UiT The Arctic University of Norway

Faculty of Science and Technology
Department of Mathematics and Statistics

Derived matroids

Comparison between three different concepts of derived matroids

Tobias Bøgner

Master's thesis in Mathematics MAT-3907, June 2023

Acknowledgments

First, I would like to thank my thesis supervisor Trygve Johnsen, for his impeccable help. His ideas and knowledge have laid the foundation for which this thesis has been written, and without him, I would not have delivered this thesis as it is.

I would also like to thank all the people who have helped me proofread the thesis and pointed out obvious, but hidden flaws. Without their help, the thesis would have been much more lackluster.

Contents

Introduction

The goal of this master's thesis is to give a summary of three different constructions of derived matroids, compare the similarities and differences between them, and highlight everything using a simple, but effective example. It also aims to give its readers a motivator as to why the study of derived matroids is a useful subject for mathematicians.

Before we can start defining derived matroids, we must first define codes, and then more specifically the family of codes classified as linear codes. Therefore, in Section 1, we will introduce the concept of codes, what it means to be an error-correcting code, and show some specific, but important, properties that linear codes possess as a subclass of block codes.

In Section 2, the focus will shift from codes to the mathematical construction: Matroids. This section will give five different, but at the same time, equally valid definitions of matroids, show why they are equal, and define some important properties of the matroid and its more specific substructures.

Thereafter, in Section 3, we will combine the first two chapters and give a connection between linear codes and matroids. In this section, we will therefore focus on how linear codes and matroids can be found using each other, and how specific properties of one can be used to find specific properties of the other.

Section 4, will then be used to delve into three different constructions of derived matroids: those given in Longyear (1980)'s text; Oxley and Wang (2019)'s text; and Freij-Hollanti et al. (2023)'s text. Here, we will focus on similarities and differences between the constructions and enhance these by using an example.

In Section 5, we will look at a specific usage of derived matroids in connection to Private Information Retrieval (PIR) and give the reader a motivator as to why mathematicians should study these constructs, aside from just the mathematical interest.

Lastly, in Section 6, we will give a short explanation as to why this master's thesis benefits me as a future teacher.

1 Codes

In general, codes give a way to convert information into another form, for which the information either can be sent as a message or stored in a specific location. The reason for encoding a piece of information may be many: we might want to shorten the information sent or stored to make the process easier and quicker; encrypt the information to make it more secure against uninvited "listeners"; or enlarge the code so that any corruption of the message may be sorted out and the information preserved.

This last reason leads us to error-correcting codes. This is a large and important group of codes with one specific ability: they can detect, and sometimes correct, corrupted messages. We say that a message is corrupted if we do not get the information encoded into the message back when decoding it.

One subclass of error-correcting codes is the block codes. To focus on and study the correspondences between codes and matroids in Section 3, we must first focus on and study block codes, and then more specifically their substructure: the linear codes. We will therefore in this section first focus on the basic definition of block codes and linear codes, before defining some essential properties of these two codes and how their structures function.

1.1 Block codes

Before defining block codes and their properties, we must first introduce two basic definitions:

Definition 1.1. An alphabet A is a finite set of symbols.

The symbols of an alphabet may be the letters in the Norwegian alphabet, a certain set of numbers, or any other arbitrary set of symbols.

Definition 1.2. $\mathbb{F}_q$ is a finite field with q elements, where q is a prime power, i.e. $q = p^e$.

By using these two notations we can define block and linear codes.

Definition 1.3. A block code C is the n'th product of an alphabet A, i.e. $C = A^n$.

Remark. If $A = \mathbb{F}_q$ and C is an $\mathbb{F}_q$-linear subspace of $(\mathbb{F}_q)^n$, then we call C a linear code and we write $C \subseteq (\mathbb{F}_q)^n$.

All linear codes have some of the same basic properties. Here we fix some of these notations:

Definition 1.4. The length of a linear code is n, i.e. the length of all codewords in C is n.

Definition 1.5. The dimension of a linear code C is its dimension as a vector space over $\mathbb{F}_q$ and is denoted by k.

Definition 1.6. The cardinality of a block code $|C| = M$ is the total number of codewords in the block code. The total number M of vectors in a linear code C over $\mathbb{F}_q$ of dimension k is then q^k.

For simplicity, when mentioning codes from now on, we will always either mean block codes or their subgroup linear codes. Furthermore, to avoid any confusion, we will denote the general block codes as C_B and the more specific linear codes as C_L.

1.2 Minimum distance

One of the most important properties of block codes; especially linear codes, is the "distance" between codewords. This property is highly important because the minimum distance between all codewords allows us to say something about the number of errors the message can have before we no longer can fix or detect them.

To begin studying this property we first have to define the difference between two different codewords. Richard Hamming, therefore, introduced the concept of Hamming distances which is one way of defining the difference between two codewords.

Definition 1.7. The Hamming distance d between two codewords $\mathbf{w}_1 = (x_1, x_2, ..., x_n)$ and $\mathbf{w}_2 = (y_1, y_2, ..., y_n)$ in C_B is:

$$d(\mathbf{w}_1, \mathbf{w}_2) = |\{i : x_i \neq y_i\}|$$

This means that the distance between two codewords is defined as the number of indexes where the values between the two codewords are different. From this, we can then define what the minimum distance of a code C_B must be.

Definition 1.8. The minimum distance of a code C_B is:

$$d(C_B) = d = min\ d(\mathbf{w}_1, \mathbf{w}_2), \forall \mathbf{w}_1, \mathbf{w}_2 \in C$$

We generally denote a linear code C_L, with values n, k and d, by $[n, k, d]$-code, we can also omit d, and just write $[n, k]$-code.

1.3 Support and Weight

The definition of the Hamming distance d of a code C_L naturally leads us to the definitions of support and weight of a codeword, as well as of a subset of $(\mathbb{F}_q)^n$.

First, we define the support as the set of indexes in a codeword where the value of the index is not equal to zero:

Definition 1.9. The support of an element $\mathbf{x} = (x_1, x_2, ..., x_n) \in (\mathbb{F}_q)^n$ is:

$$Supp(\mathbf{x}) = \{i : x_i \neq 0\}$$

The weight is then defined as the cardinality of the support:

Definition 1.10. The weight of an element $\mathbf{x} = (x_1, x_2, ..., x_n) \in (\mathbb{F}_q)^n$ is:

$$w(\mathbf{x}) = |Supp(\mathbf{x})| = |\{i : x_i \neq 0\}|$$

Remark. Finding the weight of a codeword is the same as finding the distance between the vector $\mathbf{x}$ and the zero vector $\mathbf{0}$, i.e. $d(\mathbf{x}, 0) = w(\mathbf{x})$.

Furthermore, we can then define the support for a subset X of $(\mathbb{F}_q)^n$:

Definition 1.11. The support of a subset $X \subset (\mathbb{F}_q)^n$ is:

$$Supp(X) = \bigcup_{\mathbf{x} \in X} Supp(\mathbf{x})$$

Once again, the weight of the subset X is the cardinality of its support:

Definition 1.12. The support weight of a subset $X \subset (\mathbb{F}_q)^n$ is:

$$\begin{aligned} w(X) &= |Supp(X)| \\ &= |\bigcup_{\mathbf{x} \in X} Supp(\mathbf{x})| \end{aligned}$$

Remark. In particular, these two definitions apply to a linear code $(X =)C_L$ and its codewords $(\mathbf{x} =)\mathbf{w}$.

Definition 1.13. The minimum distance $d(C_L)$ for a linear code is equal to the minimum weight of a non-zero codeword in C_L.

Proof. Assume $\mathbf{w}_1 = (x_1, x_2, ..., x_n), \mathbf{w}_2 = (y_1, y_2, ..., y_n) \in C_L$ and that $\mathbf{w}_{min}$ is a non-zero element of C_L of minimum weight.

$$\begin{aligned} d(C_L) &= min\ d(\mathbf{w}_1, \mathbf{w}_2) \\ &= min\{d((x_1, ..., x_n), (y_1, ..., y_n))\} \\ &= min\{d((x_1 - y_1, ..., x_n - y_n), (0, \cdots, 0))\} \\ &= min\{d((z_1, ..., z_n), \mathbf{0})\} \\ &= min\{d(\mathbf{w}, \mathbf{0})\} \text{ for } \mathbf{w} \in \mathbf{C} \\ &= d(\mathbf{w}_{min}, \mathbf{0}) \end{aligned}$$

Hence $d(C_L) = d(\mathbf{w}_{min}, \mathbf{0}) = w(\mathbf{w}_{min}) = min\ w(\mathbf{w})$, for $\mathbf{w} \in \mathbf{C}, \mathbf{w} \neq \mathbf{0}$. □

The minimum distance $d(C_B) = d$ of a code can be used to determine the number

of errors that can occur before we no longer can detect or correct the errors. A code will be able to detect up to $d-1$ errors and fix up to $\lfloor \frac{d-1}{2} \rfloor$ errors (Johnsen and Verdure, 2013, pp. 16-17).

1.4 Hamming weights

Using the definitions above we can generalize the idea of Hamming distance d to a larger set of Hamming weights d_i, where i is a value from 1 to k, and where k is the dimension of the code.

Definition 1.14. The i'th generalized Hamming weight $d_i = d_i(C_L)$ is $d_i = min\ w(U_i)$, where the minimum is taken over all linear subspaces $U_i \subseteq C_L$ of dimension i. In other words:

$$d_i(C_L) = d_i = min\{w(U_i) : U_i \subseteq C_L\}$$

Wei (1991, p. 1412).

Remark. This clearly gives two important remarks:

The original minimum Hamming distance d of a code defined in Definition 1.13 is equal to the 1st Hamming weight d_1.

$$d_1 = min\ w(U_1) = d$$

If C is a non-degenerate code; meaning that the $Supp(C_L) = \{1, .., n\}$ and $dim_{\mathbb{F}_q}(C_L) = k$, then the following is true:

$$d_k = min\ w(U_k) = min\ w(C_L) = n$$

Theorem 1.15. *For an $[n, k]$ linear code C_L with $k > 0$, we have*

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

Theorem 1.15 covering strict inequalities show that there is a weight hierarchy of

which there is a continuous increase in the value of the Hamming weights when the value of i increases. The proof of this can be found in Wei (1991, p. 1412).

1.5 Orthogonality

One important aspect of vectors in a vector space is the notion of orthogonality. Two vectors $\mathbf{x}$ and $\mathbf{y}$ in a vector space $(\mathbb{F}_q)^n$ are said to be orthogonal if the scalar product between them is zero. This definition can then be used to define an orthogonal complement C_L^* to a linear code $C_L \subseteq (\mathbb{F}_q)^n$.

Definition 1.16. The orthogonal complement C_L^* is the set of $\forall \mathbf{v} \in (\mathbb{F}_q)^n$ such that $\mathbf{v}$ is orthogonal to $\forall \mathbf{w} \in C_L$. This means $\sum_{i=1}^{n} \mathbf{v}_i \mathbf{w}_i = 0$ for all $\mathbf{v} \in C_L$, and $\mathbf{w} \in C_L^*$.

From this we can immediately define the word length and dimension of the orthogonal code, but not the minimum distance.

Definition 1.17. The length of the codewords in the orthogonal complement is n.

Definition 1.18. The dimension of the orthogonal complement is $n - k$.

Proof. The codewords of C_L^* come from the same vector space as the codewords of C_L come from, and they must therefore have the same length.

The dimension of the dual code C_L^* determines the number of independent linear equations that the codewords of C_L must satisfy, and must therefore be the total dimension minus the dimension of C_L. □

1.6 Wei-duality for Codes

To find the minimum distance of the orthogonal code C_L^* we must use the Hamming weights described in Definition 1.14.

The Hamming weights for the orthogonal complement C^* are denoted as d_i^*, with $1 \leq i \leq n - k$. From this, we can formulate the Wei-Duality theorem regarding the Hamming weights to a linear code C and its orthogonal complement.

Theorem 1.19.

$$\{d_i : 1 \leq i \leq k\} = \{1, 2, ..., n\} \setminus \{n + 1 - d_i^* : 1 \leq i \leq n - k\}$$

Wei (1991, p. 1413)

Remark. By knowing all $d_i, 1 \leq i \leq k$ we can then find all $d_i^*, 1 \leq i \leq n - k$. This again implies the strict inequalities in Theorem 1.15.

Example

Let C_L be a $[15, 11]$-code, with weight hierarchy {3, 5, 6, 7, 9, 10, 11, 12, 13, 14, 15}. Its complementary is then $\{1, 2, 4, 8\}$. Using Theorem 1.19, we get that the weight hierarchy of d_i^* will be $\{8, 12, 14, 15\}$ (Wei, 1991, p. 1413).

2 Matroids

A matroid M is defined as a pair $(E, \mathcal{X})$, where E is the ground set containing all elements of the matroid, and $\mathcal{X}$ is usually a family of subsets of the power set $P(E) = 2^E$. If $\mathcal{X}$ is not a family of subsets, then $\mathcal{X}$ can also be operations like a function. The family or function $\mathcal{X}$ defines the structure of the matroid M, while the ground set defines which elements this structure works over. Matroids can be defined by several different sets of axioms through $\mathcal{X}$. In this text, we are going to give five different constructions of the matroid M through $\mathcal{X}$ and their respective axiom sets. We have to a great extent given our own proofs for why the axiom sets are equivalent, although these equivalences have already been proven by other authors. We will refer to other authors in the cases where arguments are taken directly from them. Furthermore, we are going to give four examples of more specific matroids: those who are representable over a field, graphical matroids, uniform matroids, and connected matroids. From there, we will define some specific properties and operations correlated to matroids. Lastly, we are also going to look at a feature among matroids that corresponds to the orthogonality of linear codes: The dual matroid.

2.1 Representable matroids

Just as block codes can be defined as linear codes if the alphabet is a subspace of a vector space V, matroids can also be given a more specific definition if we define them over a field. If the elements of the ground set E are equivalent to any finite subset of a vector space V, we call the matroid representable. If the vector space $V = (\mathbb{F}_q)^n$ we say that the matroid is representable over $\mathbb{F}_q$ (Johnsen and Verdure, 2013, p. 82).

