UiT
THE ARCTIC UNIVERSITY OF NORWAY

Faculty of Science and Technology
Department of Mathematics and Statistics

Simplicial complexes, Demi-matroids, Flag of linear codes and pair of matroids

—

Ali Zubair
MAT-3900 Master's thesis in Mathematics May 2015

Abstract

We first describe linear error-correcting codes, and show how many of their most important properties are determined by their associated matroids . We also introduce the simplicial complex of the independent sets of a matroid.

We then proceed to study flags of linear codes, and recall the definition of demi-matroids, and how such demi-matroids associated to flags can describe important properties of these flags, analogous to how individual codes are described by associated matroids. We also study the interplay between demi-matroids and simplicial complexes.

To Karoline Skoge,
for everything she has done for me.

Acknowledgements

I would like to pay all thanks to my supervisor Professor Trygve Johnsen, Head of the Department of Mathematics and Statistics at the UiT The Arctic University of Norway. For he has been a great motivational personality for the completion of this thesis. I felt extremely lucky that I had a chance to work with Hugues Verdure, since without his help the quality of this thesis could not have been the same. I would like to thank my class fellows Anna Karpova and Violeta Huerga, for their great help during this study period.

I am very thankful to my family, especially my parents and brothers for their encouragement and humble token of affection.

Contents

Introduction

In matroid theory one is mainly interested in studying the fundamentals of linear algebra and mainly the notion of independence. A matroid M is an ordered pair $(E,\mathcal{I})$, with a finite set E called ground set and $\mathcal{I}$ is the collection of subsets of E. We will study matroids, and its many and equivalent definitions, formulated by its independent sets $\mathcal{I}$, basis $\mathcal{B}$, circuits $\mathcal{C}$, and its perhaps most important tool, the rank function r. The rank function of a matroid is a strong characterisation which is very useful in the study of linear codes and their generator matrices. To a detailed literature on the topics of matroids and linear codes, the readers should give importance to [12] and [7] which have been the main source of our study for the completion of this thesis.

In Chapter 1 we give basic definitions of codes, codewords and linear codes, including concepts as Hamming weights and minimum distance of linear codes.

In Chapter 2 we will cover fundamentals of matroid theory including a basic definition of a matroid and other equivalent defintions and remind the reader of well known results showing how these definitions are linked with each other. The basic purpose of these equivalent definitions is to show how one can find out the complete structure of a matroid from each equivalent set of information.

We also study matroids associated to linear codes, and the minimum distance and weight hierarchy of matroids. A main purpose with this is to show how much important information and data describing linear codes are in fact describable by properties of the associated matroids.

In Chapter 3 we study simplicial complexes and Stanley-Reisner ideals and facet ideals, which are of monomial ideals, and give the basics of abstract algebra in form of grading of modules and free resolutions and their Betti-numbers. A brief literature on these topics can be found in [3].

In Chapter 4 we turn to demi-matroids, a strictly wider class of objects than that of matroids. We show how many important properties of matroids carry over to this wider class, which even enjoys properties that the stricter class (of matroids) does not enjoy (an extra duality). We show how the usage of demi-matroids is relevant in the study of pairs of codes (where one is the subset of the other one). We hope his thesis is a good tool for students studying demi-matroids, since we briefly cover demi-matroids in Chapter 4. In this chapter we study basic defintion of a demi-matroid and with the help of examples we elaborate the relation between a matroid and a demi-matroid. Along with duality of demi-matroid and flag of linear codes we cover briefly the study of a demi-matroids and simplicial complexes. At the end of this chapter we have some open questions for the readers and later work.

In Chapter 5 we study pair of matroids and Betti-numbers of matroids, and to what extent properties of pairs of code as described can carry over to relevant pairs of matroids.

Chapter 1

Linear codes

1.1 Linear codes

Definition 1.1. A finite set of symbols is called an alphabet.

Definition 1.2. Let A be a finite alphabet given by $\{a_1, \ldots, a_q\}$, where $q \in \mathbb{N}$. Then a codeword over A is an element (n-tuple) of A^n for some $n \in \mathbb{N}_0$ and A^0 is the empty word.

Example 1.1.1. If $A = \{a, b, \ldots, y, z\}$ then $a \in A$, $(a, b) \in A^2$ and $(x, y, z) \in A^3$.

The set of all possible code words is given by $V = \{\emptyset\} \cup A \cup A^2 \cup A^3 \ldots$

Definition 1.3. A code is a subset of V i.e $\mathcal{C} \subseteq V$.

Example 1.1.2. If $A = \{a, b, \ldots, y, z\}$ then a list of all English words is a code.

Definition 1.4. A block code $\mathcal{C}$ is a subset of A^n for a fixed value of code word length n i.e $\mathcal{C} \subseteq A^n$,$n \geq 1$.

Definition 1.5. If A is an alphabet and A^n be the set of all words of word length n. Let $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ be two words in A^n. The Hamming distance between x and y is

$$d(x, y) = \#\{i, x_i \neq y_i\}$$

Definition 1.6. The minimum distance of a code $\mathcal{C}$ is

$$d = Min\{d(x, y) \mid x, y \in \mathcal{C}, x \neq y\}$$

This is well defined, as well as the code is not reduce to 1 codeword.

Remark 1.1. One can find this definition [12, Definition 2.5]

Remark 1.2. A code $\mathcal{C}$ has parameters defined as follows: q is the size of the alphabet, n is the length of the codewords, d is the minimal distance, M is the cardinality of $\mathcal{C}$

Theorem 1.1. *Let $\mathcal{C}$ be a code with minimum distance d. Then we can detect up to $d - 1$ errors.*

Proof. Let x be the sent codeword, and y the received codeword. Saying that there has been up to $d - 1$ errors is the same as saying that $d(x, y) \leqslant d - 1$. We can say that there has been errors if y is not a codeword. But if y was a codeword different from x, then

$$d = min\{d(u, v) \mid u, v \in \mathcal{C}, u \neq v\} \leqslant d(x, y) \leqslant d - 1$$

which is absurd. □

Definition 1.7. A linear code over a finite field $\mathbb{F}_q$ is a vector subspace of the vector space $\mathbb{F}_q^n$.

An $[n, k, d]_q$ code is a linear code over a finite field $\mathbb{F}_q$ with length n, dimension k and minimum distance d. If we do not specify the minimum distance d it is called an $[n, k]_q$ code.

Remark 1.3. The all zero vector is necessarily a codeword of any linear code.

Remark 1.4. Instead of listing all the codewords of a linear code, we just need to make a list of a basis. We can then find all the codewords as linear combinations of this basis.

Example 1.1.3. Let $\mathcal{C}$ be the $[8, 2]_3$ code, with basis $v_1 = 00111222$ and $v_2 = 12012012$. Then the set of codewords is

λ_1	λ_2	*codeword*
0	0	00000000
0	1	12012012
0	2	21021021
1	0	00111222
1	1	12120201
1	2	21102210
2	0	00222111
2	1	12201120
2	2	21210102

It is now easy to see that all non-zero codewords have weight 6.This is therefore a $[8,2,6]_3$ code. These types of codes are called one weight codes.

Definition 1.8. The weight of a codeword x is

$$wt(x) = \#\{i, x_i \neq 0\}$$

Lemma 1.1. *Let x, y be two codewords of a code. Then*

$$d(x,y) = wt(x-y)$$

Proof. We have

$$d(x,y) = \#\{i \mid x_i \neq y_i\}$$
$$= \#\{i \mid x_i - y_i \neq 0\} = wt(x-y)$$

From this, we can reformulate the definition of minimum distance, also called Hamming distance of the code. □

Theorem 1.2. *Let $\mathcal{C}$ be a linear code. Then*

$$d = Min\{wt(x) \mid x \in \mathcal{C} - \{(0,...,0)\}\}.$$

Proof. The proof of this theorem can be found in [12] □

Example 1.1.4. We illustrate an example to elaborate above Lemma 1.1. Let $x = (1,0,0,1)$ and $y = (1,1,0,1)$ be two codes words of a code. Then $wt(x) = 2$ and $wt(y) = 3$. Since number of non-zero places in x and y is 2 and 3 simultaneously. Also, $wt(x-y) = wt(0,1,0,0) = 1$ and distance $d(x,y) = 1$ i.e total number of places such that $x_i \neq y_i$ is just 1 and it gives us the final result i.e $d(x,y) = wt(x,y)$.

Theorem 1.3. *Let $\mathcal{C}$ be a linear code. Then*

$$d = Min\{wt(x) \mid x \in \mathcal{C} - \{(0, ..., 0)\}\}.$$

Proof. The proof of this theorem can be found in [12] □

Definition 1.9. The support of a codeword x is

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

The support of a set of the codewords is the union of the supports of its codewords.

$$Supp(\mathcal{S}) = \bigcup_{x \in \mathcal{S}} Supp(x)$$

Definition 1.10. Let $\mathcal{C}$ be a $[n, k]_q$ code. Then the generalized Hamming weights are

$$d_i = min\{\#supp(\mathcal{D}) \mid \mathcal{D} \text{ is a subcode of dimension } i \text{ of } \mathcal{C})\}$$

where $1 \leqslant i \leqslant k$. The sequence $(d_1, \ldots, d_k)$ is called the weight hierarchy of the code $\mathcal{C}$.

Proposition 1.1. *The weight hierarchy of a code is a strictly increasing sequence.*

Proof. Let $\mathcal{D}$ is a subcode of dimension $i + 1$ of minimal support with $v_1, \ldots, v_{i+1}$ be a basis. Then the subcode $\mathcal{D}' =< v_1, \ldots, v_i >$ is of dimension i, and $Supp(\mathcal{D}') \subset Supp(\mathcal{D})$. So

$$d_i \leqslant \#Supp(\mathcal{D}') \leqslant \#Supp(\mathcal{D}) = d_{i+1}.$$

Now, by choosing a good basis of $\mathcal{D}$, we can make the inclusion strict. Let j be such that $a = (v_{i+1})_j \neq 0$. It has to exist since $v_{i+1} \neq 0$ as a basis vector.

Consider the vectors, for $1 \leqslant j \leqslant i$,

$$w_k = v_k - \frac{(v_k)_j}{a} v_{i+1}.$$

By construction,

$$(w_k)_j = (v_k)_j - \frac{(v_k)_j}{a} (v_{i+1})_j = 0$$

Moreover, we claim that $w_1, \ldots, w_i, w_{i+1}$ is a basis. It is generating: it suffices to show that all the basis vectors v_i can be expressed as a linear combinations of the new vectors. This is obviously true for v_{i+1}. And this is true for v_k for $k \leqslant i$ since $v_k = w_k + \frac{(v_k)_j}{a} v + i + 1$. We also have to show that this is free. But let $\lambda_1, \ldots, \lambda_{i+1}$ such that

$$0 = \sum_{k=1}^{i} \lambda_k w_k + \lambda_{i+1} v_{i+1} = \sum_{k=1}^{i} \lambda_k (v_k - \frac{(v_k)_j}{a} v_{i+1}) + \lambda_{i+1} v_{i+1}.$$

Since the v_k are free, this shows that $\lambda_1 = \ldots = \lambda_i = 0$. And then, $\lambda_{i+1} v_{i+1} = 0$, which in turn implies that $\lambda_{i+1} = 0$.

