about non-representable matroids? Freij-Hollanti, Jurrius, and Kuznetsova [FJK23] propose the combinatorial derived matroid, which will solve these problems.

Let $M = (E, \mathcal{C})$ be a matroid. Define the following functions:

$$\begin{aligned} \epsilon : 2^{2^{\mathcal{C}}} &\to 2^{2^{\mathcal{C}}} \\ \mathcal{A} &\mapsto \mathcal{A} \cup \{A_1 \cup A_2 \backslash \{C\} : A_1, A_2 \in \mathcal{A}, A_1 \cap A_2 \notin \mathcal{A}, C \in A_1 \cap A_2\} \\ \uparrow : 2^{2^{\mathcal{C}}} &\to 2^{2^{\mathcal{C}}} \\ \mathcal{A} &\mapsto \{A \subseteq \mathcal{C} : \exists A' \in \mathcal{A} : A' \subseteq A\} \end{aligned}$$

and let $\min \mathcal{A}$ denote the inclusion minimal sets of $\mathcal{A}$. For notation, let

$$\begin{aligned} \mathrm{supp} : 2^{2^{E(M)}} &\to 2^{E(M)} \\ A &\mapsto \cup_{C \in A} C \end{aligned}$$

The ϵ and $\uparrow$operations will be used iteratively on some seed set to generate the dependent sets of the matroid. Let the initial seeding set be defined as

$$\mathcal{A}_0 = \{A \subseteq \mathcal{C}(M) || A| > n(\mathrm{supp}(A))\}.$$

Iteratively we let $\mathcal{A}_{i+1} = \uparrow \epsilon(\mathcal{A}_i)$, and the final dependent sets are $\mathcal{A} = \cup_{i \geq 0} \mathcal{A}_i$.

	Cardinality of circuits of $\delta_{FJK}M$			
Matroid	**3**	**4**	**5**	**6**
$\delta_{FJK}U_{2,6}$	60	510	3432	
$\delta_{FJK}U_{2,7}$	140	1785	24024	222600
$\delta_{FJK}U_{3,5}$	10			
$\delta_{FJK}U_{3,6}$	60	735		
$\delta_{FJK}U_{3,7}$	210	5145	127232	

Table 1: Number of circuits of a given size in $\delta_{FJK}M$ for the given matroid. We can see that these sizes are the same for the Oxley-Wang derived equivalents in [FJK23, Table 1]. These numbers were calculated using the software library available at `https://github.com/teo8192/matroid-rs` [Knu23]

.

Note that the sequence $\mathcal{A}_i$ is increasing and a subset of the finite set $2^{\mathcal{C}}$, so $\mathcal{A} = \mathcal{A}_n$ for some $n \geq 0$. To avoid edge cases in some proofs and/or definitions, also let $\mathcal{A}_i = \emptyset$ for any $i < 0$. We say that a set $A \in \mathcal{A}_i \backslash \mathcal{A}_{i-1}$ has *depth* i in $\mathcal{A}$.

Definition 4.8. *Let M be a matroid with circuits $\mathcal{C}$. The combinatorial derived matroid $\delta_{FJK}M$ is the matroid with ground set $\mathcal{C}$ and dependent sets $\mathcal{A}$.*

Proposition 4.9. *For any matroid $M = (E, \mathcal{C})$, the collection $\mathcal{A}$ is the collection of dependent sets of some matroid with ground set $\mathcal{C}$.*

Proof. See [FJK23, Proposition 17]. □

We can easily set an upper boundary for the rank of the combinatorial derived matroid. One way to look at this is to see that for a matroid M, any set of more than $|E(M)| - r(M)$ circuits will have its nullity at most $|E(M)| - r(M)$, so this set will be in $\mathcal{A}_0$, and is therefore dependent.

Proposition 4.10. *Let M be a matroid. The rank of $\delta_{FJK}M$ is at most $|E(M)| - r(M)$.*

Proof. See [FJK23, Lemma 37]. □

Section 4.6 deals more with a certain class of matroids where the rank of the combinatorial derived matroid is equal to the corank of the matroid. But this is not generally the case, as the next example illuminates.

Example 4.11. *Let M be the Vámos matroid. Using the software that is developed as a part of this thesis, we can calculate $\delta_{FJK}M$. $\delta_{FJK}M$ is a matroid of rank 3 on 41 elements, and has 91026 circuits. This is therefore an example of a matroid where the rank of the combinatorial derived matroid is strictly smaller than the corank of the matroid.*

We now give a new and useful result:

Proposition 4.12. *Let M be a matroid, and M' be a minor of M. Then there exists an injection $\psi : \mathcal{C}(M') \hookrightarrow \mathcal{C}(M)$ that extends to an injection $\phi : 2^{\mathcal{C}(M')} \hookrightarrow 2^{\mathcal{C}(M)}$ such that $n_{M'}(\mathrm{supp}(A)) \geq n_M(\mathrm{supp}(\phi(A)))$ for all $A \subseteq \mathcal{C}(M')$. Moreover, if $M' = M\backslash Y$ for some $Y \subseteq E(M)$, then $n_{M'}(\mathrm{supp}(A)) = n_M(\mathrm{supp}(\phi(A)))$.*

Proof. First, lets construct the first injection, call it ψ. Let $Y = \{e_1, \ldots, e_l\}$.

$$\mathcal{C}(M') = \mathcal{C}(M\backslash Y/\{e'_1, \ldots, e'_k\}) \xrightarrow{\psi_{e'_1}} \mathcal{C}(M\backslash Y/\{e'_2, \ldots, e'_k\}) \xrightarrow{\psi_{e'_2}} \cdots \xrightarrow{\psi_{e'_k}} \mathcal{C}(M\backslash Y)$$
$$\mathcal{C}(M\backslash Y) = \mathcal{C}(M\backslash\{e_1, \ldots e_l\}) \xrightarrow{\psi_{e_1}} \mathcal{C}(M\backslash\{e_2, \ldots e_l\}) \xrightarrow{\psi_{e_2}} \cdots \xrightarrow{\psi_{e_l}} \mathcal{C}(M)$$

Let $\psi = \psi_{e_l} \circ \cdots \circ \psi_{e_1} \circ \psi_{e'_k} \circ \cdots \circ \psi_{e'_1}$. For each deleted e_i, we see that by the definition of the circuits in the deletion of the matroid, $\mathcal{C}(M_1\backslash\{e_i\}) \subseteq \mathcal{C}(M_1)$, and let $\psi_{e_i} = \mathrm{id}$. Now lets construct $\psi_{e'_i} : \mathcal{C}(M_1/\{e'_i\}) \to \mathcal{C}(M_1)$. For each $C \in \mathcal{C}(M_1/\{e'_i\})$, we may find an $C' \in \mathcal{C}(M_1)$ such that $C = C'\backslash\{e'_i\}$ by Proposition 3.16, and let $\psi_{e'_i}(C) = C'$. If $\psi_{e'_i}(C_1) = \psi_{e'_i}(C_2)$, then $C_1 = C'\backslash\{e'_i\} = C_2$, so it is injective. Since each ψ_e is injective, their composition ψ is injective.

Now define

$$\begin{aligned} \phi : 2^{\mathcal{C}(M')} &\to 2^{\mathcal{C}(M)} \\ A &\mapsto \{\psi(C) : C \in A\}. \end{aligned} \tag{4.13}$$

Since ψ is injective, ϕ is injective. Also let $\phi_e(A) = \{\psi_e(C) : C \in A\}$. We see that $\phi = \phi_{e_l} \circ \cdots \circ \phi_{e_1} \circ \phi_{e'_k} \circ \cdots \circ \phi_{e'_1}$. Now consider e such that we have an ϕ_e. If this corresponds to a deletion, we have that $n_{M_1\backslash\{e\}}(\mathrm{supp}(X)) = n_{M_1}(\mathrm{supp}(\phi_e(X))) = n_{M_1}(\mathrm{supp}(X))$ for all $X \subseteq \mathcal{C}(M_1\backslash\{e\})$, by [Oxl92, (3.1.5)] and the fact that $\psi_e = \mathrm{id}$. Now consider the case when ϕ_e corresponds to a contraction. From [Oxl92,

Proposition 3.1.6] and some manipulation, we get for $X \subseteq E(M_1)\backslash\{e\}$

$$n_{M_1/\{e\}}(X) = n_{M_1}(X \cup \{e\}) - n_{M_1}(e).$$

Let $A \subseteq \mathcal{C}(M_1/\{e\})$. If e is a loop in M_1, then $e \notin \text{supp}(\phi_e(A))$, and we get

$$n_{M_1/\{e\}}(\text{supp}(A)) = n_{M_1}(\text{supp}(\phi_e(A))).$$

Otherwise, $n_{M_1}(e) = 0$, and we get

$$\begin{aligned} n_{M_1/\{e\}}(\text{supp}(A)) &= n_{M_1}(\text{supp}(A) \cup \{e\}) \\ &\geq n_{M_1}(\text{supp}(\phi_e(A))) \end{aligned} \tag{4.14}$$

Since $n_{M_1'}(\text{supp}(A)) \geq n_{M_1}(\text{supp}(\phi_e(A)))$ for all ϕ_e where either $M_1' = M_1\backslash\{e\}$ or $M_1' = M_1/\{e\}$, so we have

$$n_{M'}(\text{supp}(A)) \geq n_M(\text{supp}(\phi(A)))$$

for all $A \subseteq \mathcal{C}(M')$.

Further, we can see that since $n_{M_1'}(\text{supp}(A)) = n_{M_1}(\text{supp}(\phi_e(A)))$ when $M_1' = M_1\backslash\{e\}$, we have when $M' = M\backslash Y$

$$n_{M'}(\text{supp}(A)) = n_M(\text{supp}(\phi(A)))$$

for all $A \subseteq \mathcal{C}(M')$. □

For an example where the nullity will decrease consider the graphical matroids $M' = M(\text{Sh}(4))$ and $M = M(G_1)$ from Figure 5. If we have $A = \{12, 34, 56\} \subseteq \mathcal{C}(M')$, then $n_{M'}(\text{supp}(A)) = 4$, but $\phi(A) = \{12, 34, 45\}$ and $n_M(\text{supp}(\phi(A))) = 3$.

By the construction of ϕ defined in Equation (4.13), we have some immediate properties of this function.

Corollary 4.14.1. *$\phi(X \cap Y) = \phi(X) \cap \phi(Y)$, $\phi(X \cup Y) = \phi(X) \cup \phi(Y)$ and $\phi(X\backslash Y) = \phi(X)\backslash\phi(Y)$. If $Y \subseteq X$, then $\phi(Y) \subseteq \phi(X)$.*

A series class is a set $S \subseteq E(M)$ such that for all $e, f \in S$, $\{e, f\}$ is a cocircuit.

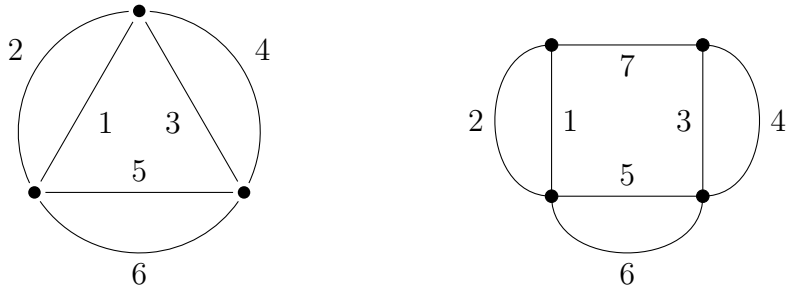


Figure 5: The graph on the left is the Shannon multigraph Sh(4), and name the graph on the right G_1. Observe that $M(\mathrm{Sh}(4)) = M(G_1)/\{7\}$.

Further, if $C \in \mathcal{C}(M)$ is a circuit and $e \in C$, then $f \in C$. This can be seen by considering $H = E(M)\backslash C$, and assume that $e \in C$ but $f \notin C$. H is a cohyperplane [Oxl92, Proposition 2.1.6 (iii)], so adding any element to it will increase the corank. But since $\{e, f\}$ is a cocircuit and $f \in H$, $r^*(H) = r^*(H \cup \{e\})$ contradicting that H is a cohyperplane. Note that if C is a cycle in M and $e \in C$, then $f \in C$.

Proposition 4.15. *Let M be a matroid, and $M' = \mathrm{cosimplify}(M)$. Then ϕ is a bijection, and $n_{M'}(\mathrm{supp}(A)) = n_M(\mathrm{supp}(\phi(A)))$ for all $A \subseteq \mathcal{C}(M')$.*

Proof. Let e be a coloop in M. Then e is not contained in any circuit nor any cycle of M, so we can see that $\mathcal{C}(M) = \mathcal{C}(M\backslash\{e\})$. Thus if $Y \subseteq E(M)$ is the set of coloops of M, then $\mathcal{C}(M) = \mathcal{C}(M\backslash Y)$.

If $X \subseteq E(M)$ is such that every series class of M has all but one element in X, then we can clearly see that $|\mathcal{C}(M)| = |\mathcal{C}(M/X)|$.

Since cosimplification is the deletions of all coloops and contraction of all but one element of each series class, $\mathrm{cosimplify}(M) = M\backslash Y/X$. We can thus see that since ϕ is an injection and $|\mathcal{C}(M)| = |\mathcal{C}(M')|$, it is a bijection.

To show that the nullity is preserved by ϕ, we need to show that it is preserved under the specific contractions. Consider $e \in S$ for a series class S with at least two elements, $M_1 = M$, $M_1' = M/\{e\}$ and $A \subseteq \mathcal{C}(M_1')$. We had the inequality (4.14)

$$n_{M_1'}(\mathrm{supp}(A)) = n_{M_1}(\mathrm{supp}(A) \cup \{e\}) \geq n_{M_1}(\mathrm{supp}(\phi_e(A))).$$

If $e \in \mathrm{supp}(\phi(A))$, then there is equality. Otherwise, we have that $\phi_e(A) = A$. Since $\mathrm{supp}(A)$ is a cycle in M_1, but $\mathrm{supp}(A) \cup \{e\}$ is not a cycle since, by the

construction of X, it does not contain all elements in the series class containing e,

$$n_{M_1}(\text{supp}(\phi_e(A))) = n_{M_1}(\text{supp}(A)) = n_{M_1}(\text{supp}(A) \cup \{e\}).$$

Thus since the nullity is preserved for each ϕ_e, their composition preserves the nullity as well,

$$n_{M'}(\text{supp}(A)) = n_M(\text{supp}(\phi(A))),$$

for all $A \subseteq \mathcal{C}(M')$. □

Corollary 4.15.1. $\delta_{FJK}M = \delta_{FJK}\,\text{cosimplify}(M)$.

Proposition 4.16. *Let M be a matroid, M' a minor of M and ϕ the injection from Proposition 4.12. If X is a dependent set in $\delta_{FJK}M'$, then $\phi(X)$ is dependent in $\delta_{FJK}M$.*

Proof. Let $X \in \mathcal{A}_0(\delta_{FJK}M')$. Since ϕ is injective, that $n(\text{supp}(X)) \geq n(\text{supp}(\phi(X)))$, and that $n(\text{supp}(X)) < |X| = |\phi(X)|$, we get that $n(\text{supp}(\phi(X))) < |\phi(X)|$.