Remark. Obviously, any matroid defined over a matrix A with entries in a field $\mathbb{F}_q$ will then be representable over the field used. The vectors used in the ground set E are then the column vectors in the matrix. We denote these matroids as $M[A] = (E, \mathcal{X})$.

2.2 Graphic matroids

A matroid is defined as a graphic matroid if the elements of its ground set E can be defined as the edges of a graph, which therefore makes $\mathcal{X}$ fulfill the different axiom sets defined in subsections 2.3, 2.4, 2.5, 2.6 and 2.7 (Johnsen and Verdure, 2013, p. 95).

Remark. This obviously leads us to the conclusion that any matroid M created from a graph is a graphic matroid.

2.3 Independent sets

The first definition of a matroid that we will give, focuses on the notion of linear independence from linear algebra. Whitney defined these matroids in 1935 using what is now known as representable matroids. Hassler saw that all sets of column vectors from a given matrix A could be categorized into one of two different classes: those that are linearly independent and those that are linearly dependent. By renaming each column vector in the matrix A from 1 to n we can create the ground set E using this new enumeration. By then creating a set containing all the independent sets, we can denote this new family of sets as $\mathcal{I}$ and see that it will follow these three properties:

(I1) The empty set is always independent, i.e. $\emptyset \in \mathcal{I}$

(I2) Every subset of an independent set is also independent, i.e. $I_1 \subset I_2 \subset E \ \& \ I_2 \in \mathcal{I} \Rightarrow I_1 \in \mathcal{I}$

(I3) If $I_1, I_2 \in \mathcal{I} \ \& \ |I_1| > |I_2| \Rightarrow \exists x \in I_1 \setminus I_2$ such that $I_2 \cup \{x\} \in \mathcal{I}$

Whitney (1935, p. 509)

By generalizing the notion of matroids from just representable matroids, these three properties can then be seen as an axiom set for any matroid $M = (E, \mathcal{I})$. They can then be used to check whether or not any set $\mathcal{I}' \subset P(E)$ can be used to create a matroid $M' = (E, \mathcal{I}')$.

Example

We can show the creation of a matroid over $\mathbb{F}_2$ using its linear independent sets from the following matrix:

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

By denoting the first column vector as 1, the second as 2, and so on until the last column 5, we can list all the independent sets in $\mathcal{I} = \{\emptyset, \{1\}, \{2\}, \{3\}, \{4\}, \{5\}, \{1,2\}, \{1,3\}, \{1,4\}, \{1,5\}, \{2,3\}, \{2,4\}, \{2,5\}, \{3,4\}, \{3,5\}, \{4,5\}, \{1,2,3\}, \{1,2,5\}, \{1,3,4\}, \{1,4,5\}, \{2,3,4\}, \{2,3,5\}, \{3,4,5\}\}$. We see that the set containing all column vectors is not included, just as the set containing column vectors 1, 2 and 4 is not. This is because these are obviously dependent, and therefore cannot be contained in the set of independent sets.

2.4 Bases

Another way to define a matroid M is by not listing all independent sets $I \in \mathcal{I}$, but rather defining the inclusion maximal independent sets $B \in \mathcal{I}$. From these bases B we can create a new set of sets $\mathcal{B}$ which contains all bases of E. One obvious conclusion from this is that $\mathcal{B} \subseteq \mathcal{I}$ and we can therefore define the set of bases as:

Definition 2.1. $\mathcal{B} = \{B \subset E : \ B \text{ is inclusion maximal independent}\}$

One special feature of the bases of a matroid is given in the following proposition.

Proposition 2.2. All bases $B \in \mathcal{B}$ have the same cardinality.

Proof. Assume that for $B_1, B_2 \in \mathcal{B}$ we have that $|B_1| < |B_2|$. By (I3) $\exists x \in B_2 \setminus B_1$ such that $B_1 \cup \{x\} \in \mathcal{I}$. This means that there exists an element that we can add to an inclusion maximal independent set B_1, and still keep it an independent set. This is a contradiction to B_1's construction. Therefore, all $B_i \in \mathcal{B}$ must have the same cardinality (Johnsen and Verdure, 2013, p. 84). □

This allows us to rewrite Definition 2.1 to the following proposition:

Proposition 2.3. $\mathcal{B} = \{B \subset E : \ |B| = max|I|, I \in \mathcal{I}\}$

Furthermore, using propositions 2.2 and 2.3, as well as the axiom set of independent sets given in Subsection 2.3, we get the following propositions for the set of bases $\mathcal{B}$:

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

(B2) If $B_1, B_2 \in \mathcal{B}$ & $x \in B_1 \setminus B_2$ *then* $\exists y \in B_2 \setminus B_1$ *such that* $B_1 \setminus \{x\} \cup \{y\} \in \mathcal{B}$

Proof. The first property (B1) is obvious and follows immediately from (I1). Since $\emptyset \in \mathcal{I}$, and $\mathcal{B}$ are the maximal independent sets in $\mathcal{I}$, then $\mathcal{B}$ cannot be empty.

To prove (B2) we first have to assume that B_1 and B_2 are two distinct bases of a matroid M. Let $x \in B_1 \setminus B_2$, then we have $|B_1 \setminus \{x\}| = |B_1| - 1 = |B_2| - 1 < |B_2|$ from (I3). Thus, there has to exist $y \in B_2 \setminus (B_1 \setminus \{x\}) = B_2 \setminus B_1$ such that $B_1 \setminus \{x\} \cup \{y\}$ is independent. Since $|B_1 \setminus \{x\} \cup \{y\}| = |B_1| = |B_2|$ it also has to be a basis and (B2) is proven (Johnsen and Verdure, 2013, p. 84). □

The properties of the set of bases $\mathcal{B}$ can be used as an axiom set for a matroid $M = (E, \mathcal{B})$, and we can then use them to prove that the axiom set for independent sets follow as properties:

Proof. To begin, we must redefine $\mathcal{I}$ using $\mathcal{B}$ as $\mathcal{I} = \{I \subseteq B : B \in \mathcal{B}\}$.

(I1) is obvious from (B1). Since there is at least one element in $B \in \mathcal{B}$ and $\emptyset \subseteq B$, $\emptyset$ has to be independent.

(I2), like (I1) is also obvious. Assume we have $I_1 \subseteq E$ which is independent, then there has to exist at least one $B \in \mathcal{B}$, where $I_1 \subseteq B$. Any subset I_2 of I_1 will then also be a subset of B, which again leads to that I_2 must be independent since there are no dependent elements in B.

(I3) can be proven by assuming we have $I_1 \subseteq B_1$, $I_2 \subseteq B_2$ and $|I_1| < |I_2|$. Due to (B2) we know that there exists an $x \in B_1 \setminus B_2$ and $y \in B_2 \setminus B_1$ such that $B_1 \setminus \{x\} \cup \{y\} \in \mathcal{B}$. We know that each subset of this will also be independent, as

proved right above. $I_1 \setminus \{x\} \cup \{y\}$ is obviously a subset of $B_1 \setminus \{x\} \cup \{y\} \in \mathcal{B}$ and it is, therefore, an independent set. By the generality of the creation of I_1 and I_2, it can then be assumed that $x \notin I_1$ and $y \in I_2$, and thus (I3) has been proven. $\square$

We can therefore say that a matroid M with ground set E can either be defined using all its independent sets or just its maximal inclusion independent sets. Therefore, a matroid can be given equivalent definitions $M = (E, \mathcal{I})$ or $M = (E, \mathcal{B})$, depending on which axiom set we chose to focus on.

Example

By continuing to use the example from Subsection 2.3 we see that the bases of the matroid are $\mathcal{B} = \{\{1,2,3\}, \{1,2,5\}, \{1,3,4\}, \{1,4,5\}, \{2,3,4\}, \{2,3,5\}, \{3,4,5\}\}$. These seven sets contain all independent sets as subsets of themselves.

2.5 Rank function

A third way to define a matroid is by using its rank function r. To study matroids in regard to the rank function, the rank function must first be defined.

Definition 2.4. The rank function of a matroid M is defined for a subset X of E as the maximum cardinality of an independent set contained in X.

$$\begin{aligned} r : 2^E &\longrightarrow \mathbb{N} \\ X &\longmapsto Max\{|I| : I \subset X, I \in \mathcal{I}\} \end{aligned}$$

It can then be proven that the rank function will satisfy the following properties:

(R1) $0 \leq r(X) \leq |X|, \forall X \in E$

(R2) If $X \subseteq Y \subseteq E \Rightarrow r(X) \leq r(Y)$

(R3) If $X, Y \subset E \Rightarrow r(X) + r(Y) \geq r(X \cup Y) + r(X \cap Y)$

Proof. The first property (R1) comes directly from the definition of the rank function as the cardinality of the biggest independent set contained in another set. This can at most be the cardinality of the set, and at least be the cardinality of the empty set which is zero.

The second property is also easily proven. Assume we have two sets $X \subseteq Y \subseteq E$. Further assume that I_X is the largest independent subset of X, in other words, $r(X) = |I_X|$. Now, since $X \subseteq Y$, we have two current situations. The first is when I_X is also the largest independent subset of Y, then $r(Y) = r(X) = |I_X|$. The second is when $\exists I_Y \subseteq Y$, which is a larger independent set in Y than I_X. Then it is clear that $r(Y) = |I_Y| > |I_X| = r(X)$.

The last property (R3) can be proven by using three bases X, Y, and Z of the sets $A \cap B, A, A \cup B \in E$ respectively. Given (I2) we can clearly choose Y and Z such that X extends into them and we get $X \subset Y$ and $X \subset Z$. $B = A \cap B \cup (B \setminus A) = A \cap B \cup ((A \cup B) \setminus A) \supset X \cup (Z \setminus Y)$ By then using (R2) we get:

$$\begin{aligned} r(B) &\geq r(X \cup (Z \setminus Y)) \\ r(B) &\geq r(X) + r(Z \setminus Y) \\ r(B) &\geq r(X) + r(Z) - r(Y) \\ r(B) &\geq r(A \cap B) + r(A \cup B) - r(A) \\ r(A) + r(B) &\geq r(A \cup B) + r(A \cap B) \end{aligned}$$

And (R3) is proven (Wilson, 1979, p. 134). □

These three properties can also be used as an axiom set for the matroid $M = (E, r)$ and we can use them to prove that the axiom set for independent sets follows as properties as well.

Proof. First, we redefine $\mathcal{I}$ as $\mathcal{I} = \{I \subset E : r(I) = |I|\}$.
(I1) is obvious since $r(\emptyset) = 0 = |\emptyset|$, which is the definition of an independent set.

(I2) is easily proven using (R2). If you have $X \subset I$ and I, is independent, then $r(I) = |I|$, and for each element removed from I to get X you have to remove one

from $r(I)$, which leads to $r(X) = |X|$. Thus X is independent.

(I3) can be proven by taking independent sets I_1, I_2 with $|I_1| < |I_2| \Rightarrow r(I_1) < r(I_2)$, and $r(I_1) = k$. We now assume that $\forall x \in I_2 \setminus I_1$, we have $r(I_1 \cup \{x\}) = k$, i.e. there $\nexists x \in I_2$ such that $I_1 \cup \{x\} \in \mathcal{I}$. By using (R3) it is easy to show that by adding $\{y\} \in I_2 \setminus I_1$ to $I_1 \cup \{x\}$ we continue to get $r(I_1 \cup \{x\} \cup \{y\}) = k$, by continuing to do this until all $z \in I_2 \setminus I_1$ have been used, we can conclude that $r(I_1 \cup I_2) = k = r(I_1)$. Thus $r(I_2) \leq r(I_1 \cup I_2) = k$ which is a contradiction. Therefore, there has to $\exists x \in I_2 \setminus I_1$ such that $r(I_1 \cup \{x\}) = k + 1$ (Wilson, 1979, p. 134). □

We can now redefine $\mathcal{B}$ using the rank function r:

Definition 2.5. $\mathcal{B} = \{B \subset E : r(B) = |B| = r(E)\}$

We can then also use the set of bases $\mathcal{B}$ to define the rank function:

Definition 2.6.

$$\begin{aligned} r : 2^E &\longrightarrow \mathbb{N} \\ X &\longmapsto Max\{|X \cap B| : B \in \mathcal{B}\} \end{aligned}$$

Therefore, a matroid can be given equivalent definitions $M = (E, \mathcal{I})$, $M = (E, \mathcal{B})$, or $M = (E, r)$, depending on which axiom set we chose to focus on.

Example

Using the example from Subsection 2.3 we see that the rank of the matroid is $r(M) = r(E) = r(B) = 3$, and that the rank of all sets varies from 0 til 3 depending on their dependency and cardinality. Furthermore, all sets with a cardinality of two or less have $r(X) = |X|$, which means that they have to be independent, and since the maximal rank is 3, any set with a cardinality higher than 3 will therefore be dependent.

2.6 Circuits

Up until now, we have used matroids to study independence, but we can also use matroids to study dependence. One of these dependencies is the minimally dependent sets, also known as circuits C. The circuits are collected in the set of sets $\mathcal{C}$.

Definition 2.7. $\mathcal{C} = \{C \subset E : C \text{ is minimal inclusion dependent}\}$

Remark. One special type of circuit is the loop; these are circuits containing only one element.

The set $\mathcal{C}$ can then be proven to possess the following properties:

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

(C2) If $C_1 \subsetneq C_2 \in \mathcal{C} \Rightarrow C_1 \notin \mathcal{C}$

(C3) If $C_1, C_2 \in \mathcal{C}$ & $c \in C_1 \cap C_2 \Rightarrow \exists C_3 \subset C_1 \cup C_2 \setminus \{c\}$ such that $C_3 \in \mathcal{C}$

Proof. The first two properties can be trivially proven using (I1) as $\emptyset \in \mathcal{I} \Rightarrow \emptyset \notin \mathcal{C}$, and due to minimality of $C \in \mathcal{C}$, no subset of C can be dependent.