Now, if we see at the code $\mathcal{D}'$, we see that no basis elements has j in its support, while is was in the support of $\mathcal{D}$. This shows that the inequalities are strict. □

Definition 1.11. Let $\mathcal{C}$ be a $[n, k]_q$ code. Then a $n \times k$ matrix over F_q whose rows form a basis of $\mathcal{C}$ is called a generator matrix.

Definition 1.12. A generator matrix of the form $[I_k \mid A]$ is said to be a standard form of generator matrix. Where I_k is a $k \times k$ identity matrix and A is an $k \times (n-k)$ matrix.

Definition 1.13. Let $\mathcal{C}$ be a $[n, k]_q$ linear code then the $[n, n-k]_q$ linear code defined as $\mathcal{C}^{\perp} = \{Y \in \mathbb{F}_q^n \mid X \bullet Y = 0, \forall X \in \mathcal{C}\}$ is called the dual of the code.

Definition 1.14. A parity check matrix of a linear code $\mathcal{C}$ is a generator matrix of $\mathcal{C}^{\perp}$.

Proposition 1.2. *If A,B are the generator and parity check matrix of the linear code $\mathcal{C}$ respectively then they are parity check and generator matrix of the dual.*

Proof. This is the immediate consequence of the definition and [12, Corollary 4.3] □

Theorem 1.4 (Wei's duality)**.** *Let $\mathcal{C}$ be a linear $[n, k]_q$ code and $\mathcal{C}^{\perp}$ be its dual and let $d_1 \leq \ldots \leq d_k$ and $e_1 \leq \ldots \leq e_{n-k}$ be the weight hierarchies of $\mathcal{C}$ and $\mathcal{C}^{\perp}$ respectively. Then*

$$\{d_1, \ldots, d_k, n+1-e_1, \ldots, n+1-e_{n-k}\} = \{1, \ldots, n\}$$

Proof. The proof of this theorem will be given in the context of matroids and linear codes. □

Theorem 1.5. *Let $\mathcal{C}$ be a linear $[n,k]_q$ code whose generator matrix is G in its standard form,*

$$G = [I_k \quad | \quad A]$$

Then a parity check matrix for $\mathcal{C}$ is given by

$$H = [-A^t \quad | \quad I_{n-k}]$$

Proof. [12, Theorem 4.6] □

Definition 1.15. A parity check matrix is said to be in its standard form when it is of the form,

$$H = [B \quad | \quad I_{n-k}]$$

Example 1.1.5. Let $\mathcal{C}$ be a linear $[4,2]_2$ code. Its generator matrix is:

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

and its parity check matrix have its standard form as:

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

Chapter 2

Matroids

2.1 Matroids via independent sets

Let V be a vector space and $v_1, \ldots, v_n$ be vectors in V. We consider the set

$$\mathcal{I} = \{X \in 2^{\{v_1,\ldots,v_n\}}, X \text{ is a linearly independent set}\}$$

This set has at least the following properties:

(1) It is not empty: $\emptyset \in 2^{\{v_1,\ldots,v_n\}}$ is linearly independent.

(2) It is closed under taken subsets: if I is a linearly independent, then any subset $J \subseteq I$ is also linearly independent.

(3) If I, J are two linearly independent sets, and $|I| < |J|$, then there is at least one element $j \in J$ such that $I \cup \{j\}$ is linearly independent.

Definition 2.1. Let E be a finite set and $\mathcal{I}$ be a collection of the subsets of the finite set E. Then the ordered pair $(E, \mathcal{I})$ is called a matroid M if it satisfies the following three conditions:

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

$(I2)$ If $J_1 \in \mathcal{I}$ and $J_2 \subseteq J_1$, then $J_2 \in \mathcal{I}$,

$(I3)$ If J_1 and J_2 are both elements of $\mathcal{I}$ with $|J_1| < |J_2|$, then there exists $x \in J_2 \setminus J_1$ such that $J_1 \cup \{x\} \in \mathcal{I}$.

Condition $(I3)$ is called the independence augmentation axiom.

If M is the matroid $(E, \mathcal{I})$, then M is called a matroid on E. The member of $\mathcal{I}$ are the independent sets of M, and E is the ground set of M. A subset of E that is not in $\mathcal{I}$ is called dependent.

Example 2.1.1. Let $E = \{1, 2, 3, 4\}$, and consider

$$\mathcal{I} = \{\{1, 2\}, \{1, 4\}, \{2, 3\}, \{3, 4\}, \{1\}, \{2\}, \{3\}, \{4\}, \emptyset\}$$

Then $M = (E, \mathcal{I})$ is a matroid. The only non-trivial thing we have to show is property $I3$. If $I1 = \emptyset$, then the verification is trivial. If $|I1| = 1$, then the verification is trivial if $I1 \subseteq I2$. So we just have to check the cases where $|I1| = 1, |I2| = 2$ but $I1 \nsubseteq I2$. It remains the couples: $(\{1\}, \{2, 3\}), (\{1\}, \{3, 4\}), (\{2\}, \{1, 4\}), (\{2\}, \{3, 4\}), (\{3\}, \{1, 2\}), (\{3\}, \{1, 4\})$ $(\{4\}, \{1, 2\}), (\{4\}, \{2, 3\})$. But it is easy to check that we can always find an element in $I2$ such that $I1$ plus this element is an independent set. Look for example at $(\{2\}, \{3, 4\})$. While $\{2\} \cup \{4\}$ is not independent, $\{2, 3\} = \{2\} \cup \{3\}$ is.

Example 2.1.2. Let $E = \{1, 2, 3, 4\}$, and consider

$$I = \{\{1, 2\}, \{2, 3\}, \{3, 4\}, \{1\}, \{2\}, \{3\}, \{4\}, \emptyset\}$$

Then $M = (E, \mathcal{I})$ is not a matroid. Namely, let $I1 = \{1\}$ and $I = \{3, 4\}$. Here neither $\{1\} \cup \{3\}$ nor $\{1\} \cup \{4\}$ are independent.

Definition 2.2. Two matroids $M_1 = (E_1, \mathcal{I}_1)$ and $M_2 = (E_2, \mathcal{I}_2)$ are isomorphic if there exists a bijection $\phi : E_1 \to E_2$ such that

$$X \in \mathcal{I}_1 \Leftrightarrow \phi(X) \in \mathcal{I}_2$$

Let M and N be two matroids on the ground sets E and F respectively are said to be isomorphic if and only if there exists a bijection $\phi : E \to F$ such that $B \subset E$ is a basis of M if and only if $\phi(B)$ is a basis of N.

Example 2.1.3. Let V be a vector space and $v_1, \ldots, v_n$ be vectors in V. We consider the set

$$\mathcal{I} = \{X \in 2^{\{1, \cdots, n\}}, \{v_k, k \in X\} \text{ is a linearly independent set } \}$$

Then $M = (\{1, \ldots, n\}, \mathcal{I})$ is a matroid. A matroid isomorphic to such a matroid is called a vector matroid or a representable matroid. If the $v_i' s$ are the columns of a matrix A, then the associated vector matroid is denoted by $M[A]$

Example 2.1.4. Let A be the matrix

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

over the field of real numbers $\mathbb{R}$. Then $E = \{1, 2, 3, 4, 5\}$ and

$$\mathcal{I} = \{\emptyset, \{1\}, \{2\}, \{4\}, \{5\}, \{1, 2\}, \{1, 5\}, \{2, 4\}, \{2, 5\}, \{4, 5\}\}.$$

2.2 Matroids via bases

Definition 2.3. Let $M = (E, \mathcal{I})$ be a matroid. A maximal independent set is called a base of a M and the set of bases is denoted by $\mathcal{B}$.

Proposition 2.1. *The bases of a matroid have the same cardinality.*

Proof. Suppose this is not the case and let B_1, B_2 be two bases with different cardinality, and we may assume that $|B_1| < |B_2|$. Since they are independent sets, axiom $(I3)$ says that we can find an element $x \in B_2 - B_1$ such that $B_1 \cup \{x\}$ still is independent. But this contradicts with the fact that B_1 is a base. Thus bases of a matroid have the same cardinality. □

Proposition 2.2. *(Base change). Let B_1, B_2 be two distinct bases of a matroid. Let $x \in B_2 \backslash B_1$. Then there exists $y \in B_1 \backslash B_2$ such that $B_2 \cup \{y\} \backslash \{x\}$ is a basis of the matroid.*

Proof. We have $|B_2 \backslash \{x\}| = |B_2| - 1 < |B_1|$. So from (I_3), there exists $y \in B_1 \backslash (B_2 \backslash \{x\} = B_1 \backslash B_2)$ such that $B_2 \cup \{y\} \backslash \{x\}$ is independent. By cardinality of this independent set, it has to be maximal, and it is therefore a basis. □

Definition 2.4. Let E be a finite set and $\mathcal{B}$ be a set of subsets of E. We say that $\mathcal{B}$ is a set of bases if it satisfies the two following axioms

(B_1) $\mathcal{B} \neq \emptyset$,

(B_2) $\forall B_1, B_2 \in \mathcal{B}$, $\forall x \in B_2 \setminus B_1$, $\exists y \in B_1 \setminus B_2$, $B_2 \cup \{y\} \setminus \{x\} \in \mathcal{B}$.

Corollary 2.1. *Let $M = (E, \mathcal{I})$ be a matroid. Then its set of bases $\mathcal{B}$ is a set of bases (in the sense of the definition).*

Proof. [12, Corollary 6.2] □

Lemma 2.1. *Let $\mathcal{B}$ be a set of bases on E. Then all the element in $\mathcal{B}$ have the same cardinality.*

Proof. If this is not the case, let B_1 and B_2 in $\mathcal{B}$ such that $|B_2| > |B_1|$ and $|B_2 \backslash B_1| > 0$ is minimal. Let $x \in B_2 \backslash B_1$, from axiom $(B2)$, there exists $y \in B_1 \backslash B_2$ such that $B_3 = B_2 \cup \{y\} \backslash \{x\} \in \mathcal{B}$. It is obvious that $|B_3| = |B_2|$. But this time we have $|B_2 \backslash B_1| > |B_3 \backslash B_1| > 0$. The first inequality comes from the fact that we took an element in B_2 that was not in B_1, and added an element in B_1 which was not in B_2, the second one that B_3 is bigger than B_1.

□

Remark 2.1. The previous lemma seems to be the same as Proposition 2.1, but it is not, since we can not use the axiom $(I3)$

Theorem 2.1. *Let $\mathcal{B}$ be a set of bases on E. Let $\mathcal{I} = \{X \subset B, B \in \mathcal{B}\}$. Then $M(\mathcal{B}) = (E, \mathcal{I})$ is a matroid, whose set of bases is $\mathcal{B}$.*

Proof. [12, Theorem 6.4] □

2.3 Matroids via Circuits

Definition 2.5. A minimal dependent set is a subset of E whose proper subsets are independent.