Now by induction, assume that this is true for all $X \in \mathcal{A}_i(\delta_{FJK}M')$ of depth i. Let $A \in \mathcal{A}_{i+1}(\delta_{FJK}M')$ have depth $i+1$. We have that $A = A_1 \cup A_2 \backslash \{C\}$ for some $C \in A_1 \cap A_2$. Then $\phi(A) = \phi(A_1 \cup A_2 \backslash \{C\}) = \phi(A_1) \cup \phi(A_2) \backslash \{\psi(C)\}$ where $\psi(C) \in \phi(A_1) \cap \phi(A_2)$. Thus $\phi(A) \in \mathcal{A}_{i+1}(\delta_{FJK}M)$. □

Proposition 4.17. *The only uniform matroids where $\delta_{FJK}U_{k,n} = U^*_{k,n}$ is $U_{0,n}$ and $U_{n-2,n}, n \geq 3$.*

Proof. We need that the number of elements in the matroid is the same as the number of elements in the derived matroid. This means that the number of elements in the matroid has to be the same as the number circuits in the matroid. For uniform matroids, this restriction means that $n = \binom{n}{k+1}$. Thus we get that either $k = 0$ or $k = n-2$.

Assume $k = 0$. We see that $U_{0,n}$ has n circuits that are loops, and since they are loops we have that for all $A \subseteq \mathcal{C}$, $|A| = n(\cup_{C \in A} C)$. Therefore we get that $\mathcal{A}_0 = \emptyset$. Observe that $\uparrow\epsilon(\emptyset) = \emptyset$, so $\delta_{FJK}U_{0,n}$ has no dependent sets. Therefore $\delta_{FJK}U_{0,n} = U_{n,n} = U^*_{0,n}$.

Otherwise, let $k = n-2$, and we may assume that $n \geq 3$. From [FJK23], we know that for this matroid, any dependent set A in $\delta_{FJK}U_{n-2,n}$ has $|A| \geq 3$.

Also since $r(\delta_{FJK}U_{n-2,n}) = 2$, all sets of cardinality greater than 2 are dependent. Therefore $\delta_{FJK}U_{n-2,n} = U_{2,n} = U^*_{n-2,n}$. □

For a comparison of the definitions, the combinatorial derived matroid is not necessarily the same matroid as the Oxley-Wang derived matroid. Proposition 4.51 will show that for a certain class of matroids it is generic, and the next example shows one possibility of how they differ.

Example 4.18. *Consider the matroid M that is the graphical matroid of* $\mathrm{Sh}(4)$*, see Figure 5. The following matrix is a representation of this matroid over $\mathbb{F}_2$.*

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

This matroid has the circuits $\{12, 34, 135, 235, 145, 245, 136, 236, 146, 246, 56\}$*, and we can create an Oxley-Wang derived matroid that is represented by the matrix*

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

We have that both $\delta_{OW}M[A]$ and $\delta_{FJK}M$ are matroids of rank 4 *on* 11 *elements, but they are not the same matroids. There are precisely two sets that are independent in $\delta_{FJK}M$, but dependent in $\delta_{OW}M[A]$: $\{3, 6, 8, 9\}$ and $\{4, 5, 7, 10\}$. Some more differences between these two matroids: $\delta_{FJK}M$ has* 78 1*-circuits, but $\delta_{OW}M[A]$ has* 66 1*-circuits. The circuits of $\delta_{FJK}M$ is listed in Appendix C.*

4.4 Redundancy

This subsection will discuss redundancy of sets of circuits of a matroid.

Definition 4.19. *A set of circuits $A \subseteq \mathcal{C}$ is*

(i) non-redundant if $C \not\subseteq \mathrm{supp}(A \backslash \{C\})$ for all $C \in A$,

(ii) redundant if there exists some $C \in A$ *such that* $C \subseteq \text{supp}(A \backslash \{C\})$,

(iii) completely redundant if $C \subseteq \text{supp}(A \backslash \{C\})$ *for all* $C \in A$.

Example 4.20. *Consider the matroid* $U_{2,5}$ *on the ground set* $\{1, 2, 3, 4, 5\}$. *The circuits of this matroid are all subsets of size* 3. *An example of a non-redundant set of circuits is* $\{123, 124, 135\}$. *We can see that every circuit in this set has a unique element not in any of the other circuits, so this set is non-redundant.*

Now look at the set $\{123, 234, 345\}$. *We have that* $234 \subseteq \text{supp}(\{123, 345\})$, *so this set is redundant, but since* $123 \not\subseteq \text{supp}(\{234, 345\})$ *it is not completely redundant.*

The set $A = \{123, 124, 234\}$ *is a completely redundant set of circuits. This can be seen by observing that every element in* $\text{supp}(A)$ *is in at least two circuits in* A.

Definition 4.21. *A set* $A \subseteq \mathcal{C}$ *is a maximal non-redundant set if* A *is non-redundant, and for all other non-redundant sets* $A' \subseteq \mathcal{C}$ *where* $\text{supp}(A) = \text{supp}(A')$ *we have* $|A'| \leq |A|$.

Proposition 4.22. *If* $A \subseteq \mathcal{C}$ *is non-redundant, then* $S \subseteq A$ *is non-redundant.*

Proof. Assume we have an $S \subseteq A$ that is redundant. Then we have an $C \in S$ such that $C \subseteq \text{supp}(S \backslash \{C\})$, but since $\text{supp}(S \backslash \{C\}) \subseteq \text{supp}(A \backslash \{C\})$, $C \subseteq \text{supp}(A \backslash \{C\})$, a contradiction. □

Proposition 4.23. *If* $A \subseteq \mathcal{C}$ *is a maximal non-redundant set, then* $S \subseteq A$ *is a maximal non-redundant set.*

Proof. Let $A = \{C_1, \ldots, C_n\}$ be in any order. Consider $n(\cup_{i<l} C_i)$ for some $l \leq n$. We have that $n(\cup_{i \leq l} C_i) + n(C_l \cap \cup_{i<l} C_i) \geq n(\cup_{i<l} C_i) + n(C_l)$. But since $C_l \not\subseteq \cup_{i<l} C_i$, we have $n(C_l \cap \cup_{i<l} C_i) = 0$. Therefore $n(\cup_{i \leq l} C_i) \geq n(\cup_{i<l} C_i) + 1$.

Assume that at some step the nullity increases by more than one. But then $n(\text{supp}(A)) > |A|$ contradicting [JV13, Proposition 1]. Therefore the nullity increases by exactly one at each step. Thus for any $S \subseteq A$, $n(\text{supp}(S)) = |S|$, and S has to be a maximal non-redundant set. □

Proposition 4.24. *If* $A \subseteq \mathcal{C}$ *is redundant, then there exists some* $C \in A$ *such that* $n(\text{supp}(A)) = n(\text{supp}(A \backslash \{C\}))$.

Proof. Since A is redundant, there exists a circuit $C \in A$ such that $\text{supp}(A) = \text{supp}(A\backslash\{C\})$. Therefore $n(\text{supp}(A)) = n(\text{supp}(A\backslash\{C\}))$. □

Proposition 4.25. *If $A \subseteq \mathcal{C}$ is non-redundant, then for all $C \in A$ we have that $n(\text{supp}(A)) > n(\text{supp}(A\backslash\{C\}))$.*

Proof. Let $C \in A$ be any element and let $A' = A\backslash\{C\}$. Since A is non-redundant, there exists some element $e \in C$ that are not in any of the other circuits of A. Therefore $e \notin C \cap \text{supp}(A')$, and $C \cap \text{supp}(A') \subsetneq C$. Since the intersection is strictly contained in C, and since C does not contain any other circuit, the intersection has nullity 0. Now, by the supermodularity of the nullity function we get

$$\begin{aligned} n(\text{supp}(A)) + n(C \cap \text{supp}(A')) &\geq n(\text{supp}(A')) + n(C) \\ n(\text{supp}(A)) &\geq n(\text{supp}(A')) + 1 \\ n(\text{supp}(A)) &> n(\text{supp}(A')) \end{aligned}$$

□

Proposition 4.26. *Let $A \subseteq \mathcal{C}$ such that $n(\text{supp}(A)) < |A|$. Then A is redundant.*

Proof. Let $A \subseteq \mathcal{C}$ where $n(\text{supp}(A)) < |A|$. Now for a contradiction, assume that A is non-redundant. By [JV13, Lemma 1] $n(\text{supp}(A)) \geq |A|$, a contradiction. Therefore there must exist a circuit $C \in A$ such that $C \subseteq \text{supp}(A\backslash\{C\})$, and A is redundant. □

Definition 4.27. *A cycle is a set $A \subseteq E$ that is minimal in the set $\{\text{supp}(S) | S \subseteq \mathcal{C}, n(\text{supp}(S)) = n(A)\}$.*

Proposition 4.28. *Let $A' \subseteq A \subseteq E$ be cycles. Then there exists a maximal set of non-redundant circuits $\{C_1, \ldots, C_h\}$ such that $A = C_1 \cup \cdots \cup C_h$ and $A' = C_1 \cup \cdots \cup C_l, l \leq h$, where $n(A) = h$ and $n(A') = l$.*

Proof. Let $I' \subseteq A'$ and $I \subseteq A$ be independent sets of the largest possible cardinality contained in the respective sets. By (I3) we may add items from $I\backslash I'$ to I' to create an independent set B such that $|I| = |B|$. Let $\{e_1, \ldots, e_l\} = A'\backslash I'$ and $\{e_{l+1}, \ldots, e_h\} = A\backslash\{B \cup A'\}$. Then let $\{C_i \in \mathcal{C} : C_i \subseteq B \cup \{e_i\}, 1 \leq i \leq h\}$.

Since every C_i contains an e_i that is not contained in any other C_j, this set is non-redundant. This set has cardinality h, so it is maximal.

Now we need to show that $C_i \subseteq A'$ for $i \leq l$. Let $i \leq l$. Observe that $n(I' \cup \{e_i\}) = 1$ so it contains a single circuit. Since $I' \cup \{e_i\} \subseteq B \cup \{e_i\}$, we must have that $C_i \subseteq I' \cup \{e_i\}$ and thus $C_i \subseteq A'$. □

4.5 Fast matroids

In this section, a new class of matroids is introduced. These have a specific property that is used in a proof later. The name comes from the fact that their combinatorial derived matroids are faster to compute since their computation do not need certain operations of quite high complexity.

Definition 4.29. *Let M be a connected matroid. M as a* fast matroid *if and only if it satisfies the following property:*

- *For all non-empty $S \subseteq \mathcal{C}(M)$ and $C \in \mathcal{C}(M)$, then if there exists a non-empty $A \subseteq S$ such that $A \cup \{C\}$ is a maximal non-redundant set, then $n(\text{supp}(S) \cup C) \leq n(\text{supp}(S)) + 1$.*

In general we define recursively:

Definition 4.30. *A matroid $M = M_1 \oplus M_2$ is a fast matroid if M_1 and M_2 are fast matroids.*

There is a necessity to specifically define the property to only be on connected matroids, and have sums of fast matroids be fast matroid as well. Example 4.33 may illuminate why the single property of Definition 4.29 alone might break down when dealing with non-connected matroids.

Proposition 4.31. *Any matroid M where $n(M) \leq 3$ is a fast matroid.*

Proof. If the matroid has nullity 0, then there are are no non-empty subsets of $\mathcal{C}(M)$, so the property holds for all of them.

If $n(M) = 1$, then $\mathcal{C} = \{C'\}$. Let $S = A = \{C'\}, C = C'$. We have that $A \neq \emptyset, A \cup \{C\} = \{C'\}$ is a maximal non-redundant set, and the property is clear.

Since the matroid has nullity 1, it contains only one circuit, and the only possible situation is the one outlined above, since neither S nor A may be empty.

Otherwise $2 \leq n(M) \leq 3$, let $S \subseteq \mathcal{C}(M)$ be any non-empty set, and let C be any circuit. Assume that $\emptyset \subsetneq A \subseteq S$ is such that $A \cup \{C\}$ is a maximal non-redundant set. If $n(M) - 1 \leq n(\text{supp}(S)) \leq n(M)$, then the addition of another circuit can only increase the nullity by at most 1. Otherwise we have that $n(\text{supp}(S)) = n(M) - 2$. But then $|S| = |A| = 1$, so therefore $S \cup \{C\}$ is a maximal non-redundant set, and $n(\text{supp}(S) \cup C) \leq n(\text{supp}(S)) + 1$.

□

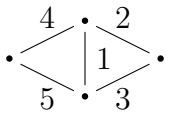
Proposition 4.32. *$U_{k,n}$ is a fast matroid.*

Proof. If $k \geq n - 3$, use the previous proposition.

Let $S \subseteq \mathcal{C}$ be any non-empty set of circuits, $C \in \mathcal{C}$ and assume that there exists a non-empty $A \subseteq S$ such that $A \cup \{C\}$ is a maximal non-redundant set. Then by Proposition 4.23 we have that A is a maximal non-redundant set. Since the matroid is uniform, and since the two sets are maximal non-redundant sets, $C \setminus \text{supp}(A) = \{e\}$. Therefore $C \setminus \text{supp}(S) \subseteq \{e\}$, and since the addition of C to S adds at most one element to the support, the nullity increases by at most one. □

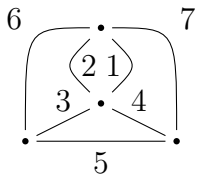
Example 4.33. *Let $M = U_{2,3} \oplus U_{2,6}$. We have the elements $E = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$, and let $\{1, 2, 3\}$ be the elements from the $U_{2,3}$ component of the matroid. Now consider $A = \{123\}$, $S = \{123, 456\}$ and $C = 789$. We can see that these sets and circuits satisfies the conditions to the property in Definition 4.29, but observe that $n(\text{supp}(S) \cup C) = 5$, while $n(\text{supp}(S)) = 2$, so this matroid does not have the property in Definition 4.29.*

Example 4.34. *An example of a fast matroid is the following graphical matroid.*



We have the circuits $\{C_1, C_2, C_3\} = \{123, 145, 2345\}$. Any subset of cardinality at most 2 of these circuits is a maximal non-redundant set. It is clear that if we add any circuit to a maximal non-redundant set in this matroid, the nullity increases by at most one, since the nullity of the matroid is 2.