The last property (C3) can be proved by using (R3). We assume the opposite, that there exists no C_3 which can be created from two circuits C_1 and C_2. This obviously means that $C_1 \cup C_2 \setminus \{c\}$ is independent and that $r(C_1 \cup C_2 \setminus \{c\}) = |C_1 \cup C_2 \setminus \{c\}| = |C_1 \cup C_2| - 1 = r(C_1 \cup C_2)$. Using (R3):

$$\begin{aligned} r(C_1 \cup C_2) + r(C_1 \cap C_2) &\leq r(C_1) + r(C_2) \\ |C_1 \cup C_2| - 1 + |C_1 \cap C_2| &\leq |C_1| - 1 + |C_2| - 1 \\ |C_1 \cup C_2| + |C_1 \cap C_2| - 1 &= |C_1| + |C_2| - 2 \\ |C_1| + |C_2| - |C_1 \cap C_2| + |C_1 \cap C_2| - 1 &= |C_1| + |C_2| - 2 \\ |C_1| + |C_2| - 1 &= |C_1| + |C_2| - 2 \end{aligned}$$

This is a contradiction and there must therefore exist a circuit in $C_1 \cup C_2 \setminus \{c\}$ (Johnsen and Verdure, 2013, p. 92-93). □

Once again, these properties can be used as an axiom set for a matroid $M = (E, \mathcal{C})$

and can be used to show that the axiom set for independent sets follows as a set of properties.

Proof. First we redefine $\mathcal{I}$ as $\mathcal{I} = \{I \subset E : \nexists C \subset I \text{ such that } C \in \mathcal{C}\}$.

(I1) is trivially proven, as the empty set has no subsets and is therefore not a circuit. Because of this it is not a dependent set and must be independent.

(I2) is proven by assuming $X \subseteq I$ and I independent. By then assuming that X is dependent, there must $\exists C \subset X, C \in \mathcal{C}$. From this I must also obviously contain C and therefore also be dependent, which is a contradiction.

(I3) is a bit harder to prove. The concept is that by assuming that (I3) does not hold, we can construct independent sets X and Y which together can be used to show several contradictions which lead to the only conclusion being that (I3) has to hold. A full proof can be found in (Johnsen and Verdure, 2013, p. 93-94). □

Once again we can redefine $\mathcal{B}$ and r using $\mathcal{C}$:

Definition 2.8. $\mathcal{B} = \{\text{inclusion maximal}(B \subset E) : C \not\subseteq B, C \in \mathcal{C}\}$

Definition 2.9.

$$\begin{aligned} r : 2^E &\longrightarrow \mathbb{N} \\ X &\longmapsto Max\{|A| : A \subseteq X, C \not\subseteq A, C \in \mathcal{C}\} \end{aligned}$$

We can also define $\mathcal{C}$ using $\mathcal{B}$ and r:

Definition 2.10. $\mathcal{C} = \{\text{inclusion minimal}(C \subset E) : C \not\subseteq B, B \in \mathcal{B}\}$

Definition 2.11. $\mathcal{C} = \{C \subset E : r(C) = |C| - 1 \ \ \& \ \ r(A) = |A|, \forall A \subsetneq C\}$

Once again, a matroid can be given equivalent definitions $M = (E, \mathcal{I})$, $M = (E, \mathcal{B})$, $M = (E, r)$, or $M = (E, \mathcal{C})$, depending on which axiom set we chose to focus on.

Example

Following the same example from Subsection 2.3 it is clear to see that the only circuits contained in $\mathcal{C}$ are $\{1,2,4\}$ and $\{1,3,5\}$. This is due to the fact that there are only two dependent sets X with a rank $r = |X| - 1$.

2.7 Dependent sets

Another way to define matroids using dependence is to look at not the inclusion minimal dependent sets, but just the dependent sets D. The relation between D and C is similar, albeit the other way, to the relation between I and B. The sets D are all dependent sets and therefore contained in the set of sets $\mathcal{D}$.

Definition 2.12. $\mathcal{D} = \{D \subset E : D \text{ is dependent}\}$

The set $\mathcal{D}$ will then have the following properties:

(D1) $\emptyset \notin \mathcal{D}$

(D2) If $D_1 \in \mathcal{D}$ and $D_1 \subset D_2, \Rightarrow D_2 \in \mathcal{D}$

(D3) If $D_1, D_2 \in \mathcal{D} \Rightarrow D_1 \cap D_2 \in \mathcal{D}$ or $(D_1 \cup D_2) \setminus \{e\} \in \mathcal{D}\ \forall e \in D_1 \cap D_2$

Proof. The first property is proven using (I1). Since $\emptyset \in \mathcal{I} \Rightarrow \emptyset \notin \mathcal{D}\}$.

The property (D2) is proven as adding any element to a dependent set cannot make that same set independent and it must therefore be dependent.

The third property can be proven using (C3). Assume $C_1 \subseteq D1\ \ \&\ \ C_2 \subseteq D_2$ then we have either $D_1 \cap D_2 \in \mathcal{D}$ or $(D_1 \cup D_2) \setminus \{e\} \in \mathcal{D}\ \forall e \in D_1 \cap D_2$. Starting with $C_1 = C_2 \Rightarrow D_1 \cap D_2 \in \mathcal{D}$. On the other hand, if $C_1 \neq C_2$ we know from (C3) that there exists $e \in C_1 \cap C_2$ such that $C_3 \subseteq C_1 \cup C_2 \setminus \{e\} \subseteq D_1 \cup D_2 \setminus \{e\}$,which means that for all $e \in D_1 \cap D_2$ there will exist at least one circuit in $D_1 \cup D_2 \setminus \{e\}$, which leads it to being dependent. □

Again, this set of axioms for a matroid $M = (E, \mathcal{D})$ can be used to prove the axiom set for independent sets.

Proof. First we redefine $\mathcal{I}$ as $\mathcal{I} = \{I \subset E : I \notin \mathcal{D}$.

(I1) is trivially proven, just as with (D1). If $\emptyset \notin \mathcal{D}$ then it has to be independent.

(I2) and (I3) are proven using the same arguments and structure as for (C2) and (C3).

□

For the last time we will redefine $\mathcal{B}$, r and $\mathcal{C}$ using $\mathcal{D}$:

Definition 2.13. $\mathcal{B} = \{\text{inclusion maximal}(B \subseteq E) : D \not\subseteq B, D \in \mathcal{D}\}$

Definition 2.14.

$$\begin{aligned} r : 2^E &\longrightarrow \mathbb{N} \\ X &\longmapsto Max\{|A| : A \subseteq X, D \not\subseteq A, D \in \mathcal{D}\} \end{aligned}$$

Definition 2.15. $\mathcal{C} = \{C \subseteq E : |C| = min|D|, D \in \mathcal{D}\}$

We can also define $\mathcal{D}$ using $\mathcal{B}$, r and $\mathcal{C}$:

Definition 2.16. $\mathcal{D} = \{D \subseteq E : D \not\subseteq B, B \in \mathcal{B}\}$

Definition 2.17. $\mathcal{D} = \{D \subseteq E : r(D) < |D|\}$

Definition 2.18. $\mathcal{D} = \{D \subseteq E : \exists C \in \mathcal{C}, C \subseteq D\}$

Therefore, a matroid can be given equivalent definitions $M = (E, \mathcal{I})$, $M = (E, \mathcal{B})$, $M = (E, r)$, $M = (E, \mathcal{C})$, or $M = (E, \mathcal{D})$, depending on which axiom set we chose to focus on.

Example

Once again, using the example in Subsection 2.3, we see that the dependent sets are {1, 2, 4}, {1, 3, 5}, {1, 2, 3, 4}, {1, 2, 4, 5}, {1, 3, 4, 5}, {1, 3, 4, 5}, {2, 3, 4, 5} and {1, 2, 3, 4, 5}. As we see, all sets of cardinality higher than 3 are dependent, as well as the circuits of the matroid.

2.8 Equivalence proof

As we have seen until now, all five axiom sets can be used to define the four other axiom sets as properties. This means that all axiom sets are equal to each other, and it, therefore, does not matter which set we use to prove that something is a matroid, or which axiom set we use to define specific properties of the given matroid.

2.9 Dual matroid

In the same way that linear codes C_L have an orthogonal complement C_L^*, so do matroids M have a dual matroid M^*. The dual matroid is defined using the base sets B from the matroid $M = (E, \mathcal{B})$. We then define the new set $\mathcal{B}^*$ as follows:

Definition 2.19. $\mathcal{B}^* = \{E \setminus B : B \in \mathcal{B}\}$

This results in $\mathcal{B}^*$ containing all the complementary sets to $\mathcal{B}$. By this definition, $M = (E, \mathcal{B}^*)$ is indeed a matroid and it can be verified that it follows the axiom sets given in the Subsections 2.3 through 2.7 above. This matroid is denoted M^* and is called the dual matroid of M (Johnsen and Verdure, 2013, p. 100).

Remark. Obviously, from this definition, the dual matroid of the dual matroid is the matroid itself, i.e. $(M^*)^* = M$.

For further denotion we call all sets in the dual matroid; be them independent, bases, circuits, etc. the cosets of the matroid M. For example we have the cocircuits of M, which are the circuits of M^*.

Resulting from this, the rank function of the dual matroid is then:

$$r^*(X) = |X| + r(E \setminus X) - r(E) \tag{1}$$

The proof for this can be found in every standard textbook about matroids, but one proof that this is the rank function of the dual matroid can be found in Wilson (1979, p. 140).

2.10 Uniform matroids

A uniform matroid $U_{r,n}$ is a matroid with the following properties:

1. It is defined over a set of n elements.
2. A subset of the n elements are independent if and only if there are at most r elements. Furthermore, this means that a subset is a basis if it contains r elements, and that all circuits contain exactly $r + 1$ elements.

Therefore, any matroid with rank r is a uniform matroid if and only if all circuits have a cardinality of $r + 1$.

Furthermore, the dual matroid of a uniform matroid is $U_{n-r,n}$ which is itself also a uniform matroid.

Remark. It is clear to see that a uniform matroid will be its own dual matroid if the rank of the uniform matroid is exactly half of the number of elements in its ground set.

2.11 Connected matroids

A connected matroid is defined as a matroid where for every pair of elements a, b in the ground set E, there exists at least one circuit containing both elements.

$$\forall e_1, e_2 \in E, \exists C \in \mathcal{C} \text{ such that } \{e_1, e_2\} \in C$$

(Johnsen and Verdure, 2013, p. 133).

Furthermore, a matroid for which this is not true is called a disconnected matroid. The disconnected matroids can also be defined by the direct sum $\oplus$ of two or more connected matroids $M = M_1 \oplus M_2 \oplus ... \oplus M_i$. For simplicity, we will focus on $M = M_1 \oplus M_2$, but the case of the general i can be described by iterating this sum.

A matroid $M = M_1 \oplus M_2$ can therefore be defined by a disjoint union $E = E_1 \cup E_2$ and $\mathcal{I} = \{I_1 \cup I_2 : I_1 \in \mathcal{I}_1 \ \& \ I_2 \in \mathcal{I}_2\}$. To prove that this is in fact a matroid we look at the axiom set for the family of independent sets.

Proof. (I1) is easily proven as $\emptyset$ is independent in both M_1 and M_2 and is, therefore, a part of $\mathcal{I}$.

(I2) is proven by taking two subsets I_3 and I_4 of I_1 and I_2 respectively. As any subset of independent subsets are independent, we know that both I_3 and I_4, therefore, have to be independent. By defining $I' = I_3 \cup I_4$ we know that $I' = I_3 \cup I_4 \subseteq I_1 \cup I_2 = I$ is independent.

(I3) can be proven by assuming we have $I_x, I_y \in \mathcal{I}$ with $I_x = \{I_1 \cup I_2 : I_1 \in \mathcal{I}_1 \ \& \ I_2 \in \mathcal{I}_2\}, I_y = \{I_3 \cup I_4 : I_3 \in \mathcal{I}_1 \ \& \ I_4 \in \mathcal{I}_2\}$. If we further assume $|I_x| > |I_y|$, then this means that $|I_1| > |I_3|$ and/or $|I_2| > |I_4|$. We choose to focus on $|I_1| > |I_3|$, as it does not matter which of these are true. Since we then know that $\exists x \in I_1 \setminus I_3$, such that $I_3 \cup \{x\} \in \mathcal{I}_1$, this x also has to exist in $I_x \setminus I_y$, such that $I_y \cup \{x\} \in \mathcal{I}$. Thus we have proven (I3) (Johnsen and Verdure, 2013, p. 139). □

By this definition, it is clear that the bases of the disconnected matroid M must be $B = \{B_1 \cup B_2; B_1 \in \mathcal{B}_1 \text{ and } B_2 \in \mathcal{B}_2\}$ as they must be inclusion maximal independent in both sets. The circuits are the circuits in either M_1 or M_2, i.e. $C = \{C_1 \cup \emptyset; C_1 \in \mathcal{C}_1 \text{ or } \emptyset \cup C_2; C_2 \in \mathcal{C}_2\}$, since if it was dependent and it had contained one element or more instead of $\emptyset$, then there would have existed an x, such that we could have removed an element and still had a dependent set. The dependent sets are therefor $D = \{D \cup A; D \in \mathcal{D}_1 \ \& \ A \subseteq E_2 \text{ or } D \in \mathcal{D}_2 \ \& \ A \subseteq E_1\}$.

2.12 Simplification and cosimplification

Every matroid M can be simplified to create a new and "simpler" matroid $si(M)$. To do this one must follow these two defined steps.

1. Remove all loops, i.e. $\{e : r(e) = 0\}$
2. Simplify all parallel edges. For non-loops, this means to remove $s-1$-elements from $\{e_1, e_2, e_3, ..., e_s\}$ when $r(\{e_1, e_2, e_3, ..., e_s\}) = 1$. In other words, remove all but one edge which connects two vertices.

$si(M) = M|_X$, where X is the set of edges that remain after removing these loops

and parallel edges.