Definition 2.6. A minimal dependent subset of E is called a circuit C of the matroid M.

Remark 2.2. A matroid is uniquely determined by its set of circuits $\mathcal{C}$, since $\mathcal{I}$ can be obtained from $\mathcal{C}$.

Proposition 2.3. *The circuits of a matroid $\mathcal{C}$ satisfy the following properties:*

(C_1) $\emptyset \notin \mathcal{C}$

(C_2) if $C_1, C_2 \in \mathcal{C}$ with $C_1 \subset C_2$, then $C_1 = C_2$.

(C_3) *If $C_1, C_2 \in \mathcal{C}$ then for any $e \in C_1 \cap C_2$, there is $C_3 \in \mathcal{C}$ such that $C_3 \subset (C_1 \cup C_2) - \{e\}$.*

Proof. The first two properties are obvious since if $\emptyset$ is a circuit, then it would not be an independent set and that would contradict with $(I1)$, and the second one comes from the minimality of circuits.

Let us show the third property. Since C_i is a circuit, we have

$$r(C_i) = |C_i| - 1.$$

Since C_1 and C_2 are distinct, $C_1 \cap C_2$ is strictly included in a circuit, and therefore independent. We therefore know that $r(C_1 \cap C_2) = |C_1 \cap C_2|$. This gives us that

$$r(C_1 \cup C_2) + r(C_1 \cap C_2) \leqslant r(C_1) + r(C_2)$$

or

$$r(C_1 \cup C_2) \leqslant |C_1| - 1 + |C_2| - 1 - |C_1 \cap C_2| = |C_1 \cup C_2| - 2.$$

Now, we have

$$r((C_1 \cup C_2)\backslash\{e\}) < |(C_1 \cup C_2) - \{e\}|.$$

This shows that $(C_1 \cup C_2)\backslash\{e\}$ is dependent and contains therefore a circuit. □

Remark 2.3. The property (C_3) is often called the weak (or global) elimination axiom for circuits, as opposed to the strong (or local) elimination axiom for circuits just below.

Proposition 2.4. *Let E be a finite set and $\mathcal{C}$ be a set of subsets of E. Let (C_3') be the following property:*

(C_3') If $C_1, C_2 \in \mathcal{C}$ are distinct and not disjoint, then for any $e \in C_1 \cap C_2$ and $f \in C_1\backslash C_2$, there exists $C_3 \in \mathcal{C}$ such that $f \in C_3 \subset (C_1 \cup C_2)\backslash\{e\}$.

Then the properties $(C_1), (C_2)$ and (C_3) are equivalent to the properties $(C_1), (C_2)$ and (C_3).

Proof. [12, Proposition 21] □

Theorem 2.2. *Let E be a finite set, and $\mathcal{C}$ satisfying the axioms (C_1), (C_2) and (C_3). Let*

$$\mathcal{I} = \{X \subseteq E,\ \nexists C \in \mathcal{C}, C \subseteq X\}$$

Then $(E, \mathcal{I})$ is a matroid whose set of circuits is $\mathcal{C}$.

Proof. [12, Theorem 6.7] □

Definition 2.7. Let $M = (E, \mathcal{I})$ be a matroid. If $\{e\} \in \mathcal{C}$, then e is called a loop. If $\{e_1, e_2\} \in \mathcal{C}$, then e_1 and e_2 are called parallel elements.

Example 2.3.1. We look at the following example to give a brief explanation for independent sets, bases and circuits. Given a vector matroid $M[A]$, where

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

over the field of real numbers. Then $E = \{1, 2, 3, 4, 5\}$ and

$$\mathcal{I} = \{\emptyset, \{1\}, \{2\}, \{3\}, \{4\}, \{5\}, \{1,2\}, \{1,3\}, \{1,5\}, \{2,3\}, \{2,4\}, \{2,5\}, \{3,4\},$$

$$\{3,5\}, \{4,5\}, \{1,2,3\}, \{1,2,5\}, \{1,3,5\}, \{2,3,4\}, \{2,4,5\}, \{3,4,5\}\}.$$

$$\mathcal{B} = \{\{1,2,3\}, \{1,2,5\}, \{1,3,5\}, \{2,3,4\}, \{2,4,5\}, \{3,4,5\}\}.$$

$$\mathcal{C} = \{\{1,4\}, \{2,3,5\}\}$$

2.4 Matroids via rank function

Definition 2.8. Let $M = (E, \mathcal{I})$ be a matroid. Then rank function of the matroid M is the function:

$$r : 2^E \longrightarrow \mathbb{N}$$

$$X \mapsto Max\{|I|, I \subset X, I \in \mathcal{I}\}$$

The nullity function is $n : 2^E \longrightarrow \mathbb{N}$ defined by

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

We shall write $r(M) = r(E)$ by abuse of notation.

Proposition 2.5. *Let $X \subseteq E$, then*

$$r(X) = Max\{|B \cap X|, B \in \mathcal{B}\}$$

Proof. For any $B \in \mathcal{B}$, $B \cap X \in \mathcal{I}$, and therefore $|B \cap X| \leqslant r(X)$. The same is of course true if we impose that $|B \cap X|$ is maximal. Conversely, let $I \subset X$ such that $r(X) = |I|$. Let B be a basis containing I. Then we have $|I| = r(X) \leqslant |B \cap X|$ and the other inequality is proved. □

The rank function has the following properties:

$((R1)')$ If $X \subseteq E$, then $0 \leqslant r(X) \leqslant |X|$

$((R2)')$ If $X \subseteq Y \subseteq E$, $r(X) \leqslant r(Y)$.

Furthermore:

Lemma 2.2. *The rank function r of a matroid M on a set E satisfies the following condition:*

$((R3)')$ If X, Y are the subsets of E, then

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

Proof. [7, Lemma 1.3.1] □

Proposition 2.6. *The rank function of a matroid $M = (E, \mathcal{I})$ satisfies the following properties:*

$(R1)$ $r(\emptyset) = 0$

$(R2)$ *If $X \subseteq E$ and $x \in E$, then $r(X) \leqslant r(X \cup x) \leqslant r(X) + 1$*

$(R3)$ *If $X \subseteq E$, and $x, y \in E$ are such that $r(X \cup \{x\}) = r(X \cup \{y\}) = r(X)$, then $r(X \cup \{x, y\}) = r(X)$.*

Proof. $R1$ is obvious. We shall prove $(R2)$. In $(R2)$ the first inequality is also obvious since if $I \subset X$, then $I \subset X \cup \{x\}$. For the second inequality, let $I \in \mathcal{I}$ such that $I \subset X \cup \{x\}$ and $|I| = r(X \cup \{x\})$. Then we have two cases. Either $x \notin I$. Then $I \subset X$, and therefore $|I| \leqslant r(X) \leqslant r(X \cup \{x\}) = |I|$ and second inequality.

Now if $x \in X$, let $J = I - \{x\}$. Then obviously, $J \in \mathcal{I}$ and $J \subset X$. Therefore $|J| \leqslant r(X) \leqslant r(X \cup \{x\}) = |I| = |J| + 1 \leqslant r(X) + 1$ and the inequality holds.

For $(R3)$, assume this is not the case, that is

$$r(X \cup \{x, y\}) > r(X).$$

In particular, there exists two independent sets I, J such that $I \subset X \cup \{x, y\}$, $J \subset X$, with $|I| = r(X \cup \{x, y\}) > r(X) = |J|$. From axiom $(I3)$, there exists an element $z \in I \backslash J$ such that $J' = J \cup \{z\}$ is still independent. But since

$I \subset X \cup \{x, y\}$, we have three possibilities which are $z \in X$, $z = x$, or $z = y$. Now if $z \in X$, then $J' \subset X$ and $|J'| = |J| + 1$ which contradicts the maximality of the cardinality of J. If $z = x$, then $J' \subset X \cup \{x\}$, and then $r(X \cup \{x\}) \leqslant |J'| = |J| + 1 = r(X) + 1$ which is also a contradiction. The same proof applies to the third case.

□

Theorem 2.3. *Let E be a finite set and $r : 2^E \longrightarrow \mathbb{N}$ a function satisfying $(R1), (R2), (R3)$. Then if*

$$\mathcal{I} = \{I \in 2^E, r(I) = |I|\},$$

then $(E, \mathcal{I})$ is a matroid, with set of bases

$$\mathcal{B} = \{I \in 2^E, r(E) = r(I) = |I|\},$$

and rank r.

Proof. Since $r(\emptyset) = 0 = |\emptyset|$, the axiom $(I1)$ is satisfied. Suppose that there exists $I_2 \in \mathcal{I}$ and $I_1 \subset I_2$ such that $I_1 \notin \mathcal{I}$. Let I_1 maximal with such a property. Let $x \in I_2 - I_1$. Then $I_3 = I_1 \cup \{x\} \in \mathcal{I}$ by maximality of I_1. This means that

$$|I_1| + 1 = |I_3| = r(I_3) = r(I_1 \cup \{x\}) \leqslant r(I_1) + 1$$

This gives $r(I_1) \geqslant |I_1|$

And $(R2)'$ says that there is actually equality, that is, $I_1 \in \mathcal{I}$.

We show now that $(I3)$ is satisfied. Let $I_1, I_2 \in \mathcal{I}$ with $|I_1| < |I_2|$. Suppose that for every $x \in I_2 \backslash I_1$, $I_1 \cup \{x\} \notin \mathcal{I}$. We translate all this information into rank language:

$$I_1 \in \mathcal{I} \Leftrightarrow r(I_1) = |I_1|.$$

$$I_2 \in \mathcal{I} \Leftrightarrow r(I_2) = |I_2|.$$

$\forall x \in I_2 \backslash I_1, |I_1| = r(I_1) \leqslant r(I_1 \cup \{x\}) < |I_1 \cup \{x\}|$

This implies $r(I_1 \cup \{x\}) = r(I_1)$.

An easy recursion on $(R3)$ shows then that

$$r(I_1 \cup I_2) = r(I_1 \cup (I_2 \backslash I_1)) = r(I_1) = |I_1|.$$

But by $(R2)'$, $r(I_1 \cup I_2) \geqslant r(I_2) = |I_2|$, this gives us that

$$|I_1| \geqslant |I_2|$$

which is absurd.

We now prove that the rank function s of the matroid $(E, \mathcal{I})$ is equal to r. Let $X \subset E$. If $X \in \mathcal{I}$, then by definition of s, we have $s(X) = |X|$. But by definition of $\mathcal{I}$, we also have $r(X) = |X|$, so that $r(X) = s(X)$. If $X \notin \mathcal{I}$, let $I \in \mathcal{I}$ be maximal (for cardinality) such that $I \subset X$. We have then

$$s(X) = |I| = r(I)$$

so we just need to show that $r(X) = r(I)$. For every $x \in X \backslash I$, we necessarily have $r(I \cup \{x\}) < |I \cup \{x\}| = |I| + 1$ by maximality of I, and since $|I| = r(I) \leqslant r(I \cup \{x\})$, we have $r(I \cup \{x\}) = r(I) = |I|$. Earlier in the proof, we showed that this means that

$$r(I \cup (X \backslash I)) = r(I).$$

But in our case, this means that

$$r(X) = r(I \cup (X \backslash I)) = r(I) = |I| = s(X).$$

In particular, it shows that since any basis B is a maximal subset of E in $\mathcal{I}$, it shows that $r(E) = r(B) = |B|$ and this completes the proof.