Example 4.35. *An example of a matroid that is not a fast matroid is the following graphical matroid.*



Let $S = \{345, 236\}$*,* $C = 147$ *and* $A = \{345\}$*. We have that* $A \cup \{C\}$ *is a maximal non-redundant set, but* $n(\text{supp}(S) \cup C) = 4 > n(\text{supp}(S)) + 1 = 2 + 1 = 3$

This example may be expanded to a simple matroid, by adding vertices on 1 *and* 7*, and an edge between these two vertices. Observe also that if we contract by* 5*, then we get* Sh(4) *from Figure 5.*

Proposition 4.36. *Let* M *be a fast matroid. Then for all* $X \subseteq E(M)$*,* $M' = M \backslash X$ *is a fast matroid.*

Proof. Let $S \subseteq \mathcal{C}(M')$, $C \in \mathcal{C}(M')$ and $A \subseteq S$ such that $A \cup \{C\}$ is a maximal non-redundant set. Let ϕ be the injection from Proposition 4.12. Since M' is a deletion, ϕ preserves the nullity. We have that $\phi(A) \subseteq \phi(S)$, and since $A \cup \{C\}$ is a maximal non-redundant set,

$$|A \cup \{C\}| = n_{M'}(\text{supp}(A \cup \{C\})) = n_M(\text{supp}(\phi(A) \cup \phi(\{C\}))) = |\phi(A) \cup \phi(\{C\})|,$$

so $\phi(A) \cup \phi(\{C\})$ is a maximal non-redundant set in M. Therefore since M is a fast matroid,

$$\begin{aligned} n_{M'}(\text{supp}(S \cup \{C\})) &= n_M(\text{supp}(\phi(S) \cup \phi(\{C\}))) \\ &\leq n_M(\text{supp}(\phi(S))) + 1 \\ &= n_{M'}(\text{supp}(S)) + 1 \end{aligned}$$

so M' is a fast matroid. □

The class of fast matroids is not closed under contractions or duals however. See in Figure 5, where the matroid on the left, $M(\text{Sh}(4))$, is not a fast matroid and contracted from the one on the right, which is a fast matroid. If we

look at $M(\mathrm{Sh}(4))^*$, this matroid has nullity 2 so it is a fast matroid, but again $(M(\mathrm{Sh}(4))^*)^* = M(\mathrm{Sh}(4))$ is not a fast matroid.

Proposition 4.37. *Let M be a matroid, and $|E(M)| < 6$. Then M is a fast matroid. Further, $M(\mathrm{Sh}(4))$ is a non-fast matroid where $|E(M(\mathrm{Sh}(4)))| = 6$.*

Proof. First to show that $M(\mathrm{Sh}(4))$ is not a fast matroid. Let $S = \{12, 34\}$, $A = \{12\}$, and $C = 56$. We have that $A \cup \{C\}$ is a maximal non-redundant set, but $n(\mathrm{supp}(S)) = 2$ and $n(\mathrm{supp}(S \cup \{C\})) = 4$, so $M(\mathrm{Sh}(4))$ is not a fast matroid.

If we want to try to find a smaller non-fast matroid M, we need a matroid of nullity at least 4. If this matroid is on 4 elements, it has rank 0, and has to be $U_{0,4}$, which is a fast matroid.

If it is on 5 elements, it has rank 1. If this matroid is not connected, one of its components has fewer than 5 elements, so the matroid has to be connected. We therefore need that for every pair $e, f \in E(M)$, there is a circuit C such that $e, f \in C$. But since M is of rank 1, this means that $\{e, f\}$ is a circuit in M for all distinct $e, f \in E(M)$. Therefore $M = U_{1,5}$, a fast matroid.

Thus the smallest possible non-fast matroid is on 6 elements and has nullity 4, which $M(\mathrm{Sh}(4))$ is. □

4.6 Combinatorial derived matroids of fast matroids

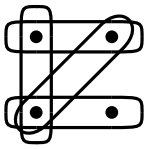
The class of fast matroids are constructed such that they do not need a certain step in the computation of the combinatorial derived matroid, the repeated iterations of ϵ to get the dependent sets. Without this step, they are both easier to compute, and it is easier to prove their rank. The key result concerning their construction will be Theorem 4.47 below. Freij-Hollanti, Jurrius, and Kuznetsova [FJK23] showed that the upper boundary of the rank of a combinatorial derived matroid $\delta_{FJK}M$ of a matroid M is $|E(M)| - r(M)$. For fast matroids, Theorem 4.46 will show that the rank of the derived matroid is exactly the corank. We first give the helpful results 4.38-4.43 regarding some properties of $\mathcal{A}_0$, valid for all matroids M.

Proposition 4.38. *If $A \in \min \mathcal{A}_0$, then $n(\mathrm{supp}(A)) = |A| - 1$.*

Proof. Let $A \in \min \mathcal{A}_0$. We know that $|A| > n(\mathrm{supp}(A))$. Assume $|A| > n(\mathrm{supp}(A)) + 1$. By Proposition 4.26 and Proposition 4.24 we may find an $C' \in$

A such that for $A' = A\backslash\{C'\}$ we have $n(\text{supp}(A')) = n(\text{supp}(A))$. But then $|A'| = |A| - 1 > n(\text{supp}(A)) + 1 - 1 = n(\text{supp}(A'))$, so $A' \in \mathcal{A}_0$, contradicting the minimality of A. Therefore we must have $|A| = n(\text{supp}(A)) + 1$ □

Note. *The converse is not true, consider the circuits* $\{12, 23, 13, 34\}$ *in* $U_{1,4}$.



The union of this set has nullity 3*, so the set satisfies the above constants. But it contains the subset* $\{12, 23, 13\}$ *which is also in* $\mathcal{A}_0$*, so the first set is not minimal.*

Proposition 4.39. *If* $M = M_1 \oplus M_2$ *and* $A \in \min \mathcal{A}_0$*, then either* $A \subseteq \mathcal{C}(M_1)$ *or* $A \subseteq \mathcal{C}(M_2)$*.*

Proof. Let $A \in \min \mathcal{A}_0$, and assume that $A \cap \mathcal{C}(M_i) \neq \emptyset$ for both $i = 1, 2$. Since A is minimal in $\mathcal{A}_0$, we know that $|S| \leq n(\text{supp}(S))$ for all proper subsets S of A. We can also split A into two sets A_1, A_2 such that $A_i \subseteq \mathcal{C}(M_i)$ such that $A = A_1 \cup A_2$. From Proposition 4.38 we know that $n(\text{supp}(A)) = |A| - 1$, so we therefore have that $|A_1| + |A_2| - 1 = n(\text{supp}(A_1)) + n(\text{supp}(A_2))$. But since all proper subsets of A have nullity at least the cardinality of the subset, we get the inequality

$$|A_1| + |A_2| \leq n(\text{supp}(A_1)) + n(\text{supp}(A_2)) = |A_1| + |A_2| - 1$$

which is absurd. Therefore the assumption is wrong, and we must have that $A \cap \mathcal{C}(M_i) = \emptyset$ for some i. Since A is not empty, we must have that $A \subseteq \mathcal{C}(M_i)$ for either $i = 1$ or $i = 2$. □

Corollary 4.39.1. *If* $A \in \min \mathcal{A}_0$*, then* $A \subseteq \mathcal{C}(M')$ *where* M' *is a connected component of* M*.*

Proposition 4.40. *If* $A \in \min \mathcal{A}_0$*, then* $n(\text{supp}(A\backslash\{C\})) = n(\text{supp}(A))$ *for all* $C \in A$*.*

Proof. Assume the statement is false, so we have $C \in A$ such that $n(\text{supp}(A\backslash\{C\})) < n(\text{supp}(A)) = |A| - 1 = |A\backslash\{C\}|$, so $A\backslash\{C\} \in \mathcal{A}_0$, contradicting the minimality of A. □

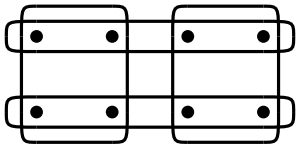
Proposition 4.41. *If $A \in \min \mathcal{A}_0$, then A is completely redundant.*

Proof. Let $C \in A$. By Proposition 4.40 we have that $n(\text{supp}(A)) = n(\text{supp}(A\backslash\{C\}))$. By the supermodularity of the nullity function, we have that

$$\begin{aligned} n(\text{supp}(A)) + n(C \cap \text{supp}(A\backslash\{C\})) &\geq n(\text{supp}(A\backslash\{C\})) + n(C) \\ n(\text{supp}(A)) + n(C \cap \text{supp}(A\backslash\{C\})) &\geq n(\text{supp}(A)) + n(C) \\ n(C \cap \text{supp}(A\backslash\{C\})) &\geq 1 \end{aligned}$$

which means that $C \cap \text{supp}(A\backslash\{C\})$ contains a 0-circuit, and the only possibility for this is C. Since C in a subset of the intersection, $C \subseteq \text{supp}(A\backslash\{C\})$. □

Example 4.42. *The converse is not true, look at the circuits* $\{1234, 5678, 1256, 3478\}$ *in* $U_{3,8}$.



We see that this set is completely redundant, i.e. each of the circuits are contained in the union of the other, but the nullity of their union is 5*, so the set is not in* $\mathcal{A}_0$.

Proposition 4.43. *If $A \in \mathcal{A}$ and $|A| = 3$, then $A \in \min \mathcal{A}_0$.*

Proof. We have that there are no elements of cardinality less than 3 in $\mathcal{A}$. This means that any possible element of $\mathcal{A}$ of cardinality 3 that are not in $\mathcal{A}_0$ must be the result of the ϵ operation. But consider two elements A_1 and A_2 of $\mathcal{A}_0$ of cardinality 3. If these were to combine to an element of cardinality 3, then their intersection must have cardinality 2. Let $A_1 = \{C, C_1, C_2\}$ and $A_2 = \{C', C_1, C_2\}$. We can see that $C \subseteq \text{supp}(C_1 \cup C_2)$ and $C' \subseteq \text{supp}(C_1 \cup C_2)$ by Proposition 4.41, and that $n(\text{supp}(C_1 \cup C_2))) = 2$ by Proposition 4.38. Therefore $\text{supp}(\{C, C', C_1\}) \subseteq \text{supp}(C_1, C_2)$ and $\text{supp}(\{C, C', C_2\}) \subseteq \text{supp}(C_1, C_2)$, so both possible combinations of these two sets are elements of $\mathcal{A}_0$. It is therefore not possible to combine 3-element sets of $\mathcal{A}_0$ to form a 3-element set that is not in $\mathcal{A}_0$, and all sets of

cardinality 3 in $\mathcal{A}$ must be elements in $\mathcal{A}_0$. They must also be minimal since $\mathcal{A}_0$ does not contain any elements of cardinality less than 3. □

Proposition 4.44. *If M is a fast matroid and $A \in \min \mathcal{A}_1$, then $A \in \min \mathcal{A}_0$.*

Proof. Let $A \in \min \mathcal{A}_1$. Either $A \in \min \mathcal{A}_0$ and we are done, or we have $A_1, A_2 \in \min \mathcal{A}_0$ such that $A = A_1 \cup A_2 \backslash \{C\}$ for some $C \in A_1 \cap A_2$ by [FJK23, Lemma 18].

Note that from Corollary 4.39.1 we know that A_1 and A_2 are contained in one component of the matroid each. Since we also have that $A_1 \cap A_2 \neq \emptyset$, we also must have that they both are in the same component.

Let $S = \text{supp}(A)$, $S_i = \text{supp}(A_i)$ and $S_3 = \text{supp}(A_1 \cap A_2)$. Let $\mathbf{C}_1$ be a maximal set of non-redundant 0-circuits constructed as in Proposition 4.28 with respect to $S_3 \subseteq S_1$, and likewise for $\mathbf{C}_2$ with respect to $S_3 \subseteq S_2$. Let $\mathbf{C}_3 = \mathbf{C}_1 \cap \mathbf{C}_2$. In the proof of Proposition 4.28, observe that it is possible to choose $I' \subseteq S_3$ such that $\mathbf{C}_1$ and $\mathbf{C}_2$ overlap in the first $n(S_3)$ circuits.

Take $\mathbf{C}_1$ and add 0-circuits from $\mathbf{C}_2 \backslash \mathbf{C}_3$ one by one. If we have added j circuits from $\mathbf{C}_2 \backslash \mathbf{C}_3$ we have the following situation (j may be 0). We have the set $\mathbf{C}_1 \cup \{C_1, \dots, C_j\}$ where $C_i \in \mathbf{C}_2 \backslash \mathbf{C}_3$, and wish to add $C_{j+1} \in \mathbf{C}_2 \backslash \mathbf{C}_3$ to it. But $\mathbf{C}_3 \cup \{C_1, \dots, C_{j+1}\} \subseteq \mathbf{C}_2$, so by Proposition 4.23 it is a maximal non-redundant set. This, in addition to the sets being contained in one connected component of the matroid and the recursiveness of the definition of fast matroids, we may use the property of the fast matroid that $n(\text{supp}(\mathbf{C}_1) \cup C_1 \cup \dots \cup C_{j+1}) \leq n(\text{supp}(\mathbf{C}_1) \cup C_1 \cup \dots \cup C_j) + 1$. Since the nullity increases by at most one for each new circuit, we get that $n(S) \leq |\mathbf{C}_1| + |\mathbf{C}_2| - |\mathbf{C}_3|$. We know that $|\mathbf{C}_1| = |A_1| - 1$ and $|\mathbf{C}_2| = |A_2| - 1$. In addition, since $A_1 \cap A_2 \notin \mathcal{A}_0$, then $|A_1 \cap A_2| \leq n(\text{supp}(A_1 \cap A_2)) = |\mathbf{C}_3| \Leftrightarrow -|\mathbf{C}_3| \leq -|A_1 \cap A_2|$. Therefore

$$\begin{aligned} n(S) &\leq |\mathbf{C}_1| + |\mathbf{C}_2| - |\mathbf{C}_3| \\ &\leq |A_1| - 1 + |A_2| - 1 - |A_1 \cap A_2| \\ &< |A_1 \backslash \{C\}| + |A_2 \backslash \{C\}| - |A_1 \cap A_2| + 1 \\ &= |A_1 \backslash \{C\}| + |A_2 \backslash \{C\}| - |A_1 \cap A_2 \backslash \{C\}| \\ &= |A| \end{aligned}$$

Thus $n(S) = n(\text{supp}(A)) < |A|$, so $A \in \mathcal{A}_0$. Since $\mathcal{A}_0 \subseteq \mathcal{A}_1$, we must have that the

inclusion minimal elements in $\mathcal{A}_1$ that are in A_0 must also be inclusion minimal in A_0. Therefore $A \in \min \mathcal{A}_0$. □

Note. *An easier version of this proof for only uniform matroids are in Proposition A.1.*

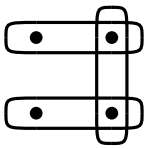
Corollary 4.44.1. *If M is a fast matroid and $A \in \mathcal{C}(\delta_{FJK}M)$, then $A \in \min \mathcal{A}_0$.*

Proof. Consider [FJK23, Proposition 20]. Here they construct the 1-circuits of $\delta_{FJK}M$. Proposition 4.44 shows that the sequence terminates at the first step, and hence the result follows. □

Corollary 4.44.2. *If M is a fast matroid and $A \subseteq E(\delta_{FJK}M)$ is non-redundant, then $A \in \mathcal{I}(\delta_{FJK}M)$.*

Proof. For a contradiction, assume that we have $C \subseteq A$ such that C is a 1-circuit. Then we have that $C \in \min \mathcal{A}_0(\delta_{FJK}M)$. By 4.41, we have that C is completely redundant. But then $C \subseteq A$, so A is redundant, a contradiction. □

Note. *The converse is not true, consider the set of 0-circuits $A = \{12, 24, 34\}$ in $U_{1,4}$.*



This is redundant, since $24 \subseteq 12 \cup 34$, but this has that $n(\mathrm{supp}(S)) \geq |S|$ for all subsets $S \subseteq A$, so it is independent.