For graphic matroids, this has a very concrete and easy-to-illustrate meaning:

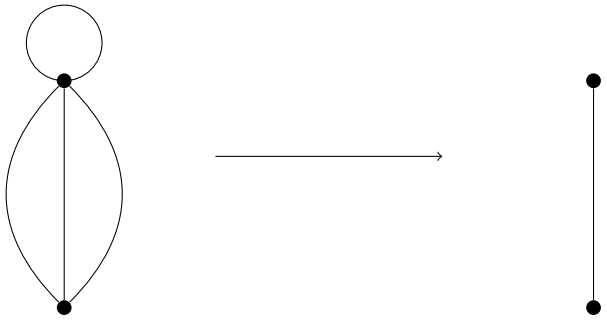

Figure 1: Simplification

Furthermore, the cosimplification of a matroid M is defined as $co(M) \equiv (si(M^*))^*$.

3 Codes and Matroids

As seen in Section 2 Subsection 2.1 we can create matroids M using a matrix. Furthermore, linear codes C_L as subspaces of $(\mathbb{F}_q)^n$ can be defined using what is called a generator matrix G. By combining these two aspects we can construct matroids $M_{C_L} = M[G]$ defined by a linear code. This matroid inherits some specific and important properties from the linear code it was defined by. By studying these matroids, one can therefore study and prove important theorems around linear codes as well. This chapter gives an overview of the creation of these matroids and the most important similarities between the matroids M_{C_L} and their linear codes C_L, as described in the literature. We will focus on definitions given in Johnsen and Verdure (2013).

3.1 Generator and parity-check matrices

Assume that C_L is a linear subspace of the vector space $(\mathbb{F}_q)^n$, then the entire code may be represented as a set of k vectors (codewords) which span C_L. These k vectors can be represented together as the rows of a matrix G, called a generator matrix for the code C_L. As there are several different linear systems of k vectors which can span C_L, there are also several different generator matrices for C_L. When a generator matrix takes the form $G = [I_k|A]$; where I_k is the identity matrix of size k and A is a matrix of size $k \times (n-k)$, we say that G is in standard form.

From this, we can then define the parity-check matrix as $H = [-A^T|I_{n-k}]$.

The orthogonal complement C_L^* also has generator matrices G^*. If C_L has a generator matrix on standard form $G = [I_k|A]$, then $G^* = H = [-A^T|I_{n-k}]$ is a generator matrix of C_L^*. Furthermore, the parity check matrix H^* of C_L^* is the generator matrix G of C_L.

3.2 Matroids from codes

From a generator matrix G corresponding to the linear code C_L, we can create a matroid M_{C_L}. The easiest way to visualize this matroid is either by the inde-

pendent sets $\mathcal{I}$ or by the inclusion maximal independent sets $\mathcal{B}$. To do this we use the columns of the generator matrix G as the elements of E and also use the definition of linear independence to decide if two columns are independent or not. The matroid generated by the orthogonal complement $M_{C_L^*}$ is similarly defined and is therefore created using a parity-check matrix of C_L.

The rank function can also be used in correlation to matroids created from linear codes. The rank r of a certain set of column vectors in the generator matrix will correspond to the rank r of the same set of elements in the ground set of the matroid.

Matroids created using linear codes over a field $\mathbb{F}_q$ are called representable over $\mathbb{F}_q$. Not all matroids are representable over a field, and therefore not all matroids can be used in relation to codes.

3.3 Matroid duality with respect to the orthogonal complement

One theorem that results from the definitions of matroids from linear codes is the theorem of duality. This states that:

$$M_{C_L^*} = (M_{C_L})^* \tag{2}$$

The proof for this theorem can be found in most standard textbooks about codes and matroids. The general outline of the proof is to show that $M_{C_L} = (M_{C_L^*})^*$, which we can then use to take the dual to get the result above. One such proof is given in Johnsen and Verdure (2013, pp. 107-108), but they have chosen to define M_{C_L} as $M[H]$ not $M[G]$. The proof is nevertheless similar in both build and argumentation as to what this would have been.

3.4 Codewords and the parity-check matrix

Since $rowspan(H) = C^*$, it is clear that:

$$C_L = \{\mathbf{w} \in (\mathbb{F}_q)^n : H \cdot \mathbf{w}^T = 0\} \tag{3}$$

This definition comes from the fact that any codeword $\mathbf{w} \in C_L$ is orthogonal on all codewords $\mathbf{v} \in C_L^*$.

From this, we can show that the minimum distance d of a code can be redefined as:

$$d = min\ \{s :\ s \text{ columns of } H \text{ are linearly dependent}\} \tag{4}$$

This can be proven as follows:

Proof. $H \cdot \mathbf{w}^T = \sum_{i=1}^{n}(w_i \cdot h_i)$, where h_i is the i'th column in H

By then removing every $w_i = 0$, it is obvious by definition that the remaining h_i with $c_i \neq 0$ have to be linearly dependent. Thus d is precisely the minimum number of linearly dependent column vectors in H (Johnsen and Verdure, 2013, p. 109). □

Since r^* refers to parity check matrices H, this automatically gives us that:

$$d = d_1 = min\ \{|X| : X \subset E\ \ \&\ \ r^*(X) < |X|\} \tag{5}$$

This can then be generalized to $d_i = min\ \{s :\ \text{such that } s \text{ columns in } H \text{ have } i \text{ linearly independent relations between them}\}$.

This again results in:

$$d_i = min\ \{|X| : X \subset E\ \ \&\ \ r^*(X) \leq |X| - i\} \tag{6}$$

4 Derived matroids

As seen in Section 2, a matroid is a mathematical structure used to study either dependency or independency within a ground set E. By focusing on the circuits of a matroid $M = (E, \mathcal{C})$, we can create a new ground set E' of which its elements are the circuits of the original matroid M. From this we can study dependencies among dependencies using the mathematical structure of derived matroids: δM.

Further, in this section, we will introduce three different concepts regarding derived matroids: $\delta_L M$ defined in Longyear (1980), $\delta_{OW} M$ defined in Oxley and Wang (2019), and $\delta_{FJK} M$ defined in Freij-Hollanti et al. (2023). Along the way, the similarities and differences between the concepts will be highlighted.

4.1 Longyear's approach

The first definition of a derived matroid we are going to focus on is taken from Longyear's article from 1979. The text focuses on a specific group of representable matroids used to define derived matroids, called binary matroids. These are matroids representable over $\mathbb{F}_2$.

The Kirchoff sum

To understand Longyear's definition we must first define *Kirchoff sums*. The *Kirchoff sum* of two subsets A and B is given as $A \triangle B = A \cup B \setminus (A \cap B)$. This gives us a new set that contains all elements either contained just in A or just in B. It can therefore also be written as $A \triangle B = (A \setminus B) \cup (B \setminus A)$. When adding a new set C, the *Kirchoff sum* between A, B and C will then be $A \triangle B \triangle C = (((A \setminus B) \cup (B \setminus A)) \setminus C) \cup (C \setminus ((A \setminus B) \cup (B \setminus A)))$. This will lead to a set which contains all elements in A and only A, B and only B, C and only C and those that are in all three (Longyear, 1980, p. 72). This can easily be shown using this illustration:

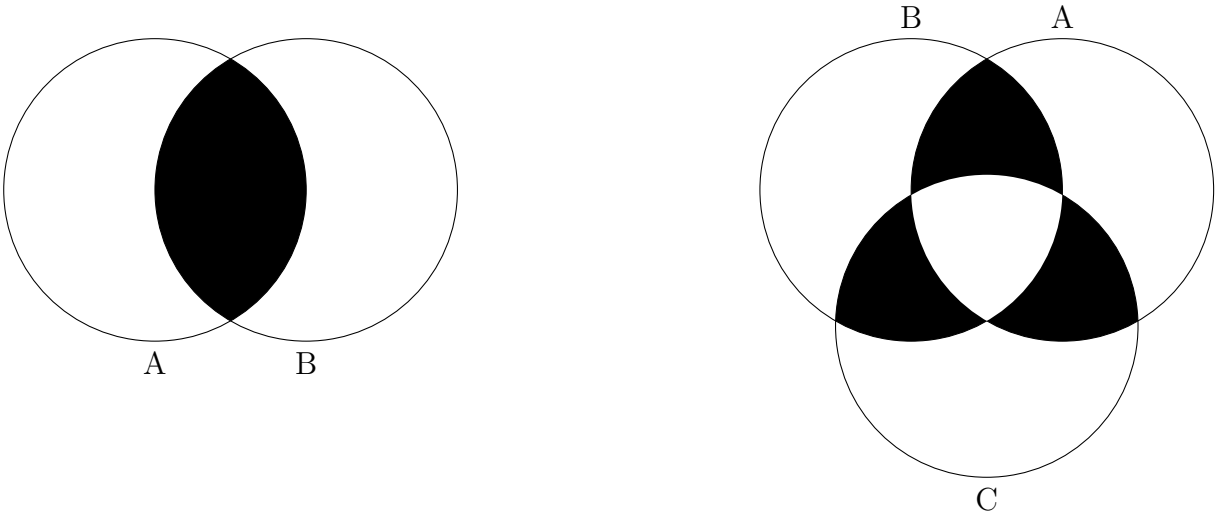

Figure 2: Kirchoff sum

The black areas are not included in the *Kirchoff sum*, while the white areas are included. This process can be continued with more and more sets, and we then get the generalized *Kirchoff sum* for n sets of A_i.

$$A_1 \triangle A_2 \triangle ... \triangle A_n = \{a \in \bigcup_{i=1}^{n} A_i : |\{A_i : a \in A_i\}| \text{ is odd}\}$$

The Kirchoff basis

Looking back at the definition of a matroid $M = (E, \mathcal{C})$ using circuits, we can define a *Kirchoff basis* using the *Kirchoff sum*. We say that the *Kirchoff basis* $\mathcal{K}$ is an inclusion minimal subset of circuits $\{C_1, C_2, ..., C_k\}$ of $\mathcal{C}$, such that every circuit in $\mathcal{C}$ can be described as a *Kirchoff sum* using any number of C_i from $\mathcal{K}$.

The derived matroid

The derived matroid $\delta_L M$ is a matroid that is defined by a new ground set E' in comparison to the ground set E of the original matroid M. The set E' is defined as the set of circuits of a matroid $M = (E, \mathcal{C})$. Any subset D' of E' is defined as dependent if there exists a non-empty subset C' of D' with its *Kirchoff sum*

equal to the empty set. In other words a set D' is dependent if $\exists\{C_1, C_2, ..., C_k\} \subset D'$ such that $C_1 \triangle C_2 \triangle ... \triangle C_k = \emptyset$. Any subset I' is defined as independent if it is not dependent. Furthermore, any circuit C' is just a dependent set D' of which the circuit sum is the empty set.

Proof. This can be proven to be a matroid using (C1), (C2), and (C3).
(C1) is trivially proven as $\emptyset$ has no non-empty subsets, and can therefore not be the summation of non-empty subsets using *Kirchoff summation*.
(C2) is also easily proven. If $X \subset C'$, and C' is a circuit, then it is clear that C' does not contain any subsets which makes the *Kirchoff sum* equal to the empty set. Therefore, as a subset of C', X cannot be dependent and therefore not a circuit.
(C3) is proven by taking two circuits C_1' and C_2', with $C \in C_1' \cap C_2'$. From calculating the *Kirchoff sum* it is easy to see that $\triangle_i\{C_i : C_i \in C_1' \setminus \{C\}\} = C$ as well as $\triangle_i\{C_i : C_i \in C_2' \setminus \{C\}\} = C$. Due to the binarity of M, it is clear that $C \triangle C = \emptyset$. Thus $\exists C_3' \in C_1' \cap C_2' \setminus \{C\}$ such that $C_3' \in \mathcal{C}'$ (Longyear, 1980, p. 73). □

Kirchoff basis and the bases of a derived matroid

The bases of the derived matroid $\delta_L M$ are precisely the *Kirchoff bases* of the ground set E. This can be proven using four lemmas.

Lemma 4.1. *If* $C_1 \triangle C_2 = \emptyset \iff C_1 = C_2$

Proof. Any $C \in C_1 \triangle C_2$ is in either both C_1 and C_2, or none of them. □

Lemma 4.2. *Any Kirchoff basis* $\mathcal{B}'$ *is independent.*

Proof. Assume that $\mathcal{B} = \{C_1, C_2, ..., C_k\}$ and that $C_1 \triangle C_2 \triangle ... \triangle C_k = \emptyset$. By dividing the *Kirchoff sum* into two different circuits $C_1 \triangle (C_2 \triangle ... \triangle C_k) = C_1 \triangle \Sigma_{i=2}^k C_i$. Then, by Lemma 4.1, $C_1 = \Sigma_{i=2}^k C_i$ and then $\mathcal{B}'$ is not a *Kirchoff basis*. Thereby we have a contradiction, and all *Kirchoff bases* must be independent. □

Lemma 4.3. *No proper superset* $\mathcal{S}$ *of* $\mathcal{B}'$ *is independent.*

Proof. Let $C_i \in \mathcal{S} \setminus \mathcal{B}'$. Then C_i can be written as a *Kirchoff sum* of a given set of elements in $\mathcal{B}'$. This leads to the conclusion that $\mathcal{S}$ is not independent, as one of its elements can be written as a *Kirchoff sum* of some of its other elements. □

Remark. From these three lemmas, we have now proven that the *Kirchoff bases* $\mathcal{B}'$ are indeed bases of $\delta_L M$ and we must now only prove that these are the only bases of $\delta_L M$.

Lemma 4.4. *If $\mathcal{R} \subseteq E$ is not a Kirchoff basis then it is not a base of $\delta_L M$.*

Proof. This leads to two possible cases (1) and (2):
(1) Not all C can be written as a *Kirchoff sum* using elements of $\mathcal{R}$. This leads us to the conclusion that $\mathcal{R}$ is not a maximal independent set and therefore not a basis.
(2) A strictly smaller set $\mathcal{R}'$ than $\mathcal{R}$ is such that all circuits are *Kirchoff sums* of those $\mathcal{R}'$. Thus, $\mathcal{R}$ is not independent and therefore not a basis. □

Proposition 4.5. The *Kirchoff bases* are the bases of $\delta_L M$

This results in the two following remarks:

1. The definition so far makes sense for non-binary matroids, but to show that $M = (E', \mathcal{C}') = (E', \mathcal{B}')$ is a new matroid, we used that it is binary.
2. This definition was made without any matrix A, and it is therefore independent of the choice of representation.