□

Proposition 2.7. . *Let M be a matroid with rank function r and suppose $X \subset E$. Then*

(i) X is independent $\Leftrightarrow |X| = r(X)$.

(ii) X is a basis $\Leftrightarrow |X| = r(X) = r(M)$

(iii) X is a circuit $\Leftrightarrow X$ is non empty and for all $x \in X$, $r(X - x) = |X| - 1 = r(X)$

Proof. [12, Corollary 6.6] □

Proposition 2.8. *Let A be a $k \times n$matrix with $k \leqslant n$. Then the rank function of the matroid $M[A]$ is given by:*

$$r(X) = rank(A[X])$$

where $A[X]$ is the matrix formed by the columns of A indexed by X.

Proof. By definition, $r(X)$ is equal to the highest number of independent columns of A indexed by X. But this is precisely the rank of $A[X]$. □

2.5 Duality

Theorem 2.4. *Let M be a matroid on the ground set E with a set of bases $\mathcal{B}$. Let*

$$\mathcal{B}^* = \{E - B, B \in \mathcal{B}\}.$$

Then M^* is a matroid on the ground set E with the set of bases $\mathcal{B}^*$.

Proof. [12, Theorem 7.2] □

Definition 2.9. Let M be a matroid on the ground set E with set of bases $\mathcal{B}$. Then a matroid on E with set of bases $\mathcal{B}^*$ is called the dual of matroid M and is deonted by M^*.

Remark 2.4. We have $(M^*)^* = M$.

Definition 2.10. Let M be a matroid, then

(1) The elements of $\mathcal{I}(M^*)$ are the coindependent sets of M

(2) The elements of $\mathcal{B}(M^*)$ are the cobases of M

(3) The elements of $\mathcal{C}(M^*)$ are the cocircuits of M

(4) The rank function of M^* is called the corank function of M

(5) A coloop of M is a loop of M^*

Example 2.5.1. Let M be the matroid on ground set E of Example 2.3.1. The dual matroid M^* has set of bases $\mathcal{B}^*$, set of independent sets $\mathcal{I}^*$ and set of circuits of $\mathcal{C}^*$ are given by:

$$\mathcal{B}^* = \{\{1,2\},\{1,3\},\{1,5\},\{2,4\},\{3,4\},\{4,5\}\}.$$

$$\mathcal{I}^* = \{\emptyset,\{1\},\{2\},\{3\},\{4\},\{5\},\{1,2\},\{1,3\},\{1,5\},\{2,4\},\{3,4\},\{4,5\}\}.$$

$$\mathcal{C}^* = \{\{1,4\},\{2,3\},\{2,5\},\{3,5\}\}.$$

Proposition 2.9. *Let M be a matroid on the ground set E with rank r. Then the rank of M^* is $\#E - r$.*

Remark 2.5. Note that in this proposition, we talk about the rank of the matroid, not the rank function. The rank of the matroid is by definition the rank function applied to E.

Proof. The rank of M is equal to the cardinality of any base. Then the cardinality of any base of M^* is equal to $\#E - r$ □

Theorem 2.5. *Let M be a matroid on the ground set E with rank function r. Then the rank function r^* of M^* is given by*

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

Proof. [12, Theorem 7.3] □

Corollary 2.2. *Let M be a matroid of nullity function n. Then the nullity function n^* of M^* is given by*

$$n^*(X) = |X| - n(E) + n(E - X)$$

2.6 Linear codes and matroids

Theorem 2.6. *Let M,N be two isomorphic matroids. Then $M^*$and N^* are isomorphic.*

Proof. [12, Theorem 7.5] □

Lemma 2.3. *Let A be a matrix over a field and B be obtained from A by one of the following operations:*

(M_1) Permute the rows

(M_2) Multiply a row by a non- zero number of the ground field

(M_3) Replace a row by the sum of the row and a multiple scalar of another row

(M_4) Adjoin or remove a zero row

(M_5) Permute the columns

(M_6) Multiply a column by a non-zero number of the ground field. Then the matroids $M[A]$ and $M[B]$ are isomorphic.

Proof. The proof of this lemma is the same as for equivalence of linear codes [12, Theorem 4.7]. All the opereations remain same, only (M_5) gives an isomorphic matroid. □

Theorem 2.7. *Let A be a $l \times m$ matrix of the form*

$$A = [I_l \mid A].$$

Let B be the $(m-l) \times m$

$$B = [-A^t \mid I_{m-l}]$$

Then

$$M[A]^* = M[B]$$

Proof. [12, Theorem 7.8] □

Theorem 2.8. *Let $\mathcal{C}$ be an $[n,k]_q$ linear code defined by a generator matrix G or a parity check matrix H. Let G' is another generator matrix of $\mathcal{C}$, and H' be another parity check matrix of $\mathcal{C}$. Then*

$$M[G] = M[G']$$

and

$$M[H] = M[H'].$$

Proof. [12, Theorem 7.11] □

Definition 2.11. Let $\mathcal{C}$ be an $[n,k]_q$ linear code. Then the matroid $M_\mathcal{C}$ associated to the code is

$$M_\mathcal{C} = M[H]$$

where H is a parity check matrix of $\mathcal{C}$.

Remark 2.6. If H_1 and H_2 are two different perity check matrices for $\mathcal{C}$, then H_1 and H_2 are two different generator matrices for $\mathcal{C}^\perp$ hence $M[H_1] = M[H_2]$.

Theorem 2.9. *Let $\mathcal{C}$ be an $[n,k]_q$ linear code. Then $M_\mathcal{C}$ a matroid on the ground set E with rank $(n-k)$. Moreover, we have*

$$M_\mathcal{C}^* = M_{\mathcal{C}^\perp}.$$

Proof. Since a parity check matrix of the linear code $\mathcal{C}$, H is $(n-k) \times n$ with rank $(n-k)$ this will be the rank of the matroid $M_\mathcal{C}$. Furthermore if the generator matrix G of the linear code $\mathcal{C}$ is of standard form, then H is of standard form, and we have

$$M_\mathcal{C} = M[H] = M[G]^* = (M_{\mathcal{C}^\perp})^*$$

so that by taking duals

$$M_{\mathcal{C}^*} = M_{\mathcal{C}^\perp}$$

Now, a finer analysis of how to get a generator matrix under standard form by rows and columns operations, and the corresponding operations one needs to perform on parity check matrices show that this is also true (even if the code has no generator matrix of standard form). □

2.7 Minimum distance and weight hierarchy of matroids

We know that for a $[n,k]_q$ linear code $\mathcal{C}$ the generalized Hamming weights are $d_i = min\{\#supp(\mathcal{D}) \mid \mathcal{D}$ is a subcode of dimension i of $\mathcal{C}\}$. In this section we will define the Hamming weights of matroids in connection with the generalized Hamming weights of linear codes and in addition weight hierarchy of the matroids too.

Lemma 2.4. *Let M be a matroid with rank function r. Let $s \in \mathbb{N}$. Then we have,*

$$min\{\#X \mid \#X - r(X) = s\} = min\{\#X \mid \#X - r(X) \geq s\}$$

Proof. [12, Lemma 7.13] □

Theorem 2.10. *Let $\mathcal{C}$ be a $[n,k]_q$ linear code and $M_{\mathcal{C}}$ be a matroid with rank function r. Let $1 \leqslant s \leqslant k$. Then we have*

$$d_s = min\{\#X \mid \#X - r(X) = s\}.$$

Proof. [12, Theorem 7.14] □

Remark 2.7. This theorem gives the possible definition of Hamming weights of a matroid.

Definition 2.12. Let M be a matroid on a ground set E with rank function r. Let $1 \leqslant i \leqslant \#E - r(E)$. Then the i-th generalized Hamming weight of M is

$$d_i = min\{\#X \mid \#X - r(X) = i\}.$$

Proposition 2.10. *Let M be a matroid of rank r on the ground set E. Then we have*

$$d_1 < \ldots < d_{\#E-r}.$$

Proof. [12, Proposition 23] □

Theorem 2.11 (Wei's duality)**.** *Let M be a matroid on E of rank r and $n = \#E$. Let*

$$d_1 < \ldots < d_{n-r}$$

the weight hierarchy of M.
Let $e_1 < \ldots < e_r$. be the weight hierarchy of M^*. Then

$$\{d_1, \ldots, d_{n-r}\} \cup \{n + 1 - e_1, \ldots, n + 1 - e_r\} = \{1, \ldots, n\}$$

and the union is disjoint.

Proof. The proof of this theorem can be found in [5]. □

Definition 2.13. Let M be a matroid on E of rank function r. Then the minimum distance of the matroid M

$$d = d_1(M) = Min\{\#X, X \subset E, \#X - r(X) = 1\}.$$

Remark 2.8. Note that $d_1(M[H])$ is equal to the minimum distance of a $[n, k]$ linear code $\mathcal{C}$ whose parity check matrix is H.

Proposition 2.11. *Let $\mathcal{C}$ be a $[n, k]$ code with weight hierarchy*

$$d_1(\mathcal{C}), ..., d_k(\mathcal{C}).$$

Let $M_\mathcal{C}$ be a matroid associated to the code $\mathcal{C}$ with its weight hierarchy

$$d_1(M_\mathcal{C}), ..., d_k(M_\mathcal{C}).$$

Then

$$d_1(\mathcal{C}) = d_1(M_\mathcal{C}), ..., d_k(\mathcal{C}) = d_k(M_\mathcal{C}).$$

Remark 2.9. Proposition 2.11 is just another formulation of Theorem 2.10 and Definition 2.2.

We study one example to elaborate Proposition 2.11. In fact we want to show that the minimum distance of a linear code is same as of the matroid associated to this code.

Example 2.7.1. Let $\mathcal{C}$ be an $[4,2]_2$ code whose generator matrix is

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

and its parity check matrix is

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

A set of bases for the matroid asssociated to this code is $\mathcal{B} = \{\{1,2\},\{1,3\},\{2,4\},\{3,4\}\}$ Then the Hamming weights yields are:

$$d = d_1 = min\{wt(0110, 1001, 1111)\} = 2$$

and by definition of generalized Hamming weights we get the following

$$d_2 = min\{|supp(\mathcal{D})| \mid \mathcal{D} \text{ is a subcode of dimension 2 of } \mathcal{C}\} = 4$$

Let M be a matroid on ground set $E = \{1,2,3,4\}$, whose set of basis is:

$$\mathcal{B} = \{\{1,2\},\{1,3\},\{2,4\},\{3,4\}\}$$

By Definition 2.12 it is clear that $|X| - r(X) = 0$
for $X = \emptyset, \{1\}, \{2\}, \{3\}, \{4\}, \{1,2\}, \{1,3\}, \{3,4\}, \{2,4\}$

Now for $X = \{2,3\}, \{1,4\}\{1,2,3\}, \{1,2,4\}, \{2,3,4\}, \{1,3,4\}$

$$|X| - r(X) = 1$$

and for $X = \{1,2,3,4\}$

$$|X| - r(X) = 2$$

So, $d_i = min\{|X| \mid |X| - r(X) = i\}$ gives

$$d_1 = min\{|X| \mid |X| - r(X) = 1\} = 2$$

and

$$d_2 = min\{|X| \mid |X| - r(X) = 2\} = 4$$

Hence we see that $d_i(\mathcal{C}) = d_i(M(\mathcal{C}))$, for both $i = 1$ and $i = 2$. So we conclude that the conclusion of Proposition 2.11 holds in this example.