Corollary 4.44.3. *If M is a fast matroid and $A \in \mathcal{C}(\delta_{FJK}M)$, then $n(\mathrm{supp}(A)) = |A| - 1$.*

Proof. Follows from Corollary 4.44.1 and Proposition 4.38. □

Example 4.45. *There are non-fast matroids where Proposition 4.44 does not hold, such as $M(\mathrm{Sh}(4))$, see Figure 5. Consider the 1-circuits $A_1 = \{34, 135, 145\}$, $A_2 = \{34, 246, 236\}$ and $A = A_1 \cup A_2 \backslash \{34\} = \{135, 145, 246, 236\}$. Observe that $A_1, A_2 \in \min \mathcal{A}_0$, and $A \in \mathcal{A}_1$. We can see that the support of A is all the elements,*

so their nullity is 4*, and therefore* $A \notin \mathcal{A}_0$*. Moreover, since* A *is completely redundant, all three element subsets of* A *also have a support of nullity* 4*, and are thus not elements in* $\min \mathcal{A}_0$*. Also by Proposition 4.43, none of these three element subsets of* A *are in* $\min \mathcal{A}_1 \setminus \min \mathcal{A}_0$*. This means that* $A \in \min \mathcal{A}_1$*, but* $A \notin \mathcal{A}_0$*.*

We now give a main result of this thesis:

Theorem 4.46. *If* M *is a fast matroid, then* $\delta_{FJK}M$ *is a matroid of rank* $|E(M)| - r(M)$*.*

Proof. Let B be a basis of M. Now let $C = \{C_e \subseteq B \cup \{e\} | e \in E(M) \setminus B\}$ be a set of fundamental circuits. We see that each C_e contains a unique element e, so C is non-redundant. By Corollary 4.44.2, we have that C is independent in $\delta_{FJK}M$. Since $|C| = |E(M) \setminus B| = |E(M)| - |B| = |E(M)| - r(M)$, the rank of $\delta(M)$ is at least $E(M) - r(M)$. By [FJK23, Lemma 37] we have that the rank of $\delta(M)$ is at most $E(M) - r(M)$, and the result follows. □

Theorem 4.47. *If* M *is a fast matroid, then* $\delta_{FJK}M$ *has dependent sets* $\uparrow \mathcal{A}_0$*.*

Proof. We know that all 1-circuits are the elements of $\min \mathcal{A}_0$, and every dependent set in $\delta_{FJK}M$ contains a 1-circuit. Therefore, $\uparrow \mathcal{A}_0$ is the set of dependent sets in $\delta_{FJK}M$. □

Example 4.48. *Consider the matroid* $\delta_{FJK}M$ *as described in Appendix C. Here,* M *is not a fast matroid. Six of it's* 1*-circuits are not in* $\mathcal{A}_0$*. These are:*

$$\{efgh, dfgi, dehi, cfgj, cehj, cdij\},$$

where all of them have nullity 4*.*

From these results we get complete descriptions of independent sets and bases of $\delta_{FJK}M$ if M is a fast matroid.

$$\mathcal{I} = \{I \subseteq \mathcal{C} : \forall S \subseteq I, n(\text{supp}(S)) \geq |S|\}, \tag{4.49}$$

$$\mathcal{B} = \{B \subseteq \mathcal{C} : |B| = r^*(M), \forall S \subseteq B, n(\text{supp}(S)) \geq |S|\} \tag{4.50}$$

We can also prove a small generalization of [FJK23, Lemma 40].

Proposition 4.51. *If M is a fast matroid, then all 1-circuits of $\delta_{FJK}M$ are dependent in $\delta_{OW}M_Q$ for every representation Q of M.*

Proof. This proof is an adapted version of [FJK23, Lemma 40]. Let A be a 1-circuit of $\delta_{FJK}M$. For a representation Q of M and $C \in A$, denote by $\mathbf{q}_C$ the circuit vector supported on C. Since A is a 1-circuit and from Equation (3.20), we have that

$$|A| > n(\operatorname{supp} A) = \dim(Q^{\perp}(\operatorname{supp} A)) \geq \dim \operatorname{span}\{\mathbf{q}_C | C \in A\}.$$

Thus the vectors $\{\mathbf{q}_C | C \in A\}$ are linearly dependent, so A is dependent in $\delta_{OW}Q$. □

Proposition 4.52. *$\delta_{FJK}M$ has a dependent set of cardinality 3 if and only if $U_{1,3}$ is a minor of M.*

Proof. Assume M has $U_{1,3}$ as a minor. Then the result follows from Proposition 4.16, since $\delta_{FJK}U_{1,3}$ contains a dependent set of cardinality 3.

Assume $\delta_{FJK}M$ has a dependent set $A = \{C_1, C_2, C_3\}$. Let $E_{i,j} = C_i \cap C_j$. Note that $E_{i,j} \neq \emptyset$. For each $E_{i,j}, i < j$, choose an $e_{i,j} \in E_{i,j}$. Now let

$$M' = M \backslash (E(M) \backslash \operatorname{supp}(A)) / (\operatorname{supp}(A) \backslash \{e_{1,2}, e_{1,3}, e_{2,3}\}).$$

To get M', all elements not in $\operatorname{supp}(A)$ are deleted, and contracted to only contain the necessary elements of the 0-circuits of A. We have that $E(M') = \{e_{1,2}, e_{1,3}, e_{2,3}\}$, where every 2 element subset is dependent, but all single element subsets are independent. Thus $M' = U_{1,3}$. □

Proposition 4.53. *$\delta_{FJK}U_{k,n}$ has $\binom{n}{k+2}\binom{k+2}{3}$ triangles when $1 \leq k \leq n-2$.*

Proof. To find 1-circuits of cardinality 3, by Corollary 4.44.3 we only need to look at sets $S \subseteq E$ where $n(S) = 2$. There are $\binom{n}{k+2}$ such sets. Let S be such a set. If we remove any element from S it becomes a 0-circuit, so there are $k+2$ 0-circuits that are a subset of S. If we pick any three of them, we get a 1-circuit. There are $\binom{k+2}{3}$ ways of choosing these three 0-circuits. Thus there are $\binom{n}{k+2}\binom{k+2}{3}$ 1-circuits of cardinality 3 in $\delta_{FJK}U_{k,n}$. □

4.7 Extending the definition to a finite graded lattice

A lattice is a poset where every pair of elements x, y have a least upper bound called the join $x \vee y$ and a greatest lower bound called the meet $x \wedge y$. For a lattice, we say that an element x covers another element y if $x > y$ and there are no element $z \notin \{x, y\}$ such that $x > z > y$. The cover of a minimal element in the lattice is called an atom, and a lattice is atomistic if every element is the join of some set of atoms. The lattice is graded if there is a rank function r such that $r(x) > r(y)$ whenever $x > y$ and $r(x) = r(y) + 1$ if x covers y. We may assume that the rank of the bottom element (the meet of the atoms) is zero. If this rank function is submodular, meaning that the identity $r(x \vee y) + r(x \wedge y) \leq r(x) + r(y)$ holds, in addition to being atomic and finite, then the lattice is a geometric lattice. A geometric lattice can also be defined by having it to be semimodular instead of submodular, but for finite lattices this is the same [Grä78, p. 173, Theorem 2].

The reason geometric lattices are interesting, is that there is a one-to-one correspondence between geometric lattices and simple matroids. We may have the geometric lattice be the lattice of flats of a matroid (having the atoms as the ground set), yielding a simple matroid. For the other way, given a matroid the lattice of flats for that matroid is a geometric lattice. The lattice of cycles of a matroid is the opposite of the lattice of flats of the dual matroid, it is turned upside down. This lattice is not geometric, since the rank function for this lattice (the nullity function of the matroid) is supermodular, not submodular.

We want to construct a matroid from this lattice of cycles in a way that yields the same matroid as the combinatorial derived matroid. It turns out that the rank function of the lattice does not need to be either supermodular, nor submodular, but simply graded. The lattice does not have to be atomistic either, but the matroid we will construct will use the atoms of the lattice as a ground set and some properties of their join, so any element in the lattice that is not the join of atoms are ignored.

Let L be a finite graded lattice where the rank of the bottom element is zero, and $A(L)$ be the atoms of this lattice. We want to define two functions from the

set of subsets of atoms of the lattice (where $\mathcal{P}(L)$ denotes the powerset of L):

$$\begin{aligned}
\epsilon : \mathcal{P}(\mathcal{P}(L)) &\to \mathcal{P}(\mathcal{P}(L)) \\
\mathcal{D} &\mapsto \mathcal{D} \cup \{D_1 \cup D_2 \backslash \{A\} : D_1, D_2 \in \mathcal{D}, D_1 \cap D_2 \notin \mathcal{D}, A \in D_1 \cap D_2\} \\
\uparrow : \mathcal{P}(\mathcal{P}(L)) &\to \mathcal{P}(\mathcal{P}(L)) \\
\mathcal{D} &\mapsto \{X \subseteq A(L) : \exists D \in \mathcal{D}, D \subseteq X\}
\end{aligned}$$

Define $\mathcal{D}_0$ to be the set $\{D \subseteq \mathcal{P}(A(L)) : r(\vee_{A \in D} A) < |D|\}$. Now define D_i iteratively as

$$\mathcal{D}_{i+1} = \uparrow \epsilon(\mathcal{D}_i).$$

Note that for all i, we have that $\mathcal{D}_i \subseteq \mathcal{D}_{i+1}$. Since the lattice is finite, this process must terminate and let $\mathcal{D} = \mathcal{D}_n$ be the final iteration.

Lemma 4.54. *Let $D \in \mathcal{D}_{i+1}$. Then there is a $D' \in \mathcal{D}_i$ such that $|D'| \leq |D|$.*

Proof. Proof from [FJK23, Lemma 16]. This is clear if $D \in \mathcal{D}_i$, so assume it is not. Since the inclusion minimal sets in $\mathcal{D}_{i+1}$ are contained in $\epsilon(\mathcal{D}_i)$, we may assume that $D \in \epsilon(\mathcal{D}_i) \backslash \mathcal{D}_i$. Thus, there exists $D_1, D_2 \in \mathcal{D}_i$ such that $D = D_1 \cup D_2 \backslash \{A\}$ for some $A \in D_1 \cap D_2$ where $D_1 \cap D_2 \notin \mathcal{D}_i$. Since $D_1 \in \mathcal{D}_i$ and $D_1 \cap D_2 \notin \mathcal{D}_i$, then $D_1 \not\subseteq D_2$. We therefore have that $|D_1| \leq |D_1 \cup D_2| - 1 = |D|$, and the lemma holds with $D' = D_1$. □

Proposition 4.55. *For any finite graded lattice L, the collection $\mathcal{D}$ is the collection of dependent sets of some matroid on the ground set $A(L)$.*

Proof.

1. Since $|\emptyset| = 0$ and that the rank function is non-negative, $\emptyset \notin \mathcal{D}_0$. By Lemma 4.54, we inductively have that $\emptyset \notin \mathcal{D}_i$ for all $i \geq 0$, so in particular $\emptyset \notin \mathcal{D}_n = \mathcal{D}$.

2. If $D_1 \in \mathcal{D}$ then there exists some minimal i such that $D_1 \in \mathcal{D}_{i+1} \backslash D_i$. Then for all $D_2 \subseteq A(L)$ such that $D_1 \subseteq D_2$, $D_2 \in \mathcal{D}_{i+2}$ and $\mathcal{D}_{i+2} \subseteq \mathcal{D}$, so $D_2 \in \mathcal{D}$.

3. Let D_1 and D_2 be two distinct sets in $\mathcal{D}$. If for some i, $D_1 \cap D_2 \in \mathcal{D}_i$, then $D_1 \cap D_2 \in \mathcal{D}$ and there is nothing to check. Otherwise, $D_1 \cap D_2 \notin \mathcal{D}$ and there exists some minimal i such that $D_1, D_2 \in \mathcal{D}_i$. Therefore for all $A \in D_1 \cap D_2, (D_1 \cup D_2) \backslash \{A\} \in \mathcal{D}_{i+1} \subseteq \mathcal{D}$.

□

Now, we may define the derived matroid of a matroid to be the derived matroid of the lattice of the cycles of the matroid, where the rank function of the lattice is the nullity function of the matroid. We can note this matroid as $\delta\mathcal{L}(\mathcal{C}(M))$ for a matroid M.

Proposition 4.56. *For a given matroid M, the matroids $\delta_{FJK}M$ and $\delta\mathcal{L}(\mathcal{C}(M))$ are isomorphic.*

Proof. We have that the ground sets of the two matroids are the same, since the circuits M is precisely the atoms of the cycle lattice of the matroid. Since the join of the atoms is the same as the union of the circuits, and that the rank function of the lattice is the nullity function of the matroid, the first iterations of the dependent sets in either cases are the same sets. Further, ϵ and $\uparrow$ are purely set-theoretic functions that does not use any specific information of the underlying objects. Therefore the final iterations of the dependent sets are the same. To find an isomorphism, it is just to take the bijection between the circuits and the atoms of the cycle lattice. A bijection between the dependent sets of the two matroid can be found by using the previous bijection pointwise on the dependent sets. □

The matroid of any such lattice still has properties that the combinatorial derived matroid has, such as being simple. To show this, we need the following lemma.

Lemma 4.57. *For any set of sets $\mathcal{D}$,*

$$\min\{|D||D \in \mathcal{D}\} = \min\{|D||D \in \epsilon(\mathcal{D})\}$$

Proof. Let D be of minimal cardinality in $\epsilon(\mathcal{D})$. If $D \in \mathcal{D}$, we are done. Otherwise we have $D_1, D_2 \in \mathcal{D}$ such that $D = D_1 \cup D_2 \backslash A$ for some $A \in D_1 \cap D_2$ and $D_1 \cap D_2 \notin \mathcal{D}$. We also have that neither D_1 nor D_2 are empty, since if they were their intersection would also be empty and an element of $\mathcal{D}$. Thus

$$|D| = |D_1| + |D_2| - |D_1 \cap D_2| - 1$$

Assume WLOG $|D| < |D_1|$. Then

$$\begin{aligned} |D_1| > |D| &= |D_1| + |D_2| - |D_1 \cap D_2| - 1 \\ &\Downarrow \\ |D_1 \cap D_2| + 1 &> |D_2| \end{aligned}$$

The only possibility for this is if $D_1 \cap D_2 = D_2$, but this is impossible, since the intersection cannot be an element of $\mathcal{D}$. Therefore $|D| \geq |D_1|$ and $|D| \geq |D_2|$. Therefore $\min\{|D||D \in \mathcal{D}\} \leq \min\{|D||D \in \epsilon(\mathcal{D})\}$.