4.2 Oxley and Wang's approach

To make a definition valid also for non-binary matroids, Oxley and Wang (2019) decided to use representations of matroids, both over $\mathbb{F}_2$ as well as over other fields.

We therefore start with a matroid M, which is representable over a field $\mathbb{F}_q$, such that the set of the column vectors of a matrix A is its ground set, and we denote it by $M = M[A]$. Using both the matrix and the matroid, Oxley and Wang (2019), defined the derived matroid $\delta_{OW} M = \delta_{OW} M[A]$.

The derived matroid

To create the derived matroid $\delta_{OW}M$, we first create a new matrix $\mathcal{A}$ based on the linear dependent column vectors of A. The column vectors of $\mathcal{A}$ correspond to the minimal linear relations between the column vectors in A obtained from circuits of M. If e_i are the column vectors of A, then the vectors created by a circuit C_i form unique linear combinations $c_1e_1 + c_2e_2 + ...c_ne_n = 0$, which give rise to columns $(c_1, c_2, ..., c_n)^T$, where some c_i might be zero, of $\mathcal{A}$. We then repeat this for each circuit in the matroid M and create the matrix $\mathcal{A}$. The matroid generated from $\mathcal{A}$ is then the derived matroid to M, i.e. $\delta_{OW}M[A] = M[\mathcal{A}]$ (Oxley and Wang, 2019, p. 3).

Example

This whole process can be shown quite effectively using a matrix and matroid created from a graph. The following graph is an augmented and expanded graph from Oxley and Wang (2019, p. 4), which again leads to an augmented and expanded example.

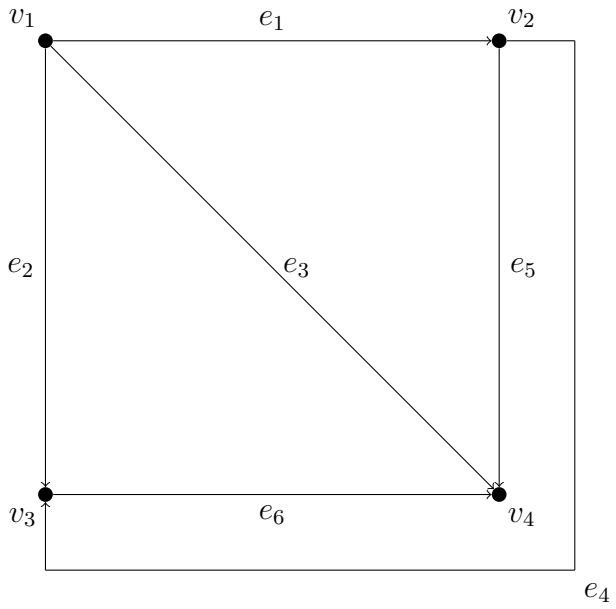

Figure 3: K_4-graph

This graph also takes into consideration the direction of each edge. For example, e_1 starts in v_1 and ends in v_2. Generally for this graph, we can say that if $i < j$ and e_k is the edge between v_i and v_j then e_k goes from v_i to v_j.

A matrix A over $\mathbb{F}_3$ generated from this graph can be:

$$A = \begin{bmatrix} -1 & -1 & -1 & 0 & 0 & 0 \\ 1 & 0 & 0 & -1 & -1 & 0 \\ 0 & 1 & 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \Rightarrow \begin{bmatrix} 1 & 0 & 0 & -1 & -1 & 0 \\ 0 & 1 & 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Here in the left matrix, we have matched the starting vertex of an edge by -1 and the end vertex by +1. Moreover, row number i corresponds to vertex number i and column number j corresponds to edge number j. From the usage of Gaussian elimination, it is clear to see that we have a span of three and therefore do not need the bottom row.

By using the new matrix A' for A:

$$A' = \begin{bmatrix} 1 & 0 & 0 & -1 & -1 & 0 \\ 0 & 1 & 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

we can now create the matrix $\mathcal{A}$ for the derived matroid. $\mathcal{A}$ will then be:

$$\mathcal{A} = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ -1 & 0 & 1 & 0 & -1 & 0 & 1 \\ 0 & -1 & -1 & 0 & 0 & -1 & -1 \\ 1 & 0 & 0 & 1 & 0 & 1 & -1 \\ 0 & 1 & 0 & -1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & -1 & 1 & 0 \end{bmatrix}$$

The matroid $M[\mathcal{A}]$ represented by this matrix is defined to be the derived matroid $\delta_{OW}M[A]$ of $M[A]$.

The same graph can also be used to give the derived matroid for a matroid $M[B]$ over a binary matrix B.

$$B = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \Rightarrow \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Just as with the matrix A we can remove the bottom row and convert it to a new matrix B'

$$B' = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

This is a matrix that is nearly identical to A' except for the fact that all -1 in A' has been converted to 1. The same is true for the matrix $\mathcal{B}$ created from B the same way $\mathcal{A}$ was created from A.

$$\mathcal{B} = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}$$

The matroid $M[\mathcal{B}]$ represented by this matrix is defined to be the derived matroid $\delta_{OW}M[B]$ of $M[B]$.

As the matrices $\mathcal{A}$ and $\mathcal{B}$ are nearly identical and the fact that we could say that A and $\mathcal{A}$, work for both $\mathbb{F}_2$ and $\mathbb{F}_3$, if we only change the -1 to 1, then we might ask ourselves what the differences between the derived matroids will be.

The difference between $\mathcal{A}$ and $\mathcal{B}$ is found by looking at their minimal dependent

sets of columns. The sets of columns given below are dependent for both matrices and therefore give rise to circuits of their given matroids. Each column is only denoted by its column index, i.e. a number from 1 to 7. These sets are $\{1,2,7\}$, $\{1,3,6\}$, $\{1,4,5\}$, $\{2,3,5\}$, $\{2,4,6\}$, $\{3,4,7\}$. For $\mathcal{B}$ which is defined over $\mathbb{F}_2$ there is one extra set of columns that is dependent. This is $\{5,6,7\}$. This leads to the same conclusion that Oxley and Wang made, which was that $\delta_{OW}M[A]$ is isomorphic to the non-Fano matroid, and that $\delta_{OW}M[B]$ is isomorphic to the Fano matroid. This can easily be shown using these two figures, with the columns now as the vertices, and the line/circle segments showing minimal dependent sets.

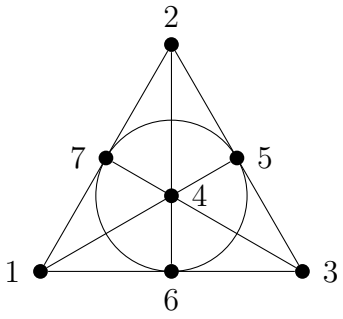

Figure 4: Fano matroid

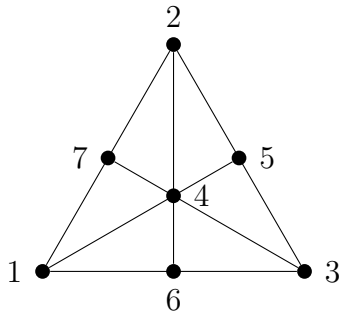

Figure 5: Non-Fano matroid

The vectors of the matrix are dependent if connected by either a straight line or a circle.

Hence $\{1,7,2\}$ and $\{2,3,5\}$ are dependent circuits, while $\{1,3,2\}$ is not. In Johnson (2016, pp. 14-16) text about dual Fano, and dual non-Fano matroidal networks, he shows that the Fano matroid has a representation over $\mathbb{F}_2$ while the non-Fano matroid has no representation over $\mathbb{F}_2$. This corresponds to our results with the Fano matroid being isomorphic to the derived matroid over $\mathbb{F}_2$, and the non-Fano matroid being isomorphic to the derived matroid over $\mathbb{F}_3$.

The following result is then given in Oxley-Wang.

Lemma 4.6. *For a field $\mathbb{F}_q$, let M be an $\mathbb{F}_q$-represented matroid. Then $\delta_{OW}M$ is a simple matroid of rank $r^*(M)$. In particular, if B is a basis of M, then $\{C(e,B) : e \in E(M) \setminus B\}$ is a basis of $\delta_{OW}M$ (Oxley and Wang, 2019, p. 3).*

Remark. $C(e, B)$ will therefore be the unique circuits contained in $\{e\} \cup B$ where B is a basis set and e is an element not contained in B. Since there are $n - k$ elements in $E \setminus B$, and since $|B| = r(B) = r(E) = k$, all the bases for $\delta_{OW}M$ will contain $n - k$ elements.

This Lemma is true for both $\delta_{OW}M[A]$ and $\delta_{OW}M[B]$ from the example above. It is clear that both matroids are simple since neither $\mathcal{A}$ nor $\mathcal{B}$ has any parallel column vectors. For the second part it is easy to see that $r(M[A]) = r(M[B]) = 3$ and that $n(M[A]) = n(M[B]) = 6$, therefore $r^*(M[A]) = r^*(M[B]) = n(M) - r(M) = 6 - 3 = 3$. By using Gaussian elimination it is easy to prove that the rank of $\delta_{OW}M[A]$ and $\delta_{OW}M[B]$, $r(\delta_{OW}M[A]) = r(\delta_{OW}M[B]) = 3$.

Equality of Longyear and Oxley-Wang for matroids with binary representation

We will now show that there is an equality between the system of determining the derived matroid from Longyear (1980) and Oxley and Wang (2019), if we focus on matroids represented over $\mathbb{F}_2$ by a matrix A.

To define the derived matroid $\delta_{OW}M$ using the matrix A as a starting point, we must find all *Kirchoff bases* using the circuits of A as elements. To find the circuits, we can do the same operations as done to find A' and B' from the previous subsection and then use these to find $\mathcal{A}$ and $\mathcal{B}$. Then, after finding our $\mathcal{A}$ for this new matrix A, we can then find the different *Kirchoff bases* corresponding to this matrix, representing the circuits. For a binary matroid $M[A]$ we have the following:

Corollary 4.6.1. *The Kirchoff sum of a set of circuits of a matroid $M[A]$ is equal to the empty set if and only if the sum of the corresponding column vectors of A is the zero-vector, i.e. that this set is a dependent set over $\mathbb{F}_2$. Therefore, the condition of dependency is equal for both Longyear and Oxley-Wangs constructions of derived matroids.*

By following the steps for Longyear's construction using $\mathcal{A}$ we can clearly see that this is correct. This is a consequence of the fact that the process of taking the *Kirchoff sum* is equal to just summation when working with binary operations, $0 + 0 = 0, 1 + 0 = 1$ and $1 + 1 = 0$, i.e. that equal values result in zero while

non-equal values result in ones.

Invariance of representation

We will now proceed to work over finite fields in general. First, we will give a helpful intermediate result.

Definition 4.7. Two matrices A and B over a field $\mathbb{F}$ are projectively equivalent if there exist matrices C and D over $\mathbb{F}$ such that $B = C \cdot A \cdot D$, where C is a non-singular $k \times k$ matrix and D is a diagonal non-singular $n \times n$ matrix.

Proposition 4.8. Given the field $\mathbb{F}_q$, let the matrices A and B over $\mathbb{F}$ be projectively equivalent. Then $\delta_{OW} M[A] = \delta_{OW} M[B]$

Proof. First set $A' = C \cdot A$, such that $B = A' \cdot B$. Since A' is obtained only from reversible row operations, all linear relations between columns of A' are exactly the same as those of A. From this, we can look at the "derived matrix" $\mathcal{A}$ derived from A', which will then be the same as if it was derived from A. As usual the columns of $\mathcal{A}$ correspond to the, say s, circuit vectors of A':

$$\mathcal{A} = \begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,s} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,s} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,s} \end{bmatrix}$$

From simple matrix calculations, we can then show that the "derived matrix" $\mathcal{B}$ corresponding to B is

$$\mathcal{B} = \begin{bmatrix} b_{1,1} & b_{1,2} & \cdots & b_{1,s} \\ b_{2,1} & b_{2,2} & \cdots & b_{2,s} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n,1} & b_{n,2} & \cdots & b_{n,s} \end{bmatrix} = \begin{bmatrix} \lambda_1 \cdot a_{1,1} & \lambda_1 \cdot a_{1,2} & \cdots & \lambda_1 \cdot a_{1,s} \\ \lambda_2 \cdot a_{2,1} & \lambda_2 \cdot a_{2,2} & \cdots & \lambda_2 \cdot a_{2,s} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_n \cdot a_{n,1} & \lambda_n \cdot a_{n,2} & \cdots & \lambda_n \cdot a_{n,s} \end{bmatrix},$$

where λ_i are the diagonal entries of D.

Therefore, to every minor of $\mathcal{A}$, the corresponding minor of $\mathcal{B}$ is of the same rank and thus $\mathcal{A}$ and $\mathcal{B}$ have the same dependent relations regarding their columns.