Chapter 3

Stanley-Reisner ring and Betti numbers

3.1 Simplicial complexes

Let E be a finite set, for simplicity we may take $E = \{1, 2, ..., n\}$.

Definition 3.1. A simplicial complex on E is a $\Delta \subset 2^E$ such that

(1) $\emptyset \in \Delta$

(2) If $\sigma_1 \in \Delta$ and $\sigma_2 \subset \sigma_1$, then $\sigma_2 \in \Delta$.

Definition 3.2. A face of Δ is $\sigma \in \Delta$.
A facet of Δ is a maximal face (for inclusion).
$\mathcal{N}(\Delta)$ is the set of minimal non-faces (for inclusion).

Remark 3.1. A simplicial complex is entirely given by its set of facets.

Definition 3.3. Let $S = \mathbb{K}[x_1, \ldots, x_n]$ be the polynomial ring in n variables.
A monomial is a polynomial of the form $\underline{x}^{\underline{a}} = \prod_{i=1}^{n} x_i^{a_i}; a_i \geq 0$.

Definition 3.4. A monomial ideal is an ideal generated by monomials in the ring $S = \mathbb{K}[x_1, ..., x_n]$ over some field $\mathbb{K}$.

Example 3.1.1. $I = (x_1^2, x_2^3, x_3)$ is a monomial ideal.

Definition 3.5. If $u = \prod_{i=1}^{n} x_i^{a_i}$ and each a_i is either $i = 0$ or $i = 1$ then u is called a squarefree monomial.

Definition 3.6. An ideal generated by squarefree monomials is called a squarefree monomial ideal.

3.2 Stanley-Reisner ideals and facet ideals

Let $S = \mathbb{K}[x_1, ..., x_n]$ be the polynomial ring in n variables over a field $\mathbb{K}$ and Δ be a simplicial complex on $E = \{1, ..., n\}$. If $\sigma \subset E$ and $S = \mathbb{K}[x_e, e \in E]$ we set $x^\sigma = \prod_{e \in \sigma} x_e$.

Example 3.2.1. Let $E = \{1, 2, 3, 4\}$ and $\sigma = \{1, 3\} \subset E$ and $S = \mathbb{K}[x_1, x_3, x_4]$. Then $x^\sigma = x_1 x_3$.

Definition 3.7. The Stanley-Reisner ideal of a simplicial complex is given by $I_\Delta = (x^\sigma, \sigma \in \mathcal{N}(\Delta))$. This is a square free monomial ideal.

Definition 3.8. The Stanley-Reisner ring of a simplicial complex Δ is $R_\Delta = S/I_\Delta$, where $S = \mathbb{K}[x_e, e \in E]$.

Proposition 3.1. *The set of all monomials* $x_1^{a_1}, ..., x_n^{a_n}$ *of the polynomial ring* $S = \mathbb{K}[x_1, ..., x_n]$ *in* n *variables with* $\{i \in E \mid a_i \neq 0\} \in \Delta$ *is a* $\mathbb{K}$ *basis of* S/I_Δ.

Proof. [3, Proposition 1.5.1] □

Proposition 3.2. *Let* M *be a matroid and* $\mathcal{I}$ *be a collection of independent subsets of* E. *Then* $\mathcal{I} \subset 2^E$ *is a simplicial complex.*

Proof. Let M be a matroid on a finite set E with $\mathcal{I} \subset 2^E$. Then it satisfies the properties $(I1)$, $(I2)$, $(I3)$. From this we can get the following:

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

$(I2)$ If $I_1 \in \mathcal{I}$ and $I_2 \subset I_1$, then $I_2 \in \mathcal{I}$

This gives that set of independent sets $\mathcal{I}$ form a simplicial complex. □

Proposition 3.3. *The Stanley-Reisner ring of a matroid* M *will be the Stanley-Reisner ring of the simplicial complex* $\Delta = \mathcal{I}$.

Remark 3.2. In this case $\mathcal{N}(\Delta) = \mathcal{N}(\mathcal{I})$ =The set of minimal dependent set=The set of circuits. Hence $\mathcal{I}_\Delta = \{x^\sigma \mid \sigma \text{ a circuit of matroid}\}$.

3.3 Grading

Definition 3.9. A ring R is called a G-graded ring if there exists a family of modules $\{R_g : g \in G\}$, where $(G, +)$ is an abelian group such that

$$R = \bigoplus_{g \in G} R_g$$

with $R_g R_h \subseteq R_{g+h} \forall g, h \in G$.

Definition 3.10. An $R-module$ M is called a graded $G-module$ if there exists a family of $\mathbb{Z}-modules$ $\{M_g : g \in G\}$, where $(G, +)$ is an abelian group, such that

$$M = \bigoplus_{g \in G} M_g$$

with $R_g M_h \subseteq M_{g+h}$ for all $g, h \in G$.

An element $x \in M - \{0\}$ is called a homogeneous element of degree i if $x \in M_i$ for some $i \in G$, the M_i is called a homogeneous component of M.

If G equals $\mathbb{Z}$ or $\mathbb{Z}^n$, we say that R is a graded or $\mathbb{Z}^n - graded$ ring and M is a graded or a $\mathbb{Z}^n - graded$ $R - module$.

For a $\mathbb{Z}^n - graded$ module M we set:

$$M_i = \bigoplus_{x \in \mathbb{Z}^n, |x| = i} M_x.$$

This gives to M a natural structure of graded module.

An R-module M is $\mathbb{Z}^n$-graded if

$$M = \bigoplus_{\underline{a} \in \mathbb{Z}^n} M_{\underline{a}}$$

and $R_{\underline{b}} M_{\underline{a}} \subseteq M_{\underline{b}+\underline{a}}$, for all $\underline{b}, \underline{a} \in \mathbb{Z}^n$ Whereas R has $\mathbb{Z}^n$ grading as:

$$R = \bigoplus_{\underline{b} \in \mathbb{Z}^n} R_{\underline{b}}$$

where

$$R_{\underline{b}} = \begin{cases} 0 & if \;\; \underline{b} \notin \mathbb{Z}^n \\ R[x_1, \cdots, x_n] x^{\underline{b}} & if \;\; \underline{b} \in \mathbb{Z}^n \end{cases}$$

Example 3.3.1. (1) Let $S = K[x_1, \dots, x_n]$ be the polynomial ring in $n-$ $variables$. S has a graded structure induced by $deg(x_i) = 1$.

(2) $S = K[x_1, \dots, x_n]$ has also a $\mathbb{Z}^n - graded$ structure by setting $deg(x_i) = \epsilon_i$, where ϵ_i denotes the ith-unit vector of $\mathbb{Z}^n$

The polynomial rings of (1) and (2) are called graded and $\mathbb{Z}^n$-graded polynomial rings respectively.

3.4 Graded resolutions

Definition 3.11. Let M, N, P be $R - modules$ and $f : M \longrightarrow N$ be a homomorphism of $R - modules$. Then one calls M the domain of f, N the range of f,

$$Imf = f(M) = \{f(m) \mid m \in M\}$$

the image of f and

$$Kerf = f^{-1}(0) = \{m \in M \mid f(m) = 0\}$$

the kernel of f. Now consider a pair (f, g) of homomorphisms so that the range of f is the same as the domain of g. We may illustrate this situation by the diagram

$$M \xrightarrow{f} N \xrightarrow{g} P$$

Such a pair is called exact if $Imf = Kerg$. More generally, a sequence of homomorphisms

$$\cdots \longrightarrow M_n \xrightarrow{f_n} M_{n+1} \xrightarrow{f_{n+1}} \cdots$$

is called exact if each adjacent pair is exact, that is if $Imf_n = Kerf_{n+1}$ for all admissible n.

Definition 3.12. An exact sequence

$$0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} P \longrightarrow 0$$

is called a short exact sequence.

Definition 3.13. Let M be an $R - module$. A free resolution of M is a complex

$$\cdots \longrightarrow F_{i+1} \xrightarrow{d_{i+1}} F_i \xrightarrow{d_i} F_{i-1} \longrightarrow \cdots \longrightarrow F_1 \xrightarrow{d_1} F_0 \longrightarrow 0$$

where the F_i are free modules over R and where

$$\cdots \longrightarrow F_{i+1} \xrightarrow{d_{i+1}} F_i \xrightarrow{d_i} F_{i-1} \longrightarrow \cdots \longrightarrow F_1 \xrightarrow{d_1} F_0 \longrightarrow M \longrightarrow 0$$

is exact.

Remark 3.3. From now on we will study the case $R = S = \mathbb{K}[x_1, \ldots, x_n]$ for a field $\mathbb{K}$.

Definition 3.14. A long exact sequence

$$\mathcal{F} : \cdots \longrightarrow F_2 \longrightarrow F_1 \longrightarrow F_0 \longrightarrow M \longrightarrow 0$$

of $\mathbb{Z} - graded\ S - modules$ with all homogeneous maps $S - module$ morphisms of degree 0, is called a $\mathbb{Z}$-graded free $S - resolution$ of M.

Definition 3.15. Let M be a finitely generated $\mathbb{Z}$-graded $R - module$. A $\mathbb{Z} - graded$ free R-resolution $\mathcal{F}$ of M is called minimal if for all i, the image of $F_{i+1} \longrightarrow F_i$ is contained in $\mathfrak{m}F_i$, where $\mathfrak{m} =< x_1, \ldots, x_n >$.

Definition 3.16. A $\mathbb{Z}$- graded S-module, $S(-j)$ is defined as

$$S(-j)_d = S_{d-j}$$

for $d \in \mathbb{Z}$. This is called a shift of S by d.

Proposition 3.4. *Let M be a finitely generated $\mathbb{Z}$-graded S-module and*

$$\mathcal{F} : \cdots \longrightarrow F_2 \longrightarrow F_1 \longrightarrow F_0 \longrightarrow M \longrightarrow 0$$

a minimal graded free S-resolution of M with $F_i = \bigoplus_j S(-j)^{\beta_{ij}}$ for all i. Then as a $\mathbb{Z}$-graded module $S(-\underline{a}) \simeq S(-|\sigma|)$, and we have $\beta_{i,j} = \sum_{|\sigma|=j} \beta_{i,\sigma}$

Definition 3.17. The numbers $\beta_{i,j}$ are called the graded Betti numbers of the S-module M over the field $\mathbb{K}$.

Remark 3.4. Two different minimal graded free S-resolutions of M give the same Betti numbers.