We also have that $\mathcal{D} \subseteq \epsilon(\mathcal{D})$, so $\min\{|D||D \in \mathcal{D}\} \geq \min\{|D||D \in \epsilon(\mathcal{D})\}$, and they have to be equal. □

Proposition 4.58. *Let L be a finite graded lattice. Then the matroid δL is a simple matroid.*

Proof. The empty set is not in $\mathcal{D}_0$, since the rank would not be strictly less than the cardinality. If $D \in \mathcal{D}_0$ is a set of cardinality 1, then it would contain one atom and the rank would be 1, again not possible.

Let $D \subseteq A(L)$ be a set with cardinality 2. The join of the two atoms is not an atom, and since the rank function is graded the join has rank at least one more than the atoms. Thus $r(\vee_{A \in D} A) \geq 2 = |D|$, so $D \notin \mathcal{D}_0$.

Therefore $\mathcal{D}_0$ has no sets of cardinality less than 3, and by Lemma 4.57 the minimal dependent sets of δL are of cardinality at least 3. □

We can also for this matroid set an upper boundary on the rank.

Proposition 4.59. *Let L be a finite graded lattice. Then the rank of δL is at most the rank of L.*

Proof. Let $D \subseteq A(L)$ be any set of atoms such that $|D|$ is greater than the rank of the lattice. We then have that $|D| > r(L) \geq r(\vee_{A \in D} A)$, so $D \in \mathcal{D}_0$, and is dependent in δL. □

4.8 Derived matroid of q-matroids

$\mathcal{E}$ denotes an n-dimensional vector space over a field $\mathbb{F}$. Furthermore $\mathcal{L}(\mathcal{E})$ denotes the lattice of subspaces of $\mathcal{E}$, where the meet of two subspaces is their sum, and

the join is the intersection. For any $A, B \in \mathcal{L}(\mathcal{E})$ with $A \subseteq B$, let $[A, B]$ be the interval between the two subspaces, in particular that is the sublattice of all subspaces $X \subseteq \mathcal{E}$ such that $A \subseteq X \subseteq B$. For $A \subseteq \mathcal{E}$, let the lattice $\mathcal{L}(A)$ be the interval $[\{0\}, A]$.

First we need definitions of the q-matroids, the following is from Byrne, Ceria, and Jurrius [BCJ22].

Definition 4.60. *A q-matroid $\mathcal{M}$ is a pair $(\mathcal{E}, \rho)$ where ρ is an integer-valued function defined on the subspaces of $\mathcal{E}$ with the following properties:*

(R1) For every subspace $A \in \mathcal{L}(\mathcal{E})$, $0 \leq \rho(A) \leq \dim A$.

(R2) For all subspaces $A \subseteq B \in \mathcal{L}(\mathcal{E})$, $\rho(A) \leq \rho(B)$.

(R3) For all A, B, $\rho(A + B) + \rho(A \cap B) \leq \rho(A) + \rho(B)$.

Now we can define a flat for a q-matroid using the rank.

Definition 4.61. *Let $\mathcal{M} = (\mathcal{E}, \rho)$ be a q-matroid. A subspace F of $\mathcal{E}$ is a flat if for all one-dimensional subspaces x such that $x \not\subseteq F$ we have that*

$$\rho(F + x) > \rho(F).$$

We write $\mathcal{F}_\rho$ to denote the set of flats for the q-matroid $(\mathcal{E}, \rho)$.

In [BCJ17, Theorem 1] it is shown that the collection $\mathcal{F}_\rho$ of flats form a geometric lattice. [Byr+23, Theorem 3.10] shows that the meet of two flats in this lattice is the intersection of the flats. We now need to define cycles for a q-matroid. First, the nullity of a subspace A is is given by $\eta(A) = \dim A - \rho(A)$. We can then define cycles.

Definition 4.62. *Let $\mathcal{M} = (\mathcal{E}, \rho)$ be a q-matroid, and let η its nullity function. For all $0 \leq i \leq \eta(\mathcal{E})$, a subspace $X \subseteq \mathcal{E}$ of nullity i is called a cycle of $\mathcal{M}$ if X is minimal in $\mathcal{N}_i$ w.r.t inclusion, where*

$$\mathcal{N}_i = \{X \in \mathcal{L}(\mathcal{E}) | \eta(X) = i\}.$$

A cycle of a q-matroid has a special relation to the flats of the dual of the q-matroid. As shown in [JPV22, Lemma 13], a subspace $X \subseteq \mathcal{E}$ is a cycle of $\mathcal{M}$ if and only if its orthogonal compliment $X^\perp$ is a flat in the q-matroid $\mathcal{M}^*$.

Definition 4.63. *Let $(E, \mathcal{R})$ be a poset. The opposite of a poset (E, R) is the poset $E, \mathcal{S}$ where $x\mathcal{S}y \Leftrightarrow y\mathcal{R}x$.*

Lemma 4.64. *let $\mathcal{M} = (\mathcal{E}, \rho)$ be a q-matroid. Then the collection of cycles of $\mathcal{M}$ is isomorphic to the opposite lattice of the lattice of flats for the dual q-matroid $\mathcal{M}^*$.*

Proof. Let ϕ be a bijection $\phi(X) = X^\perp$. We can see that this is a map between the cycles of $\mathcal{M}$ and the flats of $\mathcal{M}^*$. Let O_1 and O_2 be two cycles of $\mathcal{M}$. If $O_1 \subseteq O_2$ then $\phi(O_1) \supseteq \phi(O_2)$. Also, if $\phi(O_1) \supseteq \phi(O_2)$ then $O_1 \subseteq O_2$. Therefore the lattice of cycles of $\mathcal{M}$ is the opposite lattice of the lattice of flats of $\mathcal{M}^*$. □

Since the cycles of a q-matroid from a finite lattice where the rank in the lattice is given by η, we may use this lattice to define the derived matroid of a q-matroid.

Definition 4.65. *Let $\mathcal{M}$ be a q-matroid, and let $\mathcal{L}_\mathcal{C}$ be the lattice of cycles of $\mathcal{M}$. Then the derived matroid $\delta\mathcal{M}$ is $\delta\mathcal{L}_\mathcal{C}$.*

Given a q-matroid $(\mathcal{E}, \rho)$, Johnsen, Pratihar, and Verdure [JPV22] showed that this induces a classical matriod $\mathcal{P}(\mathcal{M})$ called the projectivization matroid on the ground set $E = \{x \subseteq \mathcal{E} | \dim x = 1\}$. They also showed that the posets of cycles of $\mathcal{P}(\mathcal{M}^*)^*$ and $\mathcal{M}$ are isomorphic. Since these two posets are the isomorphic, we get the following proposition.

Proposition 4.66. *Let $\mathcal{M}$ be a q-matroid. Then the derived matroid $\delta\mathcal{M}$ is isomorphic to the derived matroid $\delta_{FJK}\mathcal{P}(\mathcal{M}^*)^*$.*

In particular, this means that the derived matroid of q-matroids are a special case of derived matroids.

4.9 Extended Longyear derived matroid

The Longyear derived matroid was defined using the circuit bases of a matroid, but had the property that a set is dependent if and only if a subset has an empty

Kirkhoff sum. This can be used to extend the definition to any matroid, not just binary matroids.

Proposition 4.67. *Let M be any matroid and let $\mathcal{D}$ be the set*

$$\mathcal{D} = \min\{D \subseteq \mathcal{C}(M) | K(D) = \emptyset, D \neq \emptyset\}$$

Then there is a binary matroid whose ground set is $\mathcal{C}(M)$ and with the circuits $\mathcal{D}$.

Proof. $\mathcal{D}$ clearly satisfies the first two axioms for the circuits of a matroid. Now consider the third axiom. Let $\mathbf{C}_1, \mathbf{C}_2 \in \mathcal{D}$ such that $\mathbf{C}_1 \cap \mathbf{C}_2 \neq \emptyset$. WLOG consider $e \in K(\mathbf{C}_1 \backslash \mathbf{C}_2)$. We have that e occurs in an odd number of circuits of $\mathbf{C}_1 \backslash \mathbf{C}_2$, and therefore e occurs in an odd number of circuits of $\mathbf{C}_1 \cap \mathbf{C}_2$. Thus $e \in K(\mathbf{C}_2 \backslash \mathbf{C}_1)$. Therefore $K(\mathbf{C}_1 \Delta \mathbf{C}_2) = \emptyset$, so there is some $\mathbf{C}_3 \in \mathcal{D}$ such that $\mathbf{C}_3 \subseteq \mathbf{C}_1 \Delta \mathbf{C}_2$, and the third axiom is satisfied. Furthermore, by [Oxl92, Theorem 9.1.2], this matroid is binary. □

Note. *The fact that $\mathbf{C}_i$ was a set of circuits was not used in this proof, so $\mathcal{C}(M)$ may be substituted with any set of sets and the result will still be a matroid.*

Definition 4.68. *Let M be a matroid. The extended Longyear derived matroid $\delta_{EL}M$ is the matroid from the previous proposition.*

Proposition 4.69. *If M is a binary matroid, then $\delta_L M = \delta_{EL} M$.*

Proposition 4.70. *Let M be a matroid. Then $\delta_{EL}M$ is a simple matroid.*

Proof. Let D be a 1-circuit in $\delta_{EL}M$. Then D is non-empty with an empty Kirkhoff sum. If $|D| = 1$, then $K(D) = \text{supp}(D)$, so this is not possible. If $D = \{C_1, C_2\}$ and $K(D) = \emptyset$, then this implies that $C_1 \Delta C_2 = \emptyset$, so $C_1 = C_2$, and not possible. □

Proposition 4.71. *Let M be a matroid, and let B be a basis of M. Then the set $I = \{C_{eB} | e \in E(M) \backslash B\}$ is independent in $\delta_{EL}M$.*

Proof. Let $A \subseteq I$. Then $A = \{C_{e_1 B}, \ldots, C_{e_i B}\}$, and $\{e_1, \ldots, e_i\} \subseteq K(A)$, so A is not a 1-circuit in $\delta_{EL}M$. Thus I contains no 1-circuits and is not a 1-circuit itself, so it is independent in $\delta_{EL}M$. □

Even though this extended Longyear derived matroid coincides with the Longyear derived matroid for binary matroids, they do not necessarily coincide with Oxley-Wang derived matroids and combinatorial derived matroids. The following two examples illuminates this.

Example 4.72. *Let $M = U_{2,4}$, which has the circuits $\mathcal{C}(M) = \{123, 124, 134, 234\}$. We have that $\delta_{OW}M = U_{2,4}$, and further that $\delta_{FJK}M = U_{2,4}$. However the Kirkhoff sum of all non-empty subsets of $\mathcal{C}(M)$ are non-empty, so we have that $\delta_{EL}(M[A]) \simeq U_{4,4}$. We thus have that every dependent set in $\delta_{EL}M$ are dependent in $\delta_{OW}M$ and $\delta_{FJK}M$ in this case.*

Example 4.73 (Continuation of Example 4.42)**.** *We are looking at the matroid $U_{3,8}$, and we have the set $A = \{1234, 5678, 1256, 3478\}$. The Kirkhoff sum of this set is $K(A) = \emptyset$, so this is dependent in $\delta_{EL}U_{3,8}$, but we have that $A \notin \uparrow\mathcal{A}_0$ in the sense of the combinatorial derived matroid, so A is not dependent in the combinatorial derived matroid.*

5 Implemented software

Parts of the theory on matroids are implemented in a software library, as a crate in Rust, available at `https://github.com/teo8192/matroid-rs` [Knu23]. This software has been used to calculate several of the examples in this thesis. The correctness of the code is verified with several unit tests. Several of the algorithms also utilizes parallelization, which is done using the Rayon library [MS+] guaranteeing data-race free execution.

It is quite simple to implement matroids, one only needs to find an algorithm to get the rank function of the desired matroid. This is quite simple for uniform matroids, by letting the rank of a subset be the minimum of the cardinality of the subset and the rank of the uniform matroid. Vector matroids are letting the subset select the column vectors in the specified matrix, and using Gauss-Jordan to calculate the rank. If we have a list of bases for a matroid, the rank of a subset is simply the largest cardinality of the intersection of the subset with any of the bases.

When we already have a matroid, this can be used to create new ones. The rank of a subset for the dual matroid can be calculated using the rank function of the original matroid, see Section 3.5. The rank function of the l-th elongation of a matroid can be formulated using the rank function of the original matroid, and is given by

$$r_{M^{(l)}}(S) = \begin{cases} r_M(S) + l & \text{if } |S| - r_M(S) > l \\ |S| & \text{otherwise} \end{cases}$$

For combinatorial derived matroids, there are two ways this is implemented, depending on if the matroid is a fast matroid or not. If it is a fast matroid, then the bases of the matroid is computed using Equation (4.50). For non-fast matroids, a modified version of [FJK23, Proposition 20] is used to find the bases. Since the bases are the sets of maximal cardinality that are not circuits, or do not contain a circuit as a subset, we can ignore some of the elements in the construction of the circuits of the derived matroid. Algorithm 1 shows a simplified version of the algorithm that is used.

The software has some limitations; since the internal representation of a set is

Algorithm 1 Computation of bases of combinatorial derived matroid

procedure BASES OF DERIVED MATROID(Matroid M with rank function r and nullity function n)
$r_{max} \leftarrow |E(M)| - r(M)$
$\mathcal{D}_0 \leftarrow \min\{D \subseteq \mathcal{C}(M) | 3 \leq |D| \leq r_{max}, |D| > n(D)\}$
$i \leftarrow 0$
repeat
$i \leftarrow i + 1$
$\mathcal{D}_{i+1} \leftarrow \min \epsilon'(\mathcal{D}_i)$ ▷ Where $\epsilon'(\mathcal{D}) = \{D \in \epsilon(\mathcal{D}) || D| \leq r_{max}\}$
until $|\mathcal{D}_{i+1}| = |\mathcal{D}_i|$
repeat
$\mathcal{B} \leftarrow \{B \subseteq \mathcal{C}(M) || B| = r_{max}, \forall S \subseteq B, S \notin \mathcal{D}_i\}$
$r_{max} \leftarrow r_{max} - 1$
until $\mathcal{B} \neq \emptyset$
return $\mathcal{B}$
end procedure

represented by a 32-bit or 64-bit integer depending on the architecture, the largest possible sets that can be used are on 32 or 64 elements respectively. This sets a limitation to the size of matroids where we can find the combinatorial derived matroid, for example $U_{3,8}$ has 70 circuits so the combinatorial derived matroid cannot be calculated in this case. The upper limit could be extended by using larger fixed representations, but for arbitrary sizes heap allocation would most likely be necessary, causing performance loss based on the high frequency of the creation and destruction of the set-type.

The software is also capable of calculating the Betti-numbers of free resolutions of Stanley-Reisner rings from matroids. The next subsection gives an overview of what this is, and how it is calculated. Appendix B has some calculated resolutions of combinatorial derived matroids from uniform matroids and their elongations.