□

Theorem 4.9. *Let $\mathbb{F}$ be a field. Then, for all $\mathbb{F}$-represented matroids $M[A]$, the derived matroid $\delta_{OW}M[A]$ does not depend on the $\mathbb{F}$-represenation A if and only if $\mathbb{F}$ is $\mathbb{F}_2$ or $\mathbb{F}_3$.*

Proof. Given $M[A_1]$ and $M[A_2]$ for two different matrices over $\mathbb{F}_2$, both of which give the same matroid. Then, we have already proved that both $\delta_{OW}M[A_1]$ and $\delta_{OW}M[A_2]$ are the matroid obtained from Longyear. Now we have to look at $\mathbb{F}_3$. We once again study $M[A_1]$ and $M[A_2]$, both of which are equal. Since A_1 and A_2 have been proven to be projectively equivalent, we know that they have the same derived matroid. Oxley and Wang (2019, pp. 5-6) show in the proof of their Theorem 8 that this does not work for any field $\mathbb{F}_n$ with $n \geq 4$. □

Lemma 4.10. *For a field $\mathbb{F}_q$ and $n \geq 2$, let $U_{n-2,n}$ be an $\mathbb{F}_q$ representation. Then $\delta_{OW}U_{n-2,n} \cong U_{2,n}$.*

Proof. Since all circuits in $U_{n-2,n}$ have a cardinality of $n-1$, and all subsets of cardinality $n-1$ are circuits, it means that there are a total of n circuits in $U_{n-2,n}$. This means that the number of elements in $\delta_{OW}U_{n-2,n}$ will be n. Furthermore, from Lemma 4.6 we know that the rank of the derived matroid will be the corank of the matroid. $r(\delta_{OW}U_{n-2,n}) = r^*(U_{n-2,n}) = |U_{n-2,n}| - r(U_{n-2,n}) = n - (n-2) = 2$. Therefore, the rank of the derived matroid will be 2 and the cardinality will be n, and since it is simple it will also be uniform, since we know that all subsets of cardinality 2 or less are independent, and all subsets of cardinality 3 or more are dependent. Hence $\delta_{OW}U_{n-2,n} \cong U_{2,n}$. This is an extended proof inspired by the proof given in Oxley and Wang (2019, p. 5). □

Lemma 4.11. *For a field $\mathbb{F}_q$ and $n \geq 1$, let $U_{1,n}$ be an $\mathbb{F}_q$ representation. Then $\delta_{OW}U_{1,n} \cong M(K_n)$.*

Proof. Over all fields we may represent $U_{1,n}$ as [1 1 1 1 1 ...1], with n ones. We can do this since each column vector must be a multiple of each other, and none can be the zero column vector. From this, it is easy to define the column vectors representing the circuits of the matroid.

$$\begin{bmatrix} 1 & 1 & 1 & \cdots & 0 & 0 & \cdots & 0 \\ 1 & 0 & 0 & \cdots & 1 & 1 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 1 \\ 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 1 \end{bmatrix}$$

This is not only the matrix representing the derived matroid of $U_{1,n}$, it is also the matrix representation of the graph K_n (Oxley and Wang, 2019, p. 5).

□

Simplification and derived matroids

Given a representable matroid $M[A]$ over $\mathbb{F}_q$, we have a canonical representation of $co(M)$. Regard A as a generator matrix of a code D over $\mathbb{F}_q$. Let B be a parity check matrix of the code D. Remove all zero-columns of B. For all non-zero columns of B that are parallel, remove all but one of the parallel columns. This results in a simplified matrix H. Regard H as a parity check matrix of a new code C. Let G be a generator matrix of C. Then the cosimplification of $M[A]$ will be $co(M[A]) = M[G]$, with this notation:

Theorem 4.12. $\delta_{OW} M[A] = \delta_{OW} M[G]$

Remark. Oxley and Wang (2019) formulates this theorem as $\delta_{OW} M = \delta_{OW} co(M)$, but in this text, we prefer to relate it to representable matroids.

Proof. The proof of this theorem has two crucial components. Lemma 9 and Lemma 10 in Oxley and Wang (2019).

Lemma 9 proves that if $\{e_1, e_2\}$ is a circuit of M^*, then $\delta_{OW}(M/e_1) = \delta_{OW}M$. The proof of this can be found in Oxley and Wang (2019, pp. 6-7).
Lemma 10 shows that if e is a loop of M^*, then $\delta_{OW}(M \setminus e) = \delta_{OW}M$. The simple proof of this is that no loop of M^* is contained in a circuit of M. □

Furthermore, by combining this theorem with Lemma 4.10 we get the following corollary:

Corollary 4.12.1. *For a field $\mathbb{F}_q$, let $M = M[A]$ be an $\mathbb{F}_q$-represented matroid for which $r^*(M) = 2$. Then $co(M) \cong U_{n-2,n}$ for some $n \geq 2$ and $\delta_{OW}M \cong U_{2,n}$.*

Proof. $r^*(M) = 2 \Rightarrow r(M) = n - 2 \Rightarrow r(M^*) = 2 \Rightarrow si(M^*) = U_{2,n} \Rightarrow co(M) = (si(M^*))^* = U_{n-2,n}$. This is because if any set of cardinality 1 has rank 0 then it is removed during simplification. Furthermore, all sets of cardinality 2 with rank 1 will have one element removed. After this process all sets of cardinality 2 will thus have rank 2. The simplification $si(M^*)$ will therefore have all independent sets of rank 2 or less since all sets of a higher cardinality will be dependent. From this $si(M^*) = U_{2,n}$. Since $co(M) = U_{2,n}^* = U_{n-2,n}$ and $\delta_{OW}U_{n-2,n} = U_{2,n}$, then $\delta_{OW}M = \delta_{OW}co(M) = U_{2,n}$. This is an extended proof inspired by the proof given in Oxley and Wang (2019, p. 7). □

Connected derived matroids

Another important aspect of derived matroids shown in Oxley and Wang (2019) is the following lemma.

Lemma 4.13. *A derived matroid $\delta_{OW}M$ is connected if and only if the matroid M is connected.*

Remark. This also means that a derived matroid is disconnected if and only if the matroid it is constructed from is disconnected.

To prove this, Oxley and Wang (2019) first proves that a disconnected matroid gives a disconnected derived matroid in Lemma 17, they then show that a connected matroid gives a connected derived matroid in Corollary 19. Since we have

that connected matroids give connected matroids and disconnected matroids give disconnected matroids, they can then only give one another (2019, p. 7).

4.3 Freij-Hollanti, Jurrius and Kuznetsova's approach

We will now present the third main construction of derived matroids. As a starting point, the combinatorial derived matroid $\delta_{FJK}M$ defined by Freij-Hollanti et al. (2023) is quite different from those defined in Longyear (1980) and Oxley and Wang (2019). In principle, only the name "derived matroids" seems the same in the beginning. We will delve deeper into the construction and comment on similarities and differences.

The main difference from Oxley and Wang (2019)'s creation is that for a matroid M, the derived matroid δ_{FJK} is independent of any representation.
The main difference from Longyear (1980)'s creation is that the matroid does not have to be binary.

A main similarity is that like Longyear (1980)'s, and Oxley and Wang (2019)'s definition, Freij-Hollanti et al. (2023)'s definition also uses the circuits of M as its ground set for $\delta_{FJK}M$.

The derived matroid

To define their derived matroid $\delta_{FJK}M$, Freij-Hollanti et al. (2023) first define two new "operations" $\epsilon()$ and $\uparrow$.

Let $\mathcal{C}$ be the set of circuits of some matroid M, and let $\mathcal{M} \subseteq \mathcal{C}$. We then define the two new sets $\epsilon(\mathcal{M})$ and $\uparrow \mathcal{M}$:

$$\epsilon(\mathcal{M}) = \mathcal{M} \cup \{(M_1 \cup M_2) \setminus \{C\} : M_1, M_2 \in \mathcal{M}, M_1 \cap M_2 \notin \mathcal{M}, C \in M_1 \cap M_2\}$$

$$\uparrow \mathcal{M} = \{M_1 \subseteq \mathcal{C} : \exists M_2 \in \mathcal{M} : M_2 \subseteq M_1\}$$

After this Freij-Hollanti et al. (2023, pp. 7-8) defines the set $\mathcal{A}_0$. We will instead be using $\mathfrak{D}_0$ for the same set, as this follows more closely the notation $\mathcal{D}$ used for dependent sets in matroids. The set $\mathfrak{D}_0$ is defined as:

$$\mathfrak{D}_0 = \{D \subseteq \mathcal{C} : |D| > n(\cup_{C \in D} C)\}$$

This means that $\mathfrak{D}_0$ is defined as all sets of circuits in $\mathcal{C}$ where the nullity of the union of the elements of the circuits must be less than the number of circuits in the set.

Furthermore, we can define $\mathfrak{D}_{i+1}$ and $\mathfrak{D}$ as:

$$\mathfrak{D}_{i+1} = \uparrow \epsilon(\mathfrak{D}_i) \qquad \mathfrak{D} = \bigcup_{i \geq 0} \mathfrak{D}_i$$

Due to the finiteness of E and $\mathcal{C}$, this process has to "stop" after a finite number of steps. In other words, after $i+1$ steps $\mathfrak{D}_{i+1}$ will be equal to $\mathfrak{D}_i$. Therefore, we can rewrite $\mathfrak{D}$ as the following after these $i+1$ steps:

$$\mathfrak{D} = \mathfrak{D}_{i+1}, \text{ when } \mathfrak{D}_{i+1} = \mathfrak{D}_i$$

From the definition above we define the concept of depth for a set $D \in \mathfrak{D}$. We say that a set D has depth i if it is contained in $\mathfrak{D}_i$ but not in $\mathfrak{D}_{i-1}$, i.e. D has depth i if $D \in \mathfrak{D}_i \setminus \mathfrak{D}_{i-1}$ (Freij-Hollanti et al., 2023, p. 8). Furthermore, we also get the following definition for the combinatorial derived matroid.

Definition 4.14. Let M be a matroid defined by the ground set E and by its set of circuits $\mathcal{C}$. The combinatorial derived matroid $\delta_{FJK}M$ is then a matroid with ground set $E' = \mathcal{C}(M)$ and set of dependent sets $\mathfrak{D}$.

In the previous definition, there is a hidden proposition. This is the following:

Proposition 4.15. The family $\mathfrak{D}$ defined above satisfies the axioms (D1)-(D3) of dependent sets for matroids.

To prove this, we first need to prove an intermediate result.

Lemma 4.16. *Let $D \in \mathfrak{D}_i$, then there exists $D' \in \mathfrak{D}_{i-1}$ such that $|D'| \leq |D|$.*

Proof. We now have two cases; one if D has depth i and one if D has a depth less than i.

If the depth of D is lower than i, then it is itself contained in $\mathfrak{D}_{i-1}$ and therefore there exists $D' = D$ which has a cardinality equal D.

If the depth of D is i, we can say that $D \in \uparrow \epsilon(\mathfrak{D}_{i-1}) \setminus \mathfrak{D}_{i-1}$. This leads us to the conclusion that D either arose from the operation $\uparrow$ or the operation ϵ. Since $\epsilon(\mathfrak{D}_{i-1})$ contains all inclusion minimal sets we can assume that $D \in \epsilon(\mathfrak{D}_{i-1}) \setminus \mathfrak{D}_{i-1}$. From this it is safe to assume that there exists $D_1, D_2 \in \mathfrak{D}_{i-1}, D_1 \cap D_2 \notin \mathfrak{D}_{i-1}, C \in D_1 \cup D_2$ such that $D = D_1 \cup D_2 \setminus \{C\}$. Furthermore, $D_1 \not\subseteq D_2$ since $D_1 \in \mathfrak{D}_{i-1}$ and $D_1 \cap D_2 \notin \mathfrak{D}_{i-1}$, which leads us to $|D_2| \leq |D_1 \cup D_2| - 1 = |D|$. Hence there exists $D' = D_2$ such that $|D'| \leq |D|$ (Freij-Hollanti et al., 2023, p. 9). □

Using this intermediate result, and the fact that the ϵ operation is designed to perfectly fit the property of axiom (D3), we can then prove that $\mathfrak{D}$ follows the axioms of the set of dependent sets $\mathcal{D}$:

Proof. To prove that the $\emptyset \notin \mathfrak{D}$ we first look at $\mathfrak{D}_0$. Since $|\emptyset| = 0$ and nullity cannot be a negative number it is clear that $\emptyset \notin \mathfrak{D}_0$. Furthermore, from Lemma 4.16 it therefore cannot be in any higher depths and therefore also not in $\mathfrak{D}$.

If $D_1 \in \mathfrak{D}$ and $D_1 \subset D_2$, then by the operation $\uparrow$, so does D_2 have to be in $\mathfrak{D}$.

If $D_1, D_2 \in \mathfrak{D}$ we must check two things, the case where $D_1 \cap D_2 \in \mathfrak{D}_i$ for some depth i and the case where it is not. If it is, then this is proven, if not there must exist some minimal $\mathfrak{D}_j$ where both D_1 and D_2 are contained. Therefore, from ϵ there exists D for all $C \in D_1 \cap D_2$ such that $D = D_1 \cup D_2 \setminus \{C\} \in \mathfrak{D}_{j+1} \subseteq \mathfrak{D}$. □

From this, we can define the combinatorial derived matroid $\delta_{FJK}M = (E', \mathfrak{D})$, where E' is the set of circuits in the matroid M (Freij-Hollanti et al., 2023, p. 8).

We also have the following for a set $\mathfrak{C}$, which gives us an alternative definition of $\delta_{FJK}M$. We let $\mathfrak{C}_0 = min\ \mathfrak{D}_0$ and $\mathfrak{C}_{i+1} = \epsilon\mathfrak{C}_i$

$$\mathfrak{C} = min \bigcup_{i \geq 0} \mathfrak{C}_i$$

Freij-Hollanti et al. (2023, p. 8).

We then get the following definition of the derived matroid $\delta_{FJK}M$. Let M be a matroid defined by the ground set E and by its set of circuits $\mathcal{C}$. The combinatorial derived matroid $\delta_{FJK}M$ is then a matroid with ground set $E' = \mathcal{C}(M)$ and set of circuits $\mathfrak{C}$, i.e. $\delta_{FJK}M = (E', \mathfrak{C})$ (Freij-Hollanti et al., 2023, p. 8).

This can be proven by showing that $\mathfrak{C}$ is equal to the inclusion minimal $\mathfrak{D}$ and therefore is the circuits of $\delta_{FJK}M$. The key result is Lemma 4.8 in Freij-Hollanti et al. (2023) which says:

Lemma 4.17. *Let $A \in \mathfrak{D}$ have depth $i + 1 \geq 1$. Then there exists sets $A_1, A_2 \in min\ \mathfrak{D}$ of depth at most i, such that $A = (A_1 \cup A_2) \setminus C$ for some $C \in A_1 \cap A_2$.*

Furthermore, Freij-Hollanti et al. (2023) shows that the following process also allows us to construct the set of circuits of $\delta_{FJK}M$.