Definition 3.18. Since $S(-j) \simeq S$ for all j as an $S - module$, we may view F_i as

$$\bigoplus_j S^{\beta_{ij}} \simeq S^{\sum_j} \beta_{ij}.$$

As a sequence of $S - modules$ the minimal free resolution then becomes

$$\mathcal{F} : \cdots \longrightarrow S^{\beta_2} \longrightarrow S^{\beta_1} \longrightarrow S^{\beta_0} \longrightarrow M \longrightarrow 0$$

Then we have:

$$\beta_i = \sum_j \beta_{ij}.$$

The β_i are called the ungraded Betti numbers over the field $\mathbb{K}$. These numbers are also the same for all minimal free resolutions.

Definition 3.19. A long exact sequence

$$0 \longrightarrow F_l \longrightarrow \cdots \longrightarrow F_1 \longrightarrow F_0 \longrightarrow M \longrightarrow 0,$$

of $\mathbb{Z}^n$-graded modules with

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

is called a $\mathbb{Z}^n$-graded free S-resolution of M. Again this resolution is minimal if the image is contained in $\mathfrak{m}F_i$ at each step.

Definition 3.20. The $\beta_{i,\underline{a}}$ are called the $\mathbb{Z}^n$-graded Betti numbers of the matroid M over a field $\mathbb{K}$.

We will be especially interested in the case where M is the Stanley-Reisner ring S/I_Δ, where Δ is a simplicial complex.

In that case the ideal I_Δ will be generated by square free monomials, and then all $\underline{a}$ appearing in the resolution in Definition 3.20 will have entries 0 or 1, e.g $(0, 1, 1, 0, 0, 1, 0)$. In that case we also write $\beta_{i,\sigma}$ for $\beta_{i,\underline{a}}$, where σ is the set of indices i, with $\underline{a} = 1$. In the example $\sigma = \{2, 3, 6\}$.

Remark 3.5. A $\mathbb{Z}$-graded module $S(-\underline{a}) \simeq S(-|\sigma|)$, and we have $\beta_{i,j} = \sum_{|\sigma|=j} \beta_{i,\sigma}$.

Chapter 4

Demi-matroids

4.1 Fundamentals of demi-matroids

In the following section, we have used sources from the literature by various authors. We have adopted basic definitions and theorems from [6], for duality of demi-matroids and for important theorems to give a brief platform for treating them, we have studied mainly [1] and [2]. In Section 4.2 we also present material from [9]

Definition 4.1. A demi-matroid is a triple (E, s, t) consisting of a finite set E and two functions

$$s, t : 2^E \longrightarrow \mathbb{N}_0$$

satisfying the following conditions for all subsets $X \subseteq Y \subseteq E$

(R) $0 \leqslant s(X) \leqslant s(Y) \leqslant |Y|$, and $0 \leqslant t(X) \leqslant t(Y) \leqslant |Y|$.

(D) $|E - X| - s(E - X) = t(E) - t(X)$.

Proposition 4.1. *If $M = (E, r)$ is a matroid with rank r, then, the triple (E, r, r^*) is a demi-matroid, where r^* is the corank of M.*

Proof. By the definition of rank function r and its dual r^*, (R) is satisfied trivially by equating r and r^* with s and t respectively. We prove (D), i.e. if $s = r$ and $t = r^*$, then $|E - X| - s(E - X) = t(E) - t(X)\ \ \forall X \subseteq E$: This is same as

$$t(X) = t(E) - |E - X| + s(E) \tag{4.1}$$

By definition of r^*

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

Equating s and t for r and r^*

$$t(X) = |X| - s(M) + s(E - X) \tag{4.2}$$

Hence it is enough to show that (4.1) and (4.2) are the same identity. This is true if

$$t(E) - |E - X| = |X| - s(E)$$

this is true if and only if,

$$t(E) = |X| + |E - X| - s(E) = |E| - s(E).$$

This holds by setting $X = \emptyset$, in (D) we get:

$$|E| - s(E) = t(E) - t(\emptyset).$$

By (R) we have $0 \leqslant t(\emptyset) \leqslant |\emptyset|$, so $t(\emptyset) = 0$. Hence $t(E) = |E| - s(E)$ as desired.

□

Proposition 4.2. *Note that $s(\emptyset) = t(\emptyset) = 0$ by (R). It follows that (D) is equivalent to the following condition:*

(D') $|E - X| - t(E - X) = s(E) - s(X)$

Proof. Setting $X = \emptyset$ in (D) gives

$$|E| - s(E) = t(E)$$

or equivalently

$$|E| = t(E) + s(E)$$

Now put $X = E - X$ in (D) gives

$$|X| - s(X) = t(E) - t(E - X).$$

Adding $|E - X| + s(E)$ to the both sides gives us

$$|E - X| - t(E - X) = s(E) - s(X).$$

So (D) implies (D'). The converse is proven the same way. □

Remark 4.1. By the previous remark we can see that the axioms (R) and (D) imply that t is completely determined by s, in the same way as r^* is determined by r in a matroid.

Hence we could have written s^* instead of t. This is true since axiom (D) implies, for $X = \emptyset$

$$t(E) = |E| - s(E).$$

Thereby (D) gives

$$t(X) = t(E) - |E - X| + s(E - X) = |E| - s(E) - |E - X| + s(E - X)$$
$$t(X) = |X| - s(E) + s(E - X).$$

Which shows that t is entirely defined by s. This expression may be called s^*.

Proposition 4.3. $(s^*)^* = s$

Proof. The proof that $(s^*)^* = s$ is same as for matroids.
$s^*(X) = |X| - s(E) + s(E - X)$

$$\begin{aligned} (s^*)^*(X) &= |X| - s^*(E) + s^*(E - X) \\ &= |X| - (|E| - s(E)) + (|E - X| - s(E) + s(X)) \\ &= |X| - |E| + s(E) + |E - X| - s(E) + s(X) \\ &= s(X) \end{aligned}$$

□

Remark 4.2. Conversely to proposition 4.1, if (E, s, t) is a demi-matroid, then s is the rank function of a matroid M on E if and only if t is the rank function of M^*.

Example 4.1.1. Suppose that $E = \{1, 2\}$ and define $s(\emptyset) = 0, s(\{1\}) = s(\{2\}) = 0$ and $s(\{1, 2\}) = 1$. Consider (E, s, s).

(R) $0 \leqslant s(X) \leqslant s(Y) \leqslant |Y|$. We check easily that this is true for all $X \subseteq Y \subseteq E$

(D) $|E - X| - s(E - X) = s(E) - s(X)$. We check easily that this is true for $X = \emptyset, \{1\}, \{2\}, \{1, 2\}$

But (E, s) is not a matroid, since s does not satisfy $(R3)$

Remark 4.3. For matroids we think of (E, r, r^*) as (E, s, t) where

$$r^*(X) = |X| + r(E - X) - r(E)$$
$$t(X) = |X| + s(E - X) - s(E).$$

4.2 Duality of Demi-matroid

Definition 4.2. For the demi-matroid $D = (E, s, t)$ the dual demi-matroid is given by $D^* = (E, t, s)$ with $D = (D^*)^*$.

The dual demi-matroid $D = (E, r, r^*)$ which arises from the matroid $M = (E, r)$ is $D^* = (E, r^*, r)$ which corresponds to the dual matroid $M^* = (E, r^*)$.

Another type of duality operator is:

$$\overline{M} = (E, \overline{s}, \overline{t})$$

where

$$\overline{s} = s(E) - s(E - X),$$

$$\overline{t} = t(E) - t(E - X).$$

This type of duality arises from the following involution:

Definition 4.3. For any real function $f : 2^E \longrightarrow \mathbb{R}$, let $\overline{f}$ denote the function given by

$$\overline{f}(X) = f(E) - f(E - X).$$

Remark 4.4. Since $\overline{\overline{f}}(X) = \overline{f}(E) - \overline{f}(E - X)$ where

$$\overline{f}(E) = f(E) - f(E - E) = f(E) - f(\emptyset)$$

and

$$\overline{f}(E - X) = f(E) - f(E - E + X) = f(E) - f(X).$$

Which gives us:

$$\overline{\overline{f}}(X) = f(X) - f(\emptyset)$$

It follows that if $f(\emptyset) = 0$, then the operation $f \longrightarrow \overline{f}$ is an involution, i.e. $f = \overline{\overline{f}}$

Theorem 4.1. *The triple $\overline{D} = (E, \overline{s}, \overline{t})$ is a demi-matroid called the supplement of D, furthermore, $D = \overline{\overline{D}}$ and $\overline{D^*} = (\overline{D})^*$.*

Proof. To show that $\overline{D}$ is a demi-matroid, we note that $\overline{s}(\emptyset) = \overline{t}(\emptyset) = 0$ and $\overline{s}(E) = s(E)$ and $\overline{t}(E) = t(E)$. Consider the subsets $X \subseteq Y \subseteq E$. Then by (R) and (D'),

$$\begin{aligned} E - Y &\subseteq E - X \\ s(E-Y) &\leqslant s(E-X) \\ -s(E-Y) &\geqslant -s(E-X) \\ s(E) - s(E-Y) &\geqslant s(E) - s(E-X) \\ s(E) - s(E-X) &\leqslant s(E) - s(E-Y) \end{aligned}$$

but from (D') we have

$$|E - X| - t(E - X) = s(E) - s(X)$$

$$|X| - t(X) = s(E) - s(E - X)$$

This implies,

$$|Y| - t(Y) = s(E) - s(E - Y)$$

which gives

$$0 \leqslant s(E) - s(E - X) \leqslant s(E) - s(E - Y) = |Y| - t(Y) \leqslant |Y|,$$

So

$$0 \leqslant \overline{s}(X) \leqslant \overline{s}(Y) \leqslant |Y|.$$

Similarly, we can show that

$$0 \leqslant \overline{t}(X) \leqslant \overline{t}(Y) \leqslant |Y|,$$

so $\overline{D}$ satisfies (R). By (D'),

$$\begin{aligned} |E - X| - t(E - X) &= s(E) - s(X) \\ |E - X| - (s(E) - s(X)) &= t(E - X) \\ |E - X| - \overline{s}(E - X) &= t(E) - \overline{t}(X) \\ |E - X| - \overline{s}(E - X) &= \overline{t}(E) - \overline{t}(X), \end{aligned}$$

so $\overline{D}$ satisfies (D). Hence $\overline{D}$ is a demi-matroid.