It is important to note that the determination of all Betti numbers of a representable matroid associated to a linear code C over $\mathbb{F}_q$, in addition to the determination of all Betti numbers of its elongations, also determines 2 other properties of the code:

1. Its higher weight spectra, i.e.

$$A_w^{(r)} = |\{C' \subseteq C | \dim C' = r, w(C') = w\}|$$

for all w, r.

2. Its generalized weight polynomials, $P_w(z)$, for $w = 0, \ldots, n$, where $P_w(q^m)$ is the number of codewords of weight w for the code $C_m = C \underset{\mathbb{F}_q}{\otimes} \mathbb{F}_{q^m}$ for all $m \in \mathbb{N}$.

There are certain formulas for passing from one such set of data to another, see [Jur12] and [JRV16].

5.1 Calculation of Betti-numbers for matroids

Let $E = \{1, \ldots, n\}$ be a set. A *simplicial complex* $\Delta \subseteq 2^E$ is a collection of subsets of E such that if $S \subseteq T \in \Delta$ then $S \in \Delta$. We can see that this is quite reminiscent of the independent sets of a matroid, and the set of independent sets is a simplicial complex. An element $\sigma \in \Delta$ is called a face, and if it is inclusion maximal it is called a facet. Let f_k denote the number of faces of cardinality k. The *reduced Euler characteristic* of Δ is $\chi(\Delta) = -1 + f_1 - f_2 + \cdots \pm f_k$ [Bjö92]. Define $\mathcal{N}(\Delta) = \min\{\sigma | \sigma \notin \Delta\}$ as the inclusion minimal elements that are not in the simplicial complex.

Let $S = k[x_1, \ldots, x_n]$ be the polynomial ring over some field k. The Stanley-Reisner ideal of a simplicial complex Δ is the ideal $I_\Delta = \langle x^\sigma | \sigma \subseteq \mathcal{N}(\Delta) \rangle$ and the Stanley-Reisner ring R_Δ is S/I_Δ, where $x^\sigma = \prod_{i \in \sigma} x_i$.

A ring R is $\mathbb{Z}$-graded if $R = \bigoplus_{i \in \mathbb{Z}} R_i$ and $R_i R_j \subseteq R_{i+j}$ for all $i, j \in \mathbb{Z}$.

Example 5.1 ($\mathbb{Z}$-graded ring)**.** *Let $R = S = k[x_1, \ldots, x_n]$. Define $R_i = \{0\}$ for $i \leq 0$, $R_0 = k$ and $R_i = \{$homogeneous polynomials of degree $i\}$. We can see that $R = \bigoplus_{i \in \mathbb{Z}} R_i$.*

Let M be a finitely generated S-module. Similarly M is $\mathbb{Z}$-graded if $M = \bigoplus_{i \in \mathbb{Z}} M_i$ and $S_i M_j \subseteq M_{i+j}$ for all $i, j \in \mathbb{Z}$.

We can also have $\mathbb{Z}^n$-gradings. These have a quite similar construction, and a finitely generated S-module M is $\mathbb{Z}^n$-graded if $M = \bigoplus_{\mathbf{a}\in\mathbb{Z}^n} M_{\mathbf{a}}$ and $S_{\mathbf{a}}M_{\mathbf{b}} \subseteq M_{\mathbf{a}+\mathbf{b}}$ for all $\mathbf{a}, \mathbf{b} \in \mathbb{Z}^n$.

Example 5.2. *We have that* $S = \bigoplus_{\mathbf{a}\in\mathbb{Z}^n} S_{\mathbf{a}}$ *where*

$$S_{\mathbf{a}} = \begin{cases} \langle x^{\mathbf{a}} \rangle & \text{if } \mathbf{a} \in \mathbb{Z}^n_{\geq 0} \\ 0 & \text{otherwise} \end{cases}$$

where $x^{\mathbf{a}} = x_1^{a_1} \cdots x_n^{a_n}$ *if* $\mathbf{a} = (a_1, \ldots, a_n)$. *Observe that* $S_i = \bigoplus_{\sum a_j = i} S_{\mathbf{a}}$.

Note the following observation: Let $I \subseteq S$ be an ideal. Then I is a $\mathbb{Z}$-graded module if I is generated by homogeneous polynomials, and it is a $\mathbb{Z}^n$-graded module if I is generated by monomials.

Given S, we have that $S(d)$ is the same ring but with a different grading;

$$S(d)_r = S_{d+r}.$$

This is called a *shift*.

Let M and N be $\mathbb{Z}$-graded S-modules. Then $\varphi : M \to N$ is $\mathbb{Z}$-graded if $\varphi(M_i) \subseteq N_i$ for all i.

A sequence of R-modules

$$M_{i+1} \xrightarrow{\varphi} M_i \xrightarrow{\psi} M_{i-1}$$

is exact if $\ker \psi = \operatorname{im} \varphi$.

Definition 5.3. *A long exact sequence*

$$\cdots \to F_2 \xrightarrow{\varphi_1} F_1 \xrightarrow{\varphi_0} F_0 \to M \to 0$$

of $\mathbb{Z}$*-graded* S*-modules with each*

$$F_i = \bigoplus_{j\in\mathbb{Z}} S(-j)^{\beta_{i,j}}$$

is called a free $\mathbb{Z}$*-resolution.*

A $\mathbb{Z}$-graded free resolution is called *minimal* if $\mathrm{im}(\phi_i) \subseteq \mathfrak{m}F_i$, where $\mathfrak{m} = \langle x_1, \ldots, x_n \rangle$. The Hilbert series of M can be recovered from the Betti numbers, which yields s independent equations formulated as Boij and Söderberg [BS12]

$$\sum_{i=0}^{l} \sum_{j \in \mathbb{Z}} (-1)^i \beta_{i,j} j^m, \quad m = 0, 1, \ldots, s-1, \tag{5.4}$$

where s is the codimension of M and l is the length of the resolution.

Theorem 5.5. *The Betti-numbers $\beta_{i,j}$ are the same for all minimal free resolutions of a S-module M for a fixed k. Further, if the module is the Stanley-Reisner ring of a matroid, the Betti-numbers are independent of the choice of field k.*

Proof. See [JV13]. □

A minimal free resolution with the property that

$$F_i = \bigoplus_{\mathbf{a} \in \mathbb{Z}, \sum_r a_r = j} S(-\mathbf{a})^{\beta_{i,\mathbf{a}}}$$

is called a minimal $\mathbb{Z}^n$-graded free resolution.

We will now restrict our attention to the case of minimal free resolutions of a Stanley-Reisner ring, and where the simplicial complex comes from a matroid. For notation, let $\beta_{i,\sigma} = \beta_{i,\mathbf{a}}$, where $\sigma \subseteq \{1, \ldots, n\}$ and $a_i = 1$ if $i \in \sigma$ and 0 otherwise.

Proposition 5.6. *Let M be a matroid, and $\sigma \subseteq E(M)$. Then $\beta_{i,\sigma} \neq 0$ if and only if σ is a cycle of nullity i. Further,*

$$\beta_{i,\sigma} = (-1)^{r(\sigma)-1} \chi(M_\sigma),$$

where $M_\sigma = M \backslash (E \backslash \sigma)$ is the restriction of the matroid to σ and $\chi(M)$ is the Euler characteristic of the simplicial complex induced by the matroid M.

Proof. See [JV13, Theorem 1] □

Note that we have

$$\beta_{i,j} = \sum_{\sigma \subseteq E, |\sigma| = j} \beta_{i,\sigma}.$$

The software uses Proposition 5.6 and Equation (5.4) to calculate the Betti-numbers for a matroid.

The Betti-numbers of a matroid are connected to their generalized hamming weights. From Proposition 5.6 we obtain

Proposition 5.7. *For all* $1 \leq i \leq n(M) = r^*(M)$*, we have*

$$d_i(M^*) = \min\{j | \beta_{i,j}(M) \neq 0\}.$$

Proof. See [JV13, Theorem 2]. □

The $d_i(M)$ will be given by Theorem 3.24. The free resolutions listen in Appendix B will then in particular determine all the generalized weights d_i for all the combinatorial derived matroids listed.

6 Final overview

In this thesis we have described some foundational theory on codes and matroids, and shown some aspects and properties of these objects. Because of their similar nature, some connections between these topics have also been explained, such as the fact that the generalized hamming weights of a code can be determined only by its associated matroid.

Some of the history and different definitions of derived matroids has been mentioned. Further, the rank of the combinatorial derived matroid for a certain class of matroids, fast matroids, has been proven to be equal to the corank of the matroid, and an example of the combinatorial derived matroid of the Vámos matroid shows that this is not true in general. A generalization of the concept of combinatorial derived matroids for lattices has been introduced, and some properties of this matroid have been proven. This generalization is further used to define a combinatorial derived matroid for q-matroids. The last subsection discussed a possibility of generalizing a construction by Longyear for obtaining derived matroids from binary matroids only, to a construction than can be applied to all matroids. We demonstrated that the resulting derived matroids may be different from the derived matroids obtained by other authors.

Features of the software were discussed, and some details around specific optimizations to the calculation of the combinatorial derived matroid were given. Further, Stanley-Reisner rings were introduced, in addition to free resolutions, Betti-numbers and how these could be calculated.

During the research, writing and development, some questions came up that could give rise to further investigations.

- The class of fast matroids seems to have some properties that are similar to the class of transversal matroids. Uniform matroids are in both classes, both are closed under deletion and direct sums, but neither are closed under duality nor contraction. The matroid $M(\mathrm{Sh}(4))$ is in neither class, but the matroid on the right in Figure 5 is in both. Are there any relations between these two classes?

- With the construction of the derived matroid from a lattice, we could try

to look at the matroid formed by the lattice of flats of a matroid. If the matroid is simple, then the derived matroid of the lattice of flats and the original matroid works on the same ground set. Is this derived matroid of any interest?

- One way to try to determine the upper limit for the rank of $\delta_{EL}M$ could be to create an independent set as in Proposition 4.71, and add one more circuit. What would happen in this case?

The answer to whether it is possible to simplify the construction of the combinatorial derived matroid is that it is possible in some cases, namely for fast matroids, but not in cases such as for the Vámos matroid and $M(\mathrm{Sh}(4))$.

Bibliography

[Grä78] George Grätzer. *General lattice theory*. Vol. 75. Pure and applied mathematics (New York : Academic Press). New York: Academic Press, 1978. ISBN: 0122957504.

[Lon80] Judith Q Longyear. "The circuit basis in binary matroids". In: *Journal of number theory* 12.1 (1980), pp. 71–76. ISSN: 0022-314X.

[Hil86] Raymond Hill. *A first course in coding theory*. Oxford applied mathematics and computing science series. Oxford: Clarendon Press, 1986. ISBN: 0198538049.

[Wei91] V.K. Wei. "Generalized Hamming weights for linear codes". In: *IEEE transactions on information theory* 37.5 (1991), pp. 1412–1418. ISSN: 0018-9448.

[Bjö92] Anders Björner. "Homology and Shellability of Matroids and Geometric Lattices". In: *Matroid Applications*. Cambridge University Press, 1992, pp. 226–283. ISBN: 9780521381659.

[Oxl92] James G Oxley. *Matroid theory*. Vol. 3. Oxford science publications. Oxford: Oxford University Press, 1992. ISBN: 0198535635.

[Lar05] Ann-Hege Larsen. "Matroider og lineære koder". MA thesis. Universitetet i Bergen, June 2005.

[BS12] Mats Boij and Jonas Söderberg. "Betti numbers of graded modules and the multiplicity conjecture in the non-Cohen–Macaulay case". In: *Algebra & Number Theory* 6.3 (2012), pp. 437–454. ISSN: 1937-0652.

[Jur12] R.P.M.J Jurrius. "Weight enumeration of codes from finite spaces". In: *Designs, codes, and cryptography* 63.3 (2012), pp. 321–330. ISSN: 0925-1022.

[JV13] Trygve Johnsen and Hugues Verdure. "Hamming weights and Betti numbers of Stanley–Reisner rings associated to matroids". In: *Applicable Algebra in Engineering, Communication and Computing* 24.1 (Jan. 2013), pp. 73–93. ISSN: 1432-0622. DOI: 10.1007/s00200-012-0183-7. URL: https://doi.org/10.1007/s00200-012-0183-7.

[JP15] Relinde Jurrius and Ruud Pellikaan. "The coset leader and list weight enumerator". In: *Contemporary Math* 632 (2015), pp. 229–251.

[JRV16] Trygve Johnsen, Jan Roksvold, and Hugues Verdure. "A generalization of weight polynomials to matroids". In: *Discrete mathematics* 339.2 (2016), pp. 632–645. ISSN: 0012-365X.

[BCJ17] Guus Bollen, Henry Crapo, and Relinde Jurrius. "The Tutte q-Polynomial". In: (2017). arXiv: 1707.03459 [math.CO].

[OW19] James Oxley and Suijie Wang. "Dependencies Among Dependencies in Matroids". In: *The Electronic Journal of Combinatorics* 26.3 (Sept. 2019). DOI: 10.37236/8742.

[FK21] Ragnar Freij-Hollanti and Olga Kuznetsova. "Information hiding using matroid theory". In: *Advances in Applied Mathematics* 129 (2021), p. 102205. ISSN: 0196-8858. DOI: https://doi.org/10.1016/j.aam.2021.102205. URL: https://www.sciencedirect.com/science/article/pii/S0196885821000439.

[BCJ22] Eimear Byrne, Michela Ceria, and Relinde Jurrius. "Constructions of new q-cryptomorphisms". In: *Journal of Combinatorial Theory, Series B* 153 (2022), pp. 149–194. ISSN: 0095-8956. DOI: https://doi.org/10.1016/j.jctb.2021.12.001. URL: https://www.sciencedirect.com/science/article/pii/S0095895621001003.

[JPV22] Trygve Johnsen, Rakhi Pratihar, and Hugues Verdure. "Weight spectra of Gabidulin rank-metric codes and Betti numbers". In: *São Paulo Journal of Mathematical Sciences* (2022). DOI: 10.1007/s40863-022-00314-y.

[Byr+23] Eimear Byrne et al. "Constructions of new matroids and designs over $\mathbb{F}_q$". In: *Designs, Codes and Cryptography* 91 (2023), pp. 451–473. DOI: 10.1007/s10623-022-01087-3.

[FJK23] Ragnar Freij-Hollanti, Relinde Jurrius, and Olga Kuznetsova. "Combinatorial Derived Matroids". In: *The Electronic Journal of Combinatorics* (2023), P2–8. DOI: 10.37236/11327.

[Knu23] Teodor Dahl Knutsen. *matroids-rs*. Software Library. 2023. URL: https://github.com/teo8192/matroid-rs.

[MS+] Niko Matsakis, Josh Stone, et al. *rayon*. URL: https://github.com/rayon-rs/rayon.