Proposition 4.18. The set of circuits of δM can be constructed iteratively as follows:

1. $\mathcal{E}_0 = min\ \mathfrak{D}_0$
2. $\mathcal{E}_{i+1} = min\ \epsilon\mathcal{E}_i$, for all $i \geq 0$
3. The sequence $\mathcal{E}_i$ terminates, and its limit equals the collection $\mathfrak{C}$ of circuits of δM.

The following result reveals another similarity between the different constructions from Longyear (1980), Oxley and Wang (2019), and Freij-Hollanti et al. (2023).

Lemma 4.19. *Let M be a matroid. Then $\delta_{FJK}M$ is simple, that is, there are no dependent sets of size 1 or 2.*

Proof. Since we have Lemma 4.16 it is enough to prove that $\mathfrak{D}_0$ does not contain

any sets of size 1 or 2, since therefore, no set of a higher depth can contain them either.

If $D = \{C\}$ we have that the nullity and the cardinality of the set are equal and therefore cannot be a part of $\mathfrak{D}_0$.

If $D = \{C_1, C_2\}$, we know that $C_1 \cap C_2$ is independent and therefore has nullity 0. Furthermore, we know that $n(D) = n(C_1 \cup C_2)$. From (R3) we know that:

$$\begin{aligned} r(C_1) + r(C_2) &\geq r(C_1 \cup C_2) + r(C_1 \cap C_2) \\ n - n(C_1) + n - n(C_2) &\geq n - n(C_1 \cup C_2) + n - n(C_1 \cup C_2) \\ n(C_1) + n(C_2) &\leq n(C_1 \cup C_2) + n(C_1 \cap C_2) \\ n(C_1) + n(C_2) &\leq n(C_1 \cup C_2) \\ 1 + 1 = 2 &\leq n(C_1 \cup C_2) \end{aligned}$$

Therefore $n(D) \geq |D|$ and it is not in $\mathfrak{D}_0$ Freij-Hollanti et al. (2023, p. 10). □

This lemma lets us know that none of the derived matroids constructed using Longyear (1980), Oxley and Wang (2019), and Freij-Hollanti et al. (2023) give rise to any matroid which has circuits containing only two elements or a loop.

The following result shown by Freij-Hollanti et al. (2023) is a result that goes in the opposite direction.

Proposition 4.20. Suppose that M is a connected matroid with at least two circuits. Then every element of $\delta_{FJK}M$ is contained in a triangle, that is a circuit of size 3 (Freij-Hollanti et al., 2023, p. 10-11).

Connected derived matroids

Just like the derived matroid δ_{OW}, the derived matroid δ_{FJK} satisfies the following result, stated as Theorem 32 in Freij-Hollanti et al. (2023, pp. 19-20).

Theorem 4.21. *Let M be a matroid with no coloop. Then M is connected if and only if $\delta_{FJK}M$ is connected.*

This result, which is not stated by Freij-Hollanti et al. (2023) is an immediate extension of Proposition 4.20.

Proposition 4.22. If all connected matroids M_i which make up the disconnected $M = \bigoplus_i M_i$ have at least two circuits, then every element in δ_{FJK} is contained in a triangle.

Example

If we continue using the example from Section 4.2, we can then use the graph K_4 to define the derived combinatorial matroid.

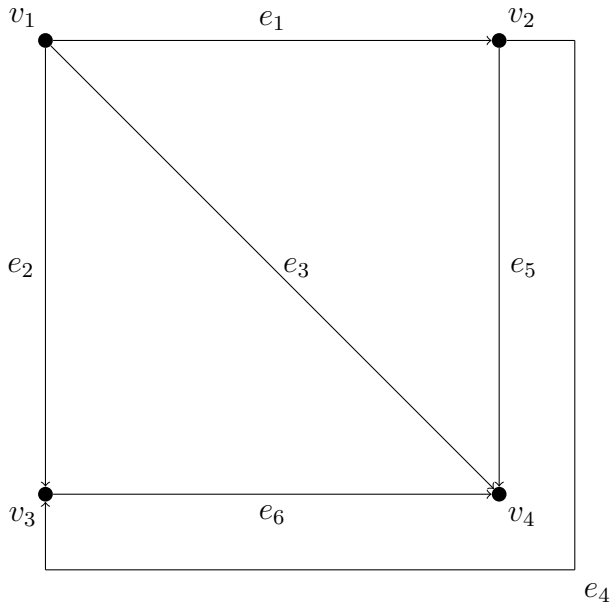

Figure 6: K_4-graph

We have previously found all circuits of this graph:

$\{e_1, e_2, e_4\}, \{e_1, e_3, e_5\}, \{e_2, e_3, e_6\}, \{e_4, e_5, e_6\}, \{e_1, e_2, e_5, e_6\}, \{e_1, e_3, e_4, e_6\}, \{e_2, e_3, e_4, e_5\}$

We denote them by $\{124\}, \{135\}, \{236\}, \{456\}, \{1256\}, \{1346\}, \{2345\}$.

To create $\mathfrak{D}_0$ we must now find all sets of these, of which the cardinality of the set is greater than the nullity of the union of the elements in the circuits in the

set. From Section 4.2 we saw that the nullity of this set was 3. Therefore, any set containing at least 4 circuits will be in $\mathfrak{D}_0$. Furthermore, the nullity of any strict subset of the ground set will be 2 or less. This also lets us define the sets with cardinality 3 which also will be in $\mathfrak{D}_0$. These are the sets where the nullity is less than 3, which means that it does not contain all elements of E. Therefore, any set of 3 circuits where not all elements of E are represented will be the dependent sets of cardinality 3, i.e. all the sets of 3 circuits where one element of E is removed. We also know that no set of cardinality 1 or 2 can be in $\mathfrak{D}_0$ from Lemma 4.19.

$$\begin{aligned}\mathfrak{D}_0 =&\{\{D : D \subseteq C, |D| \geq 4\}\}\cup \\ &\{\{236, 456, 2345\}, \{135, 456, 1346\}, \{124, 456, 1256\}, \\ &\{135, 236, 1256\}, \{124, 236, 1346\}, \{124, 135, 2345\}\}\end{aligned}$$

What happens when we look at $\epsilon(\mathfrak{D}_0)$, using sets D_1, D_2 from $\mathfrak{D}_0$ as described using the ϵ operation. As all elements created using two sets contained in $\mathfrak{D}_0$ will have the same cardinality as the set with the highest cardinality or a higher cardinality, we only need to check whether or not any two sets of cardinality 3 will give a set of cardinality 3 which is not contained in $\mathfrak{D}_0$. All sets of a higher cardinality will already be contained in $\mathfrak{D}_0$. As we see, no two sets of cardinality 3 have more than one equal circuit contained in both, which from the construction of ϵ leads us to the conclusion that from each ϵ operation, the new set will be of cardinality 4, thus already contained in $\mathfrak{D}_0$. Hence $\mathfrak{D} = \mathfrak{D}_0$.

From this, we can also see that the circuits of $\mathfrak{D}$ will be the sets in $\mathfrak{D}$ of cardinality 3. Furthermore, these sets are equivalent to the circuit sets of the derived matroid of K_4 with its representation over $\mathbb{F}_3$ given in the example in Section 4.2.

Comparison with Oxley and Wang's approach

The previous example gives an illustration of the relation between the derived matroid constructed by Oxley-Wang and the combinatorial derived matroid created by Freij. In Example 4.2 we give the derived matroid of the matroid of K_4 over

$\mathbb{F}_2$ and of the matroid over $\mathbb{F}_3$. The derived matroid over $\mathbb{F}_2$ has 7 circuits.

We now give a general result; illustrated by the example with matroids taken from K_4.

Lemma 4.23. *If $\delta_{FJK}M = (\mathcal{C}, \mathfrak{D}_0)$, then all dependent sets in $\delta_{FJK}M$ are dependent in $\delta_{OW}M$ for every representation.*

Proof. Let $D \in \mathfrak{D}_0$, then we know that $|D| > n(\cup_{C\in D}C) = n(supp(D))$.

Let G be the generator matrix of a code C, with H as its parity check matrix. Then the corresponding matroid for C is the matroid generated by the matrix G, $M[G]$. Furthermore, let X be a subset of the ground set E, then $C^*(X)$ will by definition be the elements of the orthogonal code with support in X, $C^*(X) = \{\mathbf{w} \in C^* : supp(\mathbf{w}) \subseteq X\}$. From this we know that $C^*(X) = ker(C^* \to C^*_{E\setminus X})$ and therefore $dimC^*(X) = dimC^* - dimC^*_{E\setminus X}$ which again gives us $r^*(E) - r^*(E\setminus X) = |E| + r(E \setminus E) - r(E) - |E \setminus X| - r(E \setminus (E \setminus X)) + r(E) = |X| - r(X) = n(X)$. By this proof and the fact that X may equal $supp(D)$ if we wish it, we get:

$$|D| > n(\cup_{C\in D}C) = n(Supp(D)) = dim(C^*(Supp(D)))$$

We now look at $C(X)$. This corresponds to all independent relations of columns in H over X, hence $C^*(X)$ corresponds to all independent relations in G over X. If we denote the number of independent relations by s, it means that there are precise s independent relations of the column vectors used to generate $M[G]$. Furthermore, it means that for any set of circuits D, there are at most s independent relations t, i.e. $t \leq s$. Therefore, the dimension of the span of the circuit vectors corresponding to the elements in D will be t, $dim(span(q_C : C \in D)) = t \leq s$.

In totality this gives us:

$$|D| > n(Supp(D)) = dim(C^*(Supp(D))) \geq dim(span(q_C : C \in D))$$

This shows that the circuit vectors of D are linearly dependent, thus D must also be dependent in the derived matroid generated using Oxley-Wang. This result and a shorter proof can be found in Freij-Hollanti et al. (2023, p. 22).

□

Moreover, we can use this to say something if the number of dependent sets is equal for the two constructions.

Corollary 4.23.1. *If $\delta_{FJK}M = (\mathcal{C}, \mathfrak{D}_0)$ and it contains the same number of dependent sets as $\delta_{OW}M$, then they are equal.*

Proof. From Lemma 4.23 we know that all dependent sets in $\delta_{FJK}M = (\mathcal{C}, \mathfrak{D}_0)$ are contained in $\delta_{OW}M$. Therefore, since $\delta_{FJK}M \subseteq \delta_{OW}M$ and $|\delta_{FJK}M| = |\delta_{OW}M|$ they must be equal (Freij-Hollanti et al., 2023, p. 22). □

Example 4.3 gives an illustration of this. In Example 4.2 we give the derived matroid of the matroid of K_4 over $\mathbb{F}_2$ and of the matroid over $\mathbb{F}_3$. The first matroid has 7 circuits, while the second matroid has 6 circuits. One of the 7 circuits in the matroid over $\mathbb{F}_2$ is not a circuit in the matroid over $\mathbb{F}_3$. In our example, the combinatorial derived matroid of K_4 is given. Its circuits are the ones of the derived matroid over $\mathbb{F}_3$ from Oxley and Wang's construction. Moreover, $\mathfrak{D}_0 = \mathfrak{D}$ in this case, so Lemma 4.23 and Corollary 4.23.1 can be applied. Therefore, the circuits given in Example 4.3 are exactly the same as those in Example 4.2.

Triplets in Oxley and Wang's approach

One important proposition made by Freij-Hollanti et al. (2023) was that all elements in the derived matroid $\delta_{FJK}M$ would be contained in a triangle, which by definition is a circuit of size 3. In Subsection 4.2 we also proved that all derived matroids using Oxley and Wang (2019)'s construction would be simple. This means that all subsets of circuits of cardinality 1 or 2 are independent in the derived matroid. On the other hand, we know that there are many dependent sets of cardinality 3 or more. We then have the following result, which we believe is a new one:

Proposition 4.24. If $M[A]$ is a connected matroid containing at least two circuits, then all circuits C of $M[A]$ are contained in a triangle of $\delta_{OW}M[A]$.

Proof. We have already shown the two statements needed for this proof, these are Proposition 4.22 and Lemma 4.23.

From Lemma 4.23 it is clear that this is true if the combinatorial derived matroids dependent set $\mathfrak{D}$ is equal to $\mathfrak{D}_0$. As both sets have the same ground set, and all dependent sets in the combinatorial derived matroid are dependent in the derived matroid using Oxley-Wangs construction, then automatically all circuits in δ_{OW} are contained in a triplet.

If not, we need to look at the proofs of the two statements a bit closer. In the proof of Proposition 4.22 we showed that if a connected matroid contains at least two circuits, then all circuits are contained in a triplet D, which again is a set contained in $\mathfrak{D}_0$. This means that all circuits of a matroid M are contained in a set D of cardinality 3, which is contained in $\mathfrak{D}_0$ for the combinatorial derived matroid. In the proof of Lemma 4.23 we see that every D in $\mathfrak{D}_0$ for the combinatorial derived matroid is also a dependent set for the derived matroid using Oxley-Wang's construction.

Using these two statements and their proofs, it is clear that firstly any circuit C is contained in a set D of cardinality 3 which is an element of $\mathfrak{D}_0$. Furthermore, any set D' in $\mathfrak{D}_0$ is also dependent on the derived matroid using Oxley-Wang's construction. Therefore, $D = D'$ is contained in the derived matroid using Oxley-Wang's construction, and thus all circuits are contained in a triangle for the derived matroid using Oxley-Wang's construction as well. □

Remark. Furthermore, Lemma 4.13 allows us to show that if all connected matroids M_i making up a disconnected matroid $M = \bigoplus_i M_i$ contains at least two circuits, then all circuits in M will be contained in a triplet.

5 Private information retrieval

We might ask ourselves what the theory of linear codes C_L, matroids M and derived matroids δM can be used for in a practical manner. The following is a summary of what we believe are the most important parts of Freij-Hollanti and Kuznetsova (2021), demonstrating how derived matroids enter the picture of Private Information Retrieval (PIR) in a practical manner.