Since we have seen that $f = \overline{\overline{f}}$, if $f(\emptyset) = 0$, $s = \overline{\overline{s}}$ and $t = \overline{\overline{t}}$. Hence we have $D = (E, s, t) = (E, \overline{\overline{s}}, \overline{\overline{t}}) = \overline{\overline{D}}$. Note that

$$\overline{D^*} = \overline{(E, t, s)} = (E, \overline{t}, \overline{s}) = (E, \overline{s}, \overline{t})^* = (\overline{D})^*.$$

$\square$

Example 4.2.1. Let $M = (E, r)$ be the matroid, where $E = \{1, 2, 3\}$ for $X = \emptyset, \{1\}$ $r(X) = 0$ and $r(X) = 1$ for all other subsets $X \subseteq E$. Then $D = (E, r, \overline{r})$ is a demi-matroid, so $\overline{D} = (E, \overline{r}, \overline{r}^*)$ is also a demi-matroid. Let us compute $\overline{r}$ by the formula:

$$\overline{r}(X) = r(E) - r(E - X)$$

$$\overline{r}(\emptyset) = r(E) - r(E - \emptyset) = 1 - 1 = 0$$

$$\overline{r}(\{1\}) = r(E) - r(E - \{1\}) = 1 - 1 = 0$$

$$\overline{r}(\{2\}) = r(E) - r(E - \{2\}) = 1 - 1 = 0$$

$$\overline{r}(\{3\}) = r(E) - r(E - \{3\}) = 1 - 1 = 0$$

$$\overline{r}(\{2, 3\}) = r(E) - r(E - \{2, 3\}) = 1 - 0 = 1$$

$$\overline{r}(\{1, 3\}) = r(E) - r(E - \{1, 3\}) = 1 - 1 = 0$$

$$\overline{r}(\{1, 2\}) = r(E) - r(E - \{1, 2\}) = 1 - 1 = 0$$

$$\overline{r}(\{1, 2, 3\}) = r(E) - r(E - \{1, 2, 3\}) = 1 - 0 = 1$$

Thus, $(E, \overline{r})$ is not a matroid, since it would have rank 1 but contains only loops which is not possible. So $(D, \overline{r}, \overline{r}^*))$ is a demi-matroid, but not a matroid.

Lemma 4.1. *Let E be a finite set with rank function r satisfying the subcardinal property: $r(X) \leqslant r(Y)$ whenever $X \subseteq Y$. Then the following two properties are equivalent:*

(R1) $r(X) \leqslant r(X \cup p) \leqslant r(X) + 1$ *(unit rank increase)*

(MN) If $X \subseteq Y$, then $|X| - r(X) \leqslant |Y| - r(Y)$ (monotone nullity)

Proof. Assume if $X \subseteq Y$, then

$$|X| - r(X) \leqslant |Y| - r(Y)$$

$(R1)$ is obvious if $p \in X$. Suppose $p \notin X$, then $r(X) \leqslant r(X \cup p)$ by our assumption in Lemma.

Now put $Y = X \cup p$, then

$$|X| - r(X) \leqslant |X| + 1 - r(X \cup p)$$

This gives

$$r(X \cup p) \leqslant r(X) + 1$$

Assume $r(X) \leqslant r(X \cup p) \leqslant r(X) + 1$, and let $Y = X \cup \{p_1, \ldots, p_n\}$ so $|Y| = |X| + n$. But $r(Y) - r(X) \leqslant n$, since it increases by at most 1 each time we add a new point, using last part of $(R1)$. Hence $|X| - r(X) \leqslant |Y| - r(Y)$. □

Remark 4.5. Note that monotone nullity can also be expressed in other ways. For instance, it is immediate that this property is equivalent to $X \subseteq Y$ implies $r(Y) - r(X) \leqslant |Y - X|$.

Theorem 4.2. *Let E be a finite set with rank function $r : 2^E \longrightarrow \mathbb{Z}$. Then the triple (E, r, r^*) is a demi-matroid if and only if r satisfies the following conditions, for all $p \in E$ and $X, Y \subseteq E$:*

- *(a)* $0 \leqslant r(X) \leqslant |X|$ *(non-negative subcardinal)*
- *(b) if $X \subset Y$, then $r(X) \leqslant r(Y)$ (monotone rank)*
- *(c)* $r(X \cup p) \leqslant r(X) + 1$ *(unit rank increase)*

Proof. Suppose r satisfies the three conditions $(a), (b), (c)$. We show the triple (E, r, r^*) is a demi-matroid where:

$$r^*(X) = |X| + r(E - X) - r(E)$$

because of (a)

$$r^*(E) = |E| - r(E)$$

By subtracting these two equations we get

$$r^*(E) - r^*(X) = |E| - r(E) - |X| - r(E - X) + r(E)$$

$$r^*(E) - r^*(X) = |E| - |X| - r(E - X)$$
$$r^*(E) - r^*(X) = |E - X| - r(E - X)$$

This immediately implies that (D) holds in Definition 4.1 for any $X \subseteq E$. Thus, to show that triple (E, r, r^*) is a demi-matroid, we must show the dual rank r^* also satisfies (R) in Definition 4.1 for all subsets $X \subseteq Y \subseteq E$:

(1) $0 \leqslant r^*(X) \leqslant |X|$, and

(2) if $X \subseteq Y$, then $r^*(X) \leqslant r^*(Y)$.

First we show $0 \leqslant r^*(X)$ for all X. Since $r^*(X) = |X| + r(E-X) - r(E)$ $0 \leqslant r^*(X)$ if and only if $0 \leqslant |X| + r(E-X) - r(E)$, i.e if and only if

$$r(E) \leqslant |X| + r(E-X)$$

Monotone nullity follows from (b) and (c).

To show $r^*(X) \leqslant |X|$, we note that this is equivalent to $|X| + r(E-X) - r(E) \leqslant |X|$, i.e $r(E-X) \leqslant r(E)$. This now follows directly from condition (b).

It remains to show that if $X \subseteq Y$, then $r^*(X) \leqslant r^*(Y)$. Now

$$\begin{aligned} r^*(X) \leqslant r^*(Y) &\Leftrightarrow |X| + r(E-X) - r(E) \leqslant |Y| + r(E-Y) - r(E) \\ &\Leftrightarrow r(E-X) - r(E-Y) \leqslant -|X| + |Y| \\ &\Leftrightarrow r(E-X) - r(E-Y) \leqslant |E-X| - |E-Y| \\ &\Leftrightarrow |Y'| - r(Y') \leqslant |X'| - r(X'). \end{aligned}$$

where $X' = E - X$ and $Y' = E - Y$, with $Y' \subseteq X'$. This follows from monotone nullity (Lemma 4.1).

For the converse, we first observe that if (E, r, s) is a demi-matroid, then (D) in Definition 4.1 requires $s = r^*$, where $r^*(X) = |X| + r(E-X) - r(E)$. Then r must satisfy conditions (a) and (b) this follows from Definition 4.1. It remains to show r also satisfies the monotone nullity property (MN)(Lemma 4.1). Assume $X \subseteq Y$. Then the argument given above shows that r satisfies (MN) if and only if r^* satisfies Definition 4.1(R):

$$|X| - r(X) \leqslant |Y| - r(Y) \Leftrightarrow r^*(E-Y) \leqslant r^*(E-X).$$

Since $E - Y \subseteq E - X$ and (E, r, r^*) is a demi-matroid, we know $r^*(E-Y) \leqslant r^*(E-X)$. This completes the proof.

□

4.3 Flags of linear codes

Definition 4.4. A flag over a finite field $\mathbb{F}_q$ is a sequence X of strictly embedded subspaces $V_{i_1} \subset V_{i_2} \subset \ldots V_{i_s}$ of dimension $i_1, i_2, \ldots, i_s$ of an n-dimensional vector space. A flag variety of type $(i_1, i_2, \ldots, i_s)$ is the variety of all flags $X = \{V_{i_1}, V_{i_2}, \ldots, V_{i_s}\}$ with $(i_1, i_2, \ldots, i_s)$ given.

Consider a flag $F := (\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_m)$ of linear codes with $\mathcal{C}_m \subset \ldots \subset \mathcal{C}_2 \subset \mathcal{C}_1 \subset \mathbb{F}^n$ and coordinates $E = \{1, 2, \ldots, n\}$, where $\mathbb{F}_q$ is a field. For each code $\mathcal{C} \subset \mathbb{F}_q^n$ with coordinates E, and for each subset $X \subset E$, the restricted code $\mathcal{C}|X$ is the subcode of ${\mathbb{F}_q}^{|X|}$ obtained by deleting the coordinates $E - X$ from all codewords of $\mathcal{C}$. We define the Euler rank s_F by

$$s_F(X) = \sum_{i=1}^{m} (-1)^{(i-1)} r_i(X)$$

for all subsets $X \subseteq E$, where $r_i(X) = dim(\mathcal{C}_i|X)$ is the rank function of the vector matroid $M_{\mathcal{C}_i}$. We also define the function t_F by $t_F(X) = |X| + s_F(E - X) - s_F(E)$ for each $X \subseteq E$.

Theorem 4.3. *The triple $D_F = (E, s_F, t_F)$ is a demi-matroid.*

Remark 4.6. If $m = 1$, then s_1 is the matroid rank function associated with the code C_1. Theorem 4.3 thus extends the vector matroid concept to flags of any finite length.

Proof. For the triple $D_F = (E, s_F, t_F)$ to be a demi-matroid we check if it satisfies (R) and (D) in Definition 4.1. By the definition of t_F we get (D) as

$$t_F(E) - t_F(X) = |E| + s_F(\emptyset) - s_F(E) - |X| - s_F(E - X) + s_F(E)$$

$$t_F(E) - t_F(X) = |E - X| - s_F(E - X)$$

We will now verify that axiom (R) is also satisfied, so let $X \subseteq Y \subseteq E$. If m is even, then

$$s_F(X) = r_1(X) - r_2(X) + r_3(X) - r_4(X) + \cdots + r_{m-1}(X) - r_m(X)$$

Since $r_{2i-1}(X) \geq r_{2i}(X)$ for each i, we see that $s_F(X) \geq 0$. The odd m case is treated similarly. Next, note that $s_{F_-}(Y) \geq 0$ by the previous statement applied to the flag $F_- = (C_2, \ldots, C_m)$ and the set Y. Then

$$s_F(Y) = r_1(Y) - s_{F_-}(Y) \leqslant |Y| - 0 = |Y|.$$

Now we will show that $s_F(X) \leqslant s_F(Y)$. Suppose that m is even; then

$$s_F(Y) - s_F(X) = \sum_{i=1}^{m/2} [(r_{2i-1}(Y) - r_{2i}(Y)) - (r_{2i-1}(Y) - r_{2i}(Y))].$$

Let

$$G' = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$$

be a generator matrix for the restricted code $C_1|Y$ so that $\begin{bmatrix} A & B \end{bmatrix}$ is a generator matrix for $C_2|Y$, and so that the rows of G' are linearly independent. Without loss of generality, we may assume that the columns of A (and C) are indexed by X. Then,

$$r_1(Y) - r_2(Y) = rankG' - rank \begin{bmatrix} A & B \end{bmatrix} = rank \begin{bmatrix} C & D \end{bmatrix}$$

$$\geq rankC \geq rank \begin{bmatrix} A & C \end{bmatrix}^t - rankA = r_1(X) - r_2(X).$$