A Alternative proof of Proposition 4.44 for uniform matroids

Proposition A.1. *If $M = U_{k,n}$ and $A \in \min \mathcal{A}_1$, then $A \in \min \mathcal{A}_0$.*

Proof. Let $A \in \min \mathcal{A}_1$. Either $A \in \min \mathcal{A}_0$ and we are done, or we may find $A_1, A_2 \in \min \mathcal{A}_0$ such that $A = A_1 \cup A_2 \backslash \{C\}$ for some $C \in A_1 \cap A_2$ (from [FJK23, Lemma 18], $i = 0$). Let $S_i = \operatorname{supp}(A_i)$ denote the union of the circuits. We want to show that $n(\operatorname{supp}(A)) < |A|$. First, observe that

$$|A_i| = n(\operatorname{supp}(A_i)) + 1 = |S_i| - k + 1. \tag{A.2}$$

Since $A_1 \cap A_2 \notin \mathcal{A}_0$, we know that $n(\operatorname{supp}(A_1 \cap A_2)) \geq |A_1 \cap A_2|$. Also, note that $\operatorname{supp}(A_1 \cap A_2) \subseteq S_1 \cap S_2$ so $n(S_1 \cap S_2) \geq n(\operatorname{supp}(A_1 \cap A_2))$. From this, we may see that

$$|S_1 \cap S_2| - k \geq n(\operatorname{supp}(A_1 \cap A_2)) \geq |A_1 \cap A_2| \Rightarrow -|S_1 \cap S_2| \leq -|A_1 \cap A_2| - k \tag{A.3}$$

$$\begin{aligned}
n(\operatorname{supp}(A)) &= n(S_1 \cup S_2) \\
&= |S_1 \cup S_2| - k \\
&= |S_1| + |S_2| - |S_1 \cap S_2| - k \\
&\leq |S_1| + |S_2| - |A_1 \cap A_2| - 2k && \text{(from (A.3))} \\
&= |A_1| + k - 1 + |A_2| + k - 1 - |A_1 \cap A_2| - 2k && \text{(from (A.2))} \\
&= |A_1| - 1 + |A_2| - 1 - |A_1 \cap A_2| \\
&< |A_1| - 1 + |A_2| - 1 - |A_1 \cap A_2| + 1 \\
&= |A_1 \backslash \{C\}| + |A_2 \backslash \{C\}| - |A_1 \cap A_2 \backslash \{C\}| \\
&= |A|
\end{aligned}$$

Thus $n(\operatorname{supp}(A)) < |A|$, so $A \in \mathcal{A}_0$. Since $\mathcal{A}_0 \subseteq \mathcal{A}_1$, we must have that the inclusion minimal elements in $\mathcal{A}_1$ that are in A_0 must also be inclusion minimal in A_0. Therefore $A \in \min \mathcal{A}_0$. □

B The resolutions of elongations of combinatorial derived matroids of several uniform matroids

By $\delta_{FJK}U_{k,n}^{(l)}$, we mean the l'th elongation of $\delta_{FJK}U_{u,k}$.

$\delta_{FJK}U_{1,2}$: $0 \leftarrow S/I \leftarrow S \leftarrow 0$

$\delta_{FJK}U_{1,3}$: $0 \leftarrow S/I \leftarrow S \leftarrow S(-3) \leftarrow 0$

$\delta_{FJK}U_{1,3}^{(1)}$: $0 \leftarrow S/I \leftarrow S \leftarrow 0$

$\delta_{FJK}U_{2,3}$: $0 \leftarrow S/I \leftarrow S \leftarrow 0$

$\delta_{FJK}U_{1,4}$: $0 \leftarrow S/I \leftarrow S \leftarrow S(-3)^4 \oplus S(-4)^3 \leftarrow S(-5)^{12} \leftarrow S(-6)^6 \leftarrow 0$

$\delta_{FJK}U_{1,4}^{(1)}$: $0 \leftarrow S/I \leftarrow S \leftarrow S(-5)^6 \leftarrow S(-6)^5 \leftarrow 0$

$\delta_{FJK}U_{1,4}^{(2)}$: $0 \leftarrow S/I \leftarrow S \leftarrow S(-6) \leftarrow 0$

$\delta_{FJK}U_{1,4}^{(3)}$: $0 \leftarrow S/I \leftarrow S \leftarrow 0$

$\delta_{FJK}U_{2,4}$: $0 \leftarrow S/I \leftarrow S \leftarrow S(-3)^4 \leftarrow S(-4)^3 \leftarrow 0$

$\delta_{FJK}U_{2,4}^{(1)}$: $0 \leftarrow S/I \leftarrow S \leftarrow S(-4) \leftarrow 0$

$\delta_{FJK}U_{2,4}^{(2)}$: $0 \leftarrow S/I \leftarrow S \leftarrow 0$

$\delta_{FJK}U_{3,4}$: $0 \leftarrow S/I \leftarrow S \leftarrow 0$

$\delta_{FJK}U_{1,5}$: $0 \leftarrow S/I \leftarrow S \leftarrow S(-3)^{10} \oplus S(-4)^{15} \oplus S(-5)^{12} \leftarrow S(-5)^{60} \oplus S(-6)^{155} \leftarrow S(-6)^{30} \oplus S(-7)^{450} \leftarrow S(-8)^{510} \leftarrow S(-9)^{260} \leftarrow S(-10)^{51} \leftarrow 0$

$\delta_{FJK}U_{1,5}^{(1)}$: $0 \leftarrow S/I \leftarrow S \leftarrow S(-5)^{30} \oplus S(-6)^{85} \leftarrow S(-6)^{25} \oplus S(-7)^{420} \leftarrow S(-8)^{645} \leftarrow S(-9)^{410} \leftarrow S(-10)^{96} \leftarrow 0$

$\delta_{FJK}U_{1,5}^{(2)}$: $0 \leftarrow S/I \leftarrow S \leftarrow S(-6)^5 \oplus S(-7)^{100} \leftarrow S(-8)^{285} \leftarrow S(-9)^{260} \leftarrow S(-10)^{79} \leftarrow 0$

$\delta_{FJK}U_{1,5}^{(3)}$: $0 \leftarrow S/I \leftarrow S \leftarrow S(-8)^{45} \leftarrow S(-9)^{80} \leftarrow S(-10)^{36} \leftarrow 0$

$\delta_{FJK}U_{1,5}^{(4)}$: $0 \leftarrow S/I \leftarrow S \leftarrow S(-9)^{10} \leftarrow S(-10)^9 \leftarrow 0$

$\delta_{FJK}U_{1,5}^{(5)}$: $0 \leftarrow S/I \leftarrow S \leftarrow S(-10) \leftarrow 0$

$\delta_{FJK}U_{1,5}^{(6)}$: $0 \leftarrow S/I \leftarrow S \leftarrow 0$

$\delta_{FJK}U_{2,5}$: $0 \leftarrow S/I \leftarrow S \leftarrow S(-3)^{20} \oplus S(-4)^{85} \leftarrow S(-4)^{15} \oplus S(-5)^{588} \leftarrow S(-6)^{1400} \leftarrow S(-7)^{1700} \leftarrow S(-8)^{1155} \leftarrow S(-9)^{420} \leftarrow S(-10)^{64} \leftarrow 0$

$\delta_{FJK}U_{2,5}^{(1)}$: $0 \leftarrow S/I \leftarrow S \leftarrow S(-4)^5 \oplus S(-5)^{222} \leftarrow S(-6)^{975} \leftarrow S(-7)^{1700} \leftarrow S(-8)^{1500} \leftarrow S(-9)^{670} \leftarrow S(-10)^{121} \leftarrow 0$

$\delta_{FJK}U_{2,5}^{(2)}$: $0 \leftarrow S/I \leftarrow S \leftarrow S(-6)^{210} \leftarrow S(-7)^{720} \leftarrow S(-8)^{945} \leftarrow S(-9)^{560} \leftarrow S(-10)^{126} \leftarrow 0$

$\delta_{FJK}U_{2,5}^{(3)}$: $0 \leftarrow S/I \leftarrow S \leftarrow S(-7)^{120} \leftarrow S(-8)^{315} \leftarrow S(-9)^{280} \leftarrow S(-10)^{84} \leftarrow 0$

$\delta_{FJK}U_{2,5}^{(4)}$: $0 \leftarrow S/I \leftarrow S \leftarrow S(-8)^{45} \leftarrow S(-9)^{80} \leftarrow S(-10)^{36} \leftarrow 0$

$\delta_{FJK}U_{2,5}^{(5)}$: $0 \leftarrow S/I \leftarrow S \leftarrow S(-9)^{10} \leftarrow S(-10)^{9} \leftarrow 0$

$\delta_{FJK}U_{2,5}^{(6)}$: $0 \leftarrow S/I \leftarrow S \leftarrow S(-10) \leftarrow 0$

$\delta_{FJK}U_{2,5}^{(7)}$: $0 \leftarrow S/I \leftarrow S \leftarrow 0$

$\delta_{FJK}U_{3,5}$: $0 \leftarrow S/I \leftarrow S \leftarrow S(-3)^{10} \leftarrow S(-4)^{15} \leftarrow S(-5)^{6} \leftarrow 0$

$\delta_{FJK}U_{3,5}^{(1)}$: $0 \leftarrow S/I \leftarrow S \leftarrow S(-4)^{5} \leftarrow S(-5)^{4} \leftarrow 0$

$\delta_{FJK}U_{3,5}^{(2)}$: $0 \leftarrow S/I \leftarrow S \leftarrow S(-5) \leftarrow 0$

$\delta_{FJK}U_{3,5}^{(3)}$: $0 \leftarrow S/I \leftarrow S \leftarrow 0$

$\delta_{FJK}U_{4,5}$: $0 \leftarrow S/I \leftarrow S \leftarrow 0$

$\delta_{FJK}U_{1,6}$: $0 \leftarrow S/I \leftarrow S \leftarrow S(-3)^{20} \oplus S(-4)^{45} \oplus S(-5)^{72} \oplus S(-6)^{60} \leftarrow S(-5)^{180} \oplus S(-6)^{940} \oplus S(-7)^{1620} \leftarrow S(-6)^{90} \oplus S(-7)^{2700} \oplus S(-8)^{11565} \leftarrow S(-8)^{3060} \oplus S(-9)^{36560} \leftarrow S(-9)^{1560} \oplus S(-10)^{64350} \leftarrow S(-10)^{306} \oplus S(-11)^{69660} \leftarrow S(-12)^{47995} \leftarrow S(-13)^{20700} \leftarrow S(-14)^{5130} \leftarrow S(-15)^{560} \leftarrow 0$

$\delta_{FJK}U_{1,6}^{(1)}$: $0 \leftarrow S/I \leftarrow S \leftarrow S(-5)^{90} \oplus S(-6)^{520} \oplus S(-7)^{900} \leftarrow S(-6)^{75} \oplus S(-7)^{2520} \oplus S(-8)^{11295} \leftarrow S(-8)^{3870} \oplus S(-9)^{48520} \leftarrow S(-9)^{2460} \oplus S(-10)^{106038} \leftarrow S(-10)^{576} \oplus S(-11)^{136080} \leftarrow S(-12)^{108030} \leftarrow S(-13)^{52650} \leftarrow S(-14)^{14535} \leftarrow S(-15)^{1748} \leftarrow 0$

$\delta_{FJK}U_{1,6}^{(2)}$: $0 \leftarrow S/I \leftarrow S \leftarrow S(-6)^{15} \oplus S(-7)^{600} \oplus S(-8)^{2805} \leftarrow S(-8)^{1710} \oplus S(-9)^{22280} \leftarrow S(-9)^{1560} \oplus S(-10)^{69312} \leftarrow S(-10)^{474} \oplus S(-11)^{114240} \leftarrow S(-12)^{110250} \leftarrow S(-13)^{63120} \leftarrow S(-14)^{19995} \leftarrow S(-15)^{2712} \leftarrow 0$

$\delta_{FJK}U_{1,6}^{(3)}$: $0 \leftarrow S/I \leftarrow S \leftarrow S(-8)^{270} \oplus S(-9)^{3595} \leftarrow S(-9)^{480} \oplus S(-10)^{21573} \leftarrow S(-10)^{216} \oplus S(-11)^{51975} \leftarrow S(-12)^{65625} \leftarrow S(-13)^{46305} \leftarrow S(-14)^{17415} \leftarrow S(-15)^{2733} \leftarrow 0$

$\delta_{FJK}U_{1,6}^{(4)}$: $0 \leftarrow S/I \leftarrow S \leftarrow S(-9)^{60} \oplus S(-10)^{2697} \leftarrow S(-10)^{54} \oplus S(-11)^{12750} \leftarrow S(-12)^{23825} \leftarrow S(-13)^{22200} \leftarrow S(-14)^{10365} \leftarrow S(-15)^{1942} \leftarrow 0$

$\delta_{FJK}U_{1,6}^{(5)}$: $0 \leftarrow S/I \leftarrow S \leftarrow S(-10)^{6} \oplus S(-11)^{1335} \leftarrow S(-12)^{4945} \leftarrow S(-13)^{6870} \leftarrow S(-14)^{4260} \leftarrow S(-15)^{995} \leftarrow 0$

$\delta_{FJK}U_{1,6}^{(6)}$: $0 \leftarrow S/I \leftarrow S \leftarrow S(-12)^{455} \leftarrow S(-13)^{1260} \leftarrow S(-14)^{1170} \leftarrow S(-15)^{364} \leftarrow 0$

$\delta_{FJK}U_{1,6}^{(7)}$: $0 \leftarrow S/I \leftarrow S \leftarrow S(-13)^{105} \leftarrow S(-14)^{195} \leftarrow S(-15)^{91} \leftarrow 0$

$\delta_{FJK}U_{1,6}^{(8)}$: $0 \leftarrow S/I \leftarrow S \leftarrow S(-14)^{15} \leftarrow S(-15)^{14} \leftarrow 0$

$\delta_{FJK}U_{1,6}^{(9)}$: $0 \leftarrow S/I \leftarrow S \leftarrow S(-15) \leftarrow 0$

$\delta_{FJK}U_{1,6}^{(10)}$:$0 \leftarrow S/I \leftarrow S \leftarrow 0$

$\delta_{FJK}U_{2,6}$: $0 \leftarrow S/I \leftarrow S \leftarrow S(-3)^{60} \oplus S(-4)^{510} \oplus S(-5)^{3432} \leftarrow S(-4)^{45} \oplus S(-5)^{3528} \oplus S(-6)^{64800} \leftarrow S(-6)^{8400} \oplus S(-7)^{484200} \leftarrow S(-7)^{10200} \oplus S(-8)^{2084460} \leftarrow S(-8)^{6930} \oplus S(-9)^{6015800} \leftarrow S(-9)^{2520} \oplus S(-10)^{12554640} \leftarrow S(-10)^{384} \oplus S(-11)^{19741800} \leftarrow S(-12)^{23916750} \leftarrow S(-13)^{22550880} \leftarrow S(-14)^{16564080} \leftarrow S(-15)^{9404304} \leftarrow S(-16)^{4053525} \leftarrow S(-17)^{1284000} \leftarrow S(-18)^{282160} \leftarrow S(-19)^{38460} \leftarrow S(-20)^{2451} \leftarrow 0$