The general problem regarding PIR is being able to receive a message without revealing which message was received. In correspondence to sending messages this can be seen as two communicators A and B, who are sending the symbol of the messages over a set of links; n in total. Unfortunately, there may be outside observers $I = \{T_1, T_2, ..., T_r\}$ which has access to a given set of links, $T_i \subseteq \{1, ..., n\}$. PIR then wants to lay a foundation as to how we can prevent these observers from finding out the message, as well as making sure that the receiver is able to.

This section, just like the text written by Freij-Hollanti and Kuznetsova (2021), is not going to answer the question above, but rather focus on some important aspects of PIR which can be studied using the theories given in previous sections.

5.1 Important definitions

Before we can begin to study the theories regarding PIR, we first need to understand some basic definitions.

Given a linear code C_L over $(\mathbb{F}_q)^n$, with corresponding matroid $M(C_L) = M[G] = (E, \mathcal{C})$. Let $T \subseteq E$, then $C_L|_T$ is a projection of C_L down to T.

Example Assume $E = \{1, 2, 3, 4, 5\}$ and $T = \{2, 3, 4\}$. Then for $\mathbf{w} = (w_1, w_2, w_3, w_4, w_5)$ we have $C_L|_T = \{(w_2, w_3, w_4) : \mathbf{w} \in C_L\}$.

Furthermore, if we have several different T's we can collect them in the set $\mathcal{T} = \{T_1, T_2, ..., T_s\}$. From this we can define $C_L^{\mathcal{T}}$ as follows:

$$C_L^{\mathcal{T}} = \{\mathbf{v} \in (\mathbb{F}_q)^n : \forall T \in \mathcal{T}, \exists \mathbf{w} \in C_L \ s.t. \ \mathbf{v}|_T = \mathbf{w}|_T\}.$$

Suppose now that we have a general codeword $\mathbf{w} \in (\mathbb{F}_q)^n$. We then want to test to see if it is part of $C_L \subseteq (\mathbb{F}_q)^n$. We therefore test to see if $\mathbf{w}|_T \in C_L|_T$ for all $T \in \mathcal{T}$. If yes, then we know that $\mathbf{w} \in C_L^{\mathcal{T}}$. If $C_L \subsetneq C_L^{\mathcal{T}}$ then we cannot conclude that $\mathbf{w} \in C_L$ only that $\mathbf{w} \in C_L^{\mathcal{T}}$. The bigger the difference between C_L and $C_L^{\mathcal{T}}$, the bigger the uncertainty that $\mathbf{w} \in C_L$ after a successful test. We can quantify this as:

$$\frac{dim(C_L^{\mathcal{T}}/C_L)}{n}$$

This number is also known as the secrecy rate, and tells us how much of the code can be used to send information using $C_L^{\mathcal{T}}$ which will not interfere with the information sent in C_L. If $C_L = C_L^{\mathcal{T}}$, then there is no possibility of sending information using $C_L^{\mathcal{T}}$ which would not be able to be sent through C_L. This justifies the interest in $C_L^{\mathcal{T}}$, given a linear code C_L and collusion patterns $\mathcal{T}$.

5.2 Multiple collusion patterns

We will now look at situations where the linear code is exposed to multiple collusion patterns at once.

First, we make the following observation:

$$\text{If } \mathbf{w} \in C_L^{\mathcal{T}}, \text{ then } \mathbf{w} \in C_L^{\mathcal{T}'} \text{ if } \mathcal{T}' = \{T' : T' \subseteq T, T \in \mathcal{T}\}.$$

This is because if $\mathbf{w}$ coincides with a codeword on $\mathcal{T}$, then it also coincides with the same codeword on any $\mathcal{T}' \subseteq \mathcal{T}$.

We will therefore assume that $\mathcal{T}$ is a simplicial complex, i.e. satisfying (I1) and (I2) given in Section 2.3. It does however not necessarily fulfill (I3). If $\{T_1, T_2, ..., T_S\}$ are the facets of this simplicial complex, i.e. the maximal sets of $\mathcal{T}$, then we write $\mathcal{T} = \langle T_1, T_2, ..., T_S \rangle$.

Lemma 5.1. *Given two collusion patterns $\mathcal{S} = \{S_1, S_2, ..., S_r\}$, $\mathcal{T} = \{T_1, T_2, ..., T_s\}$ and a linear code $C_L \subseteq (\mathbb{F}_q)^n$. We now want to focus on $C_L^{\mathcal{S}\cup\mathcal{T}}$ and $C_L^{\mathcal{S}\cap\mathcal{T}}$.*

1. $C_L^{\mathcal{S}\cup\mathcal{T}} = C_L^{\mathcal{S}} \cap C_L^{\mathcal{T}}$
2. $C_L^{\mathcal{S}\cap\mathcal{T}} = (C_L^{\mathcal{S}})^{\mathcal{T}}$

Using Lemma 5.1 and the circuits of $M(C_L)$ we get the following definition:

Definition 5.2. $C_L = C_L^{\mathcal{C}}$

Proof.

$$\begin{aligned} C_L &= \{\mathbf{w} \in (\mathbb{F}_q)^n : \mathbf{w} \cdot \mathbf{v} = 0, \forall C_L^*, \text{ with } supp(\mathbf{v}) \in \mathcal{C}\} \\ &= \bigcap_{c \in \mathcal{C}} \{\mathbf{w} \in (\mathbb{F}_q)^n : \mathbf{w} \cdot \mathbf{v} = 0, \forall C_L^*, \text{ with } supp(\mathbf{v}) = C\} \end{aligned}$$

This is because the words in C_L^* with support in $\mathcal{C}$, span the entirety of C_L^*. These are precisely the circuit vectors that we described in the definition of the $\delta_{OW} M_{C_L}$. They gave rise to a matroid where the rank was $r(\delta_{OW} M_{C_L})$. By Lemma 4.6 we know that this is $r(M_{C_L}^*) = dim(C_L^*)$. Therefore:

$$C_L = \bigcap_{c \in \mathcal{C}} \{\mathbf{w} \in (\mathbb{F}_q)^n : \mathbf{w}_C \in (C_L)_C\} = C_L^{\mathcal{C}}$$

□

Furthermore, we then immediately see that:

Lemma 5.3. *For any linear code C_L, we have $C_L^{\mathcal{T}} = C_L^{\mathcal{T} \cap \mathcal{C}}$.*

Proof. $C_L^{\mathcal{T} \cap \mathcal{C}} = C_L^{\mathcal{C}^{\mathcal{T}}} = C_L^{\mathcal{T}}$ Here we have assumed that $\mathcal{T}$ is a simplicial complex, but for $\mathcal{C}$, we do not need to consider any subset strictly contained in a circuit. This is because no codeword of C_L^* has support strictly contained in a circuit. □

This means that $C_L^{\mathcal{T}}$ is only dependent on those T in the simplicial complex $\mathcal{T}$, that are circuits.

Moreover, the linear equations cutting out $C_L^{\mathcal{T}}$ inside $(\mathbb{F}_q)^n$, obtained by circuits $C_1, C_2, ..., C_r$ are $\mathbf{w} \cdot \mathbf{v}$, for $Supp(\mathbf{v}) = C_i, i = 1, 2, ..., r$.

The coefficient matrix is then:

$$\begin{bmatrix} q_1 & q_2 & \cdots & q_r \\ & & & \end{bmatrix}$$

But the rank of this matrix is precisely the rank of this $r - set$ in $\delta_{OW}M[G]$, say S_r. Hence a collusion pattern, which separates C_{L_1} and C_{L_2} can be taken as a set of circuits whose ranks are different, viewed as subsets of the ground set of the derived matroid $\delta_{OW}M[G]$.

Let C_{L_1} and C_{L_2} be two linear codes in $(\mathbb{F}_q)^n$, such that $M_{C_{L_1}} = M[G_1] = M[G_2] = M_{C_{L_2}}$. The generator matrices G_1 and G_2 correspond respectively to codes C_{L_1} and C_{L_2}. We then say that a collusion pattern $\mathcal{T}$ separates C_{L_1} and C_{L_2} if $M_{C^{\mathcal{T}}_{L_1}} \neq M_{C^{\mathcal{T}}_{L_1}}$. An important result is the following Lemma.

Lemma 5.4. *Let C_{L_1} and C_{L_2} be linear codes with $M_{C_{L_1}} = M_{C_{L_1}}$, but $\delta_{OW}M_{C_{L_1}} \neq \delta_{OW}M_{C_{L_1}}$, then there exists at least one collusion pattern $\mathcal{T}$ which separates C_{L_1} and C_{L_2}.*

An extension of this which is even more powerful can be given as the following theorem.

Theorem 5.5. *Let C_{L_1} and C_{L_2} be two different linear codes with $M_{C^{\mathcal{T}}_{L_1}} = M_{C^{\mathcal{T}}_{L_1}}$. Then $\delta_{OW}M_{C^{\mathcal{T}}_{L_1}} = \delta_{OW}M_{C^{\mathcal{T}}_{L_1}}$ if and only if $M_{C^{\mathcal{T}}_{L_1}} = M_{C^{\mathcal{T}}_{L_1}}$ for all $\mathcal{T}$.*

Combining this with the example in Example 4.2, we see that the collusion pattern $T = \{q_5, q_6, q_7\} = \{\{1,2,5,6\},\{1,3,4,6\},\{2,3,4,5\}\}$ separates the matroids generated over $\mathbb{F}_2$ from $\mathbb{F}_3$.

Then we get the following $C^{\mathcal{T}}_{\mathbb{F}_i}$ for $i = 2$ or 3:

$$\begin{aligned} C^{\mathcal{T}}_{\mathbb{F}_2} = \{(x_1,x_2,x_3,x_4,x_5,x_6) : & x_1 + x_2 + x_5 + x_6 = 0, \\ & x_1 + x_3 + x_4 + x_6 = 0, \\ & x_2 + x_3 + x_4 + x_5 = 0\} \end{aligned}$$

$$C_{\mathbb{F}_3}^{\mathcal{T}} = \{(x_1, x_2, x_3, x_4, x_5, x_6) : x_1 - x_2 + x_5 - x_6 = 0,$$
$$x_1 - x_3 + x_4 + x_6 = 0,$$
$$x_2 - x_3 - x_4 + x_5 = 0\}$$

Furthermore, we can use this to show that $dim(C_{\mathbb{F}_2}^{\mathcal{T}}) = 6 - r(\{q_5, q_6, q_7\}) = 6 - 2 = 4$ and $dim(C_{\mathbb{F}_3}^{\mathcal{T}}) = 6 - r(\{q_5, q_6, q_7\}) = 6 - 3 = 3$.

6 School

In their new curriculum for mathematics R, the Norwegian government has put an increased focus on several core elements, which are to be vital in mathematics education in the years to come. The core elements this thesis will focus on are: *Exploration and problem-solving*, *Reasoning and argumentation*, and *Representation and communication* Utdanningsdirektoratet (2020). To be able to properly aid their pupils and students with these core elements, I believe a teacher must first have properly focused their attention on this study on their own. During the process of writing this master's thesis, I have had to focus on my ability to represent and properly formulate mathematical definitions, theorems, examples, and proofs. Furthermore, this has forced me to make sure my reasoning and argumentation are both sound and easily followed. I have chosen to formulate some of my own proofs or simplified others' proofs on several different occasions. This has made me more aware of the importance of mathematical reasoning and how to formulate this into arguments. When making my own proofs, or simplifying other's proofs I have had to take a deep dive into exploration and problem-solving. I have also had to think algorithmically and develop my own toolset to make sure that I would be able to analyze, reformulate and solve both known and unknown problems. I therefore believe that the skillset I have acquired by writing this thesis will support me in helping my future students, especially in fields regarding the core elements: *Exploration and problem-solving*, *Reasoning and argumentation*, and *Representation and communication*.

Summary

In this master's thesis, we spent the first three sections giving and proving several important definitions, theorems, lemmas, propositions, and corollaries regarding codes and matroids. We had a special a focus on proving the equivalence between the five different sets of axioms regarding matroids in Section 2.

In the fourth section, we studied three different concepts of derived matroids. First we looked at derived matroids defined over binary matroids as described by Longyear (1980). Afterwards, we looked at the derived matroid described by Oxley and Wang (2019). This matroid, was unlike the matroid described by Longyear, representable over all fields, but it needed a matrix (code) to be described. The last concept we studied was the one defined by Freij-Hollanti et al. (2023). This derived matroid functioned over all fields, like the one described by Oxley and Wang (2019), and did not need any matrix. Finally, we used some important properties proved in Freij-Hollanti et al. (2023) to prove that all circuits in the derived matroid defined by Oxley and Wang (2019) all belonged to a triplet if there were at least two circuits in the matroid.

In the last two sections of the thesis, we pointed toward some practical applications of derived matroids in Private Information Retrieval, as well as giving a reason for the thesis' relevance for me as a future teacher.

Bibliography

Freij-Hollanti, R., Jurrius, R., and Kuznetsova, O. (2023). Combinatorial derived matroids. *The Electronic Journal of Combinatorics*, 30(2):P2–8.

Freij-Hollanti, R. and Kuznetsova, O. (2021). Information hiding using matroid theory. *Advances in Applied Mathematics*, 129:102205.

Johnsen, T. and Verdure, H. (2013). *Code theory and matroid theory*. Manuscript UiT.

Johnson, S. L. (2016). A dual fano, and dual non-fano matroidal network. Master's thesis, California State University, San Bernardino.

Longyear, J. Q. (1980). The circuit basis in binary matroids. *Journal of Number Theory*, 12(1):71–76.

Oxley, J. and Wang, S. (2019). Dependencies among dependencies in matroids. *The Electronic Journal of Combinatorics*, 26(3).

Utdanningsdirektoratet (2020). Læreplan i matematikk for realfag (matematikk r) (mat03-02). `https://www.udir.no/lk20/mat03-02`. Accessed: 2018-12-06.

Wei, V. K. (1991). Generalized hamming weights for linear codes. *IEEE Transactions on information theory*, 37(5):1412–1418.

Whitney, H. (1935). On the abstract properties of linear dependence. *American Journal of Mathematics*, 57(3):509–533.

Wilson, R. J. (1979). *Introduction to graph theory*. Pearson Education India.