$\delta_{FJK}U_{2,6}^{(1)}$: $0 \leftarrow S/I \leftarrow S \leftarrow S(-4)^{15} \oplus S(-5)^{1332} \oplus S(-6)^{22830} \leftarrow S(-6)^{5850} \oplus S(-7)^{318660} \leftarrow S(-7)^{10200} \oplus S(-8)^{1966410} \leftarrow S(-8)^{9000} \oplus S(-9)^{7329520} \leftarrow S(-9)^{4020} \oplus S(-10)^{18679386} \leftarrow S(-10)^{726} \oplus S(-11)^{34629660} \leftarrow S(-12)^{48275370} \leftarrow S(-13)^{51451620} \leftarrow S(-14)^{42136380} \leftarrow S(-15)^{26383812} \leftarrow S(-16)^{12431055} \leftarrow S(-17)^{4272660} \leftarrow S(-18)^{1012460} \leftarrow S(-19)^{148020} \leftarrow S(-20)^{10071} \leftarrow 0$

$\delta_{FJK}U_{2,6}^{(2)}$: $0 \leftarrow S/I \leftarrow S \leftarrow S(-6)^{1260} \oplus S(-7)^{64200} \leftarrow S(-7)^{4320} \oplus S(-8)^{772800} \leftarrow S(-8)^{5670} \oplus S(-9)^{4247600} \leftarrow S(-9)^{3360} \oplus S(-10)^{14259000} \leftarrow S(-10)^{756} \oplus S(-11)^{32749080} \leftarrow S(-12)^{54414360} \leftarrow S(-13)^{67304160} \leftarrow S(-14)^{62728380} \leftarrow S(-15)^{44035992} \leftarrow S(-16)^{22987965} \leftarrow S(-17)^{8670480} \leftarrow S(-18)^{2236780} \leftarrow S(-19)^{353640} \leftarrow S(-20)^{25872} \leftarrow 0$

$\delta_{FJK}U_{2,6}^{(3)}$: $0 \leftarrow S/I \leftarrow S \leftarrow S(-7)^{720} \oplus S(-8)^{118500} \leftarrow S(-8)^{1890} \oplus S(-9)^{1289200} \leftarrow S(-9)^{1680} \oplus S(-10)^{6445800} \leftarrow S(-10)^{504} \oplus S(-11)^{19640400} \leftarrow S(-12)^{40643460} \leftarrow S(-13)^{60160320} \leftarrow S(-14)^{65276640} \leftarrow S(-15)^{52283088} \leftarrow S(-16)^{30662775} \leftarrow S(-17)^{12835680} \leftarrow S(-18)^{3638960} \leftarrow S(-19)^{627120} \leftarrow S(-20)^{49668} \leftarrow 0$

$\delta_{FJK}U_{2,6}^{(4)}$: $0 \leftarrow S/I \leftarrow S \leftarrow S(-8)^{270} \oplus S(-9)^{165200} \leftarrow S(-9)^{480} \oplus S(-10)^{1645200} \leftarrow S(-10)^{216} \oplus S(-11)^{7498800} \leftarrow S(-12)^{20651400} \leftarrow S(-13)^{38158560} \leftarrow S(-14)^{49634640} \leftarrow S(-15)^{46344672} \leftarrow S(-16)^{31043925} \leftarrow S(-17)^{14612400} \leftarrow S(-18)^{4601080} \leftarrow S(-19)^{871920} \leftarrow S(-20)^{75312} \leftarrow 0$

$\delta_{FJK}U_{2,6}^{(5)}$: $0 \leftarrow S/I \leftarrow S \leftarrow S(-9)^{60} \oplus S(-10)^{184150} \leftarrow S(-10)^{54} \oplus S(-11)^{1676300} \leftarrow S(-12)^{6918450} \leftarrow S(-13)^{17034600} \leftarrow S(-14)^{27685680} \leftarrow S(-15)^{31011288} \leftarrow S(-16)^{24229425} \leftarrow S(-17)^{13031700} \leftarrow S(-18)^{4615600} \leftarrow S(-19)^{971740} \leftarrow S(-20)^{92318} \leftarrow 0$

$\delta_{FJK}U_{2,6}^{(6)}$: $0 \leftarrow S/I \leftarrow S \leftarrow S(-10)^6 \oplus S(-11)^{167900} \leftarrow S(-12)^{1385400} \leftarrow S(-13)^{5115600} \leftarrow S(-14)^{11084100} \leftarrow S(-15)^{15517992} \leftarrow S(-16)^{14548275} \leftarrow S(-17)^{9128400} \leftarrow S(-18)^{3694850} \leftarrow S(-19)^{875100} \leftarrow S(-20)^{92372} \leftarrow 0$

$\delta_{FJK}U_{2,6}^{(7)}$: $0 \leftarrow S/I \leftarrow S \leftarrow S(-12)^{125970} \leftarrow S(-13)^{930240} \leftarrow S(-14)^{3023280} \leftarrow S(-15)^{5643456} \leftarrow S(-16)^{6613425} \leftarrow S(-17)^{4979520} \leftarrow S(-18)^{2351440} \leftarrow S(-19)^{636480} \leftarrow S(-20)^{75582} \leftarrow 0$

$\delta_{FJK}U_{2,6}^{(8)}$: $0 \leftarrow S/I \leftarrow S \leftarrow S(-13)^{77520} \leftarrow S(-14)^{503880} \leftarrow S(-15)^{1410864} \leftarrow S(-16)^{2204475} \leftarrow S(-17)^{2074800} \leftarrow S(-18)^{1175720} \leftarrow S(-19)^{371280} \leftarrow S(-20)^{50388} \leftarrow 0$

$\delta_{FJK}U_{2,6}^{(9)}$: $0 \leftarrow S/I \leftarrow S \leftarrow S(-14)^{38760} \leftarrow S(-15)^{217056} \leftarrow S(-16)^{508725} \leftarrow S(-17)^{638400} \leftarrow S(-18)^{452200} \leftarrow S(-19)^{171360} \leftarrow S(-20)^{27132} \leftarrow 0$

$\delta_{FJK}U_{2,6}^{(10)}$:$0 \leftarrow S/I \leftarrow S \leftarrow S(-15)^{15504} \leftarrow S(-16)^{72675} \leftarrow S(-17)^{136800} \leftarrow S(-18)^{129200} \leftarrow S(-19)^{61200} \leftarrow S(-20)^{11628} \leftarrow 0$

$\delta_{FJK}U_{2,6}^{(11)}$:$0 \leftarrow S/I \leftarrow S \leftarrow S(-16)^{4845} \leftarrow S(-17)^{18240} \leftarrow S(-18)^{25840} \leftarrow S(-19)^{16320} \leftarrow S(-20)^{3876} \leftarrow 0$

$\delta_{FJK}U_{2,6}^{(12)}$:$0 \leftarrow S/I \leftarrow S \leftarrow S(-17)^{1140} \leftarrow S(-18)^{3230} \leftarrow S(-19)^{3060} \leftarrow S(-20)^{969} \leftarrow 0$

$\delta_{FJK}U_{2,6}^{(13)}$:$0 \leftarrow S/I \leftarrow S \leftarrow S(-18)^{190} \leftarrow S(-19)^{360} \leftarrow S(-20)^{171} \leftarrow 0$

$\delta_{FJK}U_{2,6}^{(14)}$:$0 \leftarrow S/I \leftarrow S \leftarrow S(-19)^{20} \leftarrow S(-20)^{19} \leftarrow 0$

$\delta_{FJK}U_{2,6}^{(15)}$:$0 \leftarrow S/I \leftarrow S \leftarrow S(-20) \leftarrow 0$

$\delta_{FJK}U_{2,6}^{(16)}$:$0 \leftarrow S/I \leftarrow S \leftarrow 0$

$\delta_{FJK}U_{3,6}$: $0 \leftarrow S/I \leftarrow S \leftarrow S(-3)^{60} \oplus S(-4)^{735} \leftarrow S(-4)^{90} \oplus S(-5)^{8088} \leftarrow S(-5)^{36} \oplus S(-6)^{36850} \leftarrow S(-7)^{99000} \leftarrow S(-8)^{177705} \leftarrow S(-9)^{224840} \leftarrow S(-10)^{204732} \leftarrow S(-11)^{134100} \leftarrow S(-12)^{61875} \leftarrow S(-13)^{19140} \leftarrow S(-14)^{3570} \leftarrow S(-15)^{304} \leftarrow 0$

$\delta_{FJK}U_{3,6}^{(1)}$: $0 \leftarrow S/I \leftarrow S \leftarrow S(-4)^{30} \oplus S(-5)^{2697} \leftarrow S(-5)^{24} \oplus S(-6)^{23375} \leftarrow S(-7)^{91575} \leftarrow S(-8)^{215325} \leftarrow S(-9)^{336490} \leftarrow S(-10)^{364518} \leftarrow S(-11)^{276750} \leftarrow S(-12)^{145200} \leftarrow S(-13)^{50325} \leftarrow S(-14)^{10395} \leftarrow S(-15)^{971} \leftarrow 0$

$\delta_{FJK}U_{3,6}^{(2)}$: $0 \leftarrow S/I \leftarrow S \leftarrow S(-5)^6 \oplus S(-6)^{4945} \leftarrow S(-7)^{38340} \leftarrow S(-8)^{134415} \leftarrow S(-9)^{279020} \leftarrow S(-10)^{376866} \leftarrow S(-11)^{342720} \leftarrow S(-12)^{209490} \leftarrow S(-13)^{82890} \leftarrow S(-14)^{19245} \leftarrow S(-15)^{1996} \leftarrow 0$

$\delta_{FJK}U_{3,6}^{(3)}$: $0 \leftarrow S/I \leftarrow S \leftarrow S(-7)^{6435} \leftarrow S(-8)^{45045} \leftarrow S(-9)^{140140} \leftarrow S(-10)^{252252} \leftarrow S(-11)^{286650} \leftarrow S(-12)^{210210} \leftarrow S(-13)^{97020} \leftarrow S(-14)^{25740} \leftarrow S(-15)^{3003} \leftarrow 0$

$\delta_{FJK}U_{3,6}^{(4)}$: $0 \leftarrow S/I \leftarrow S \leftarrow S(-8)^{6435} \leftarrow S(-9)^{40040} \leftarrow S(-10)^{108108} \leftarrow S(-11)^{163800} \leftarrow S(-12)^{150150} \leftarrow S(-13)^{83160} \leftarrow S(-14)^{25740} \leftarrow S(-15)^{3432} \leftarrow 0$

$\delta_{FJK}U_{3,6}^{(5)}$: $0 \leftarrow S/I \leftarrow S \leftarrow S(-9)^{5005} \leftarrow S(-10)^{27027} \leftarrow S(-11)^{61425} \leftarrow S(-12)^{75075} \leftarrow S(-13)^{51975} \leftarrow S(-14)^{19305} \leftarrow S(-15)^{3003} \leftarrow 0$

$\delta_{FJK}U_{3,6}^{(6)}$: $0 \leftarrow S/I \leftarrow S \leftarrow S(-10)^{3003} \leftarrow S(-11)^{13650} \leftarrow S(-12)^{25025} \leftarrow S(-13)^{23100} \leftarrow S(-14)^{10725} \leftarrow S(-15)^{2002} \leftarrow 0$

$\delta_{FJK}U_{3,6}^{(7)}$: $0 \leftarrow S/I \leftarrow S \leftarrow S(-11)^{1365} \leftarrow S(-12)^{5005} \leftarrow S(-13)^{6930} \leftarrow S(-14)^{4290} \leftarrow S(-15)^{1001} \leftarrow 0$

$\delta_{FJK}U_{3,6}^{(8)}$: $0 \leftarrow S/I \leftarrow S \leftarrow S(-12)^{455} \leftarrow S(-13)^{1260} \leftarrow S(-14)^{1170} \leftarrow S(-15)^{364} \leftarrow 0$

$\delta_{FJK}U_{3,6}^{(9)}$: $0 \leftarrow S/I \leftarrow S \leftarrow S(-13)^{105} \leftarrow S(-14)^{195} \leftarrow S(-15)^{91} \leftarrow 0$

$\delta_{FJK}U_{3,6}^{(10)}$:$0 \leftarrow S/I \leftarrow S \leftarrow S(-14)^{15} \leftarrow S(-15)^{14} \leftarrow 0$

$\delta_{FJK}U_{3,6}^{(11)}$:$0 \leftarrow S/I \leftarrow S \leftarrow S(-15) \leftarrow 0$

$\delta_{FJK}U_{3,6}^{(12)}$:$0 \leftarrow S/I \leftarrow S \leftarrow 0$

$\delta_{FJK}U_{4,6}$: $0 \leftarrow S/I \leftarrow S \leftarrow S(-3)^{20} \leftarrow S(-4)^{45} \leftarrow S(-5)^{36} \leftarrow S(-6)^{10} \leftarrow 0$

$\delta_{FJK}U_{4,6}^{(1)}$: $0 \leftarrow S/I \leftarrow S \leftarrow S(-4)^{15} \leftarrow S(-5)^{24} \leftarrow S(-6)^{10} \leftarrow 0$

$\delta_{FJK}U_{4,6}^{(2)}$: $0 \leftarrow S/I \leftarrow S \leftarrow S(-5)^{6} \leftarrow S(-6)^{5} \leftarrow 0$

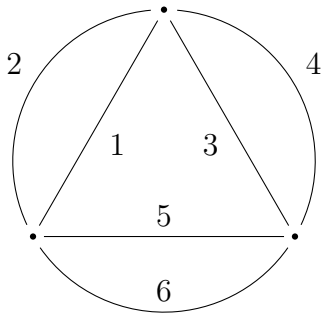
$\delta_{FJK}U_{4,6}^{(3)}$: $0 \leftarrow S/I \leftarrow S \leftarrow S(-6) \leftarrow 0$

$\delta_{FJK}U_{4,6}^{(4)}$: $0 \leftarrow S/I \leftarrow S \leftarrow 0$

$\delta_{FJK}U_{5,6}$: $0 \leftarrow S/I \leftarrow S \leftarrow 0$

C Circuits of a derived non-fast matroid

Let M be the matroid of the following graph.



Label the circuits of this matroid in the following way:

a: 12
b: 34
c: 135
d: 235
e: 145
f: 245
g: 136
h: 236
i: 146
j: 246
k: 56

The matroid $\delta_{FJK}M$ has the following 1-circuits: {acd, bce, abde, abcf, bdf, aef, cdef, agh, cdgh, bdegh, bcfgh, efgh, bgi, cegi, adegi, acfgi, dfgi, abhi, bcdhi, acehi, dehi, acfhi, bcfhi, adfhi, cdfhi, befhi, cefhi, cfghi, abgj, bcdgj, acegj, adegj, bdegj, cdegj, cfgj, adfgj, befgj, defgj, bhj, cehj, adehj, acfhj, dfhj, deghj, aij, cdij, bdeij, bcfij, efij, degij, cfhij, ghij, cgk, adgk, begk, abfgk, defgk, achk, dhk, abehk, bfhk, cefhk, bcik, abdik, eik, afik, cdfik, cfhik, fghik, abcjk, bdjk, aejk, cdejk, fjk, degjk, eghjk, dgijk, chijk}