By the same argument, $r_{2i-1}(Y) - r_{2i}(Y) \geqslant r_{2i-1}(X) - r_{2i}(X)$ for each i, so $s_F(Y) - s_F(X) \geqslant 0$. A slight addition to these arguments proves that $s_F(X) \leqslant s_F(Y)$ also when m is odd. We conclude that
$0 \leqslant s_F(X) \leqslant s_F(Y) \leqslant |Y|$, so axiom (R) holds for s_F. Let us now check that axiom (R) also holds for t_F:

$$\begin{aligned} t_F(Y) - t_F(X) &= |Y| - |X| + s_F(E-Y) - s_F(E-X) \\ &= |Y| - |X| + r_1(E-Y) - r_1(E-X) - s_{F_-}(E-Y) + s_{F_-}(E-X) \end{aligned}$$

$$t_F(Y) - t_F(X) \geqslant |Y| - |X| + r_1(E-Y) - r_1(E-X)$$

$$t_F(Y) - t_F(X) = r_1^*(Y) - r_1^*(X) \geqslant 0$$

Hence, $t_F(X) \leqslant t_F(Y)$ for all subsets $X \subset Y \subset E$. In particular, $t_F(X) \geqslant t_F(\emptyset) = 0$. Finally,

$$t_F(Y) = |Y| - (s_F(E) - s_F(E-Y)) \leqslant |Y| - 0 = |Y|,$$

so axiom (R) also holds for t_F. This concludes the proof. □

Theorem 4.4. *The demi-matroid $D_F^{\perp}$ associated to the dual flag $F^{\perp} = (C_m^{\perp}, \cdots, C_1^{\perp})$ is given by:*

$$D_F^{\perp} = \begin{cases} \overline{D_F}, & \text{if } m \text{ is even} \\ {D_F}^*, & \text{if } m \text{ is odd.} \end{cases}$$

Proof. By Theorem 4.3, $S_F^{\perp}$ induces the demi-matroid $D_F^{\perp} = (E, s_F^{\perp}, t_F^{\perp})$. Since by Remark 4.2 $t_F^{\perp}$ is uniquely determined by $s_F^{\perp}$, so it is enough to show that $s_F^{\perp} = \overline{s_F}$ if m is even and $s_F^{\perp} = t_F$ if m is odd. Suppose that m is even and write $m = 2h$. The Euler rank of $F^{\perp}$ is then given by

$$\begin{aligned} s_F^{\perp}(X) &= \sum_{i=1}^{2h} (-1)^{i-1} r^*_{m+1-i}(X) \\ &= \sum_{j=1}^{h} [-r^*_{m+1-2j}(X) + r^*_{m+2-2j}(X)] \\ &= \sum_{j=1}^{h} [(|X| - r^*_{m+1-2j}(X)) - (|X| - r^*_{m+2-2j}(X))]. \end{aligned}$$

Since we know by definition

$$r^*(X) = |X| + r(E - X) - r(E)$$

This implies

$$|X| - r^*(X) = |X| - |X| + r(E) - r(E - X)$$

Thus we get

$$\begin{aligned} s_F^{\perp}(X) &= \sum_{j=1}^{h} [(r_{m+1-2j}(E) - r_{m+1-2j}(E - X)) - (r_{m+2-2j}(E) - r_{m+2-2j}(E - X)] \\ &= \sum_{j=1}^{h} [r_{m+1-2j}(E) - r_{m+2-2j}(E) - r_{m+1-2j}(E - X) - r_{m+2-2j}(E - X)] \\ &= \sum_{j=1}^{h} r_{m+1-2j}(E) - r_{m+2-2j}(E) - \sum_{j=1}^{h} r_{m+1-2j}(E - X) - r_{m+2-2j}(E - X) \\ &= \sum_{i=1}^{m} (-1)^{i-1} r_i(E) - \sum_{i=1}^{m} (-1)^{i-1} r_i(E - X) \\ &= s_F(E) - s_F(E - X) = \overline{s_F}(X). \end{aligned}$$

for each subset $X \subseteq E$.

Now suppose that m is odd, and define $F^+ = (C_1, \ldots, C_m, C_{m+1})$ where $C_{m+1} = \{0\}$ consists of the zero vector in $\mathbb{F}_q^n$. Then $F^{+\perp} = (R^n, {C_m}^\perp, \ldots, {C_2}^\perp, {C_1}^\perp)$, $r_{m+1}(X) = 0$, and $r^*_{m+1}(X) = |X|$.

Therefore, $s_F^+(X) = s_F(X) - r_{m+1}(X) = s_F(X)$ and

$$s_{F^+}^\perp(X) = r^*_{m+1}(X) - s_F^\perp(X) = |X| - s_F^\perp(X).$$

Since F^+ is a flag on an even number of linear codes, we therefore see that

$$s_F^\perp(X) = |X| - s_{F^+}^\perp(X)$$

$$s_F^\perp(X) = |X| - \overline{s_{F^+}(X)}$$

since $\overline{s_F} = s_F(E) - s_F(E - X)$

$$s_F^\perp(X) = |X| - (s_F(E) - s_F(E - X)) = t_F(X)$$

This completes the proof. □

4.4 Simplicial complexes and demi-matroids

Let E be a set containing n elements, and let $r : 2^E \longrightarrow \mathbb{N}_0$ be a function such that (E, r) is a demi-matroid, that is, a function such that for all $X \subset Y \subset E$ and for all $x \in E$ we have:

$$0 \leqslant r(X) \leqslant r(Y) \leqslant |Y|$$

and

$$r(X \cup x) \leqslant r(X) + 1$$

Proposition 4.4. *The set $\Delta_r = \{Y \subset E : r(Y) = |Y|\}$ is a simplicial complex on E.*

Proof. We prove that if $Y \in \Delta_r$ and $X \subset Y$ then $X \in \Delta_r$, so our goal is to show that $r(X) = |X|$.

Since $X \subset Y$, we can set $Y = X \cup \{y_1, \ldots, y_l\}$ and $l = |Y| - |X|$.

By $r(X \cup x) \leqslant r(X) + 1$, we have

$$r(X \cup \{y_1\}) \leqslant r(X) + 1$$

$$r(X \cup \{y_1, y_2\}) \leqslant r(X) + 2$$

Similarly

$$r(X \cup \{y_1, \ldots, y_l\}) \leqslant r(X) + l$$

So

$$r(Y) \leqslant r(X) + l$$

$$r(Y) - l \leqslant r(X)$$

By definition $r(Y) = |Y|$, thus we get

$$|Y| - l \leqslant r(X)$$

and

$$r(X) \geq |X|$$

Also we have $r(X) \leqslant |X|$ hence $r(X) = |X|$. This proves that $X \in \Delta_r$.

□

Proposition 4.5. *Let Δ be a simplicial complex then (E, r_Δ) is a demi-matroid with $r_\Delta = max\{|F| : F$ is a face and $F \subset X\}$.*

Proof. We use Theorem 4.2 and verify (a),(b) and (c).

(a) $0 \leqslant r_\Delta(X) \leqslant |X|$

Since $\emptyset \subseteq X$, and $\emptyset$ is a face, then:

$$r_\Delta(X) \geq |\emptyset| = 0$$

Since for any $F \subset X$, we have $|F| \leqslant |X|$

$$max|F| \leqslant |X|$$

$$r_\Delta(X) \leqslant |X|$$

Hence $0 \leqslant r_\Delta(X) \leqslant |X|$

(b) If $X \subseteq Y$, then $r_\Delta(X) \leqslant r_\Delta(Y)$. If F is a face of maximal cardinality among those contained in X, then obviously $F \subset Y$ since $X \subset Y$ and $|F| = r_\Delta(X)$.

   Hence $\{|F| \mid F$ is a face of Δ and $F \subset Y\}$ contains F

   Therefore $r_\Delta(X) \leqslant max\{|F| \mid F$ is a face of Δ and $F \subset Y\} = r_\Delta(Y)$.

   Thus $r_\Delta(X) \leqslant r_\Delta(Y)$

(c) $r_\Delta(X \cup x) \leqslant r_\Delta(X) + 1$ Let F be a face of Δ of maximal cardinality, among those contained in $X \cup \{x\}$. Then $r_\Delta(X \cup \{x\}) = |F|$ by definition. Here we look at two cases:

(1) When $F \subset X$, then

$$|F| \leqslant r_\Delta(X) \leqslant r_\Delta(X) + 1$$

$$r_\Delta(X \cup \{x\}) \leqslant r_\Delta(X) + 1$$

Since $r_\Delta(X \cup \{x\}) = |F|$

(2) When F is not a subset of X, we set $F = (F - \{x\}) \cup \{x\}$. Then $F - \{x\}$ is a face of X, since Δ is a simplicial complex. Then

$$|F - \{x\}| \leqslant r_\Delta(X)$$

and

$$|F| = |F - \{x\}| + 1 \leqslant r_\Delta(X) + 1$$

Since $|F| = r_\Delta(X \cup \{x\})$ so we get:

$$r_\Delta(X \cup \{x\}) \leqslant r_\Delta(X) + 1$$

□

Proposition 4.6. $\Delta_{r_\Delta} = \Delta$

Proof. $\Delta_{r_\Delta} = \{X \mid r_\Delta(X) = |X|\}$. Identify those X such that $r_\Delta(X) = |X|$. Such X are precisely those which contains a face F with $|X| = |F|$. But if $F \subset X$, and $|F| = |X|$, then $F = X$ and hence all those X are faces F of Δ.

On the other hand if we know that X is a face of Δ then $r_\Delta(X) = |X|$, since X is itself a maximal face among those contained in X. Hence $r_\Delta(X) = |X|$ if and only if X is a face of Δ. Therefore

$$\{X \mid r(X) = |X|\} = \{\text{ faces of } \Delta\} = \Delta$$

Thus $\Delta_{r_\Delta} = \Delta$ □

Given a demi-matroid (E, r) on the set E. We can of course look at the simplicial complex Δ_r, and we can make a new demi-matroid r_{Δ_r}. The question arise here whether $r_{\Delta_r} = r$. Answer in general is no.

Example 4.4.1. For example, let $E = \{1, 2\}$, $r\{\emptyset\} = r\{1\} = r\{2\} = 0$ while $r\{1, 2\} = 1$.

$$\Delta_r = \{X \mid r(X) = |X|\} = \{\emptyset\}$$

and

$$r_{\Delta_r}(X) = max\{|F| \mid F \text{ is a face of } \Delta_r \text{ contained in } X\} = 0$$

Remark 4.7. In general $r_{\Delta_r} \neq r$ for a demi-matroid (E, r). But if r is of the form r_Δ, for a simplicial complex, then $r_{\Delta_r} = r$.

Proposition 4.7. $r = r_{\Delta_r}$

Proof. $r = r_\Delta = r_{\Delta_{r_\Delta}} = r_{\Delta_r}$ □

Proposition 4.8. *If Δ is a simplicial complex and (E, r) is a demi-matroid with underlying Δ then, $r_{\Delta_r}(X) \leqslant r(X)$ for all $X \subset E$.*

Proof. By definition $r_{\Delta_r}(X) = max\{|F| \mid F$ is a face of $\Delta_r\}$, where F has the maximal cardinality among those faces of Δ_r contained in X. But $F \subset X$, also F is a face of Δ_r, thus we have

$$|F| = r(F) \leqslant r(X)$$

$$|F| = r_{\Delta_r}(X) \leqslant r(X)$$

This concludes the proof. □

Remark 4.8. (E, r) is a demi-matroid with underlying simplicial complex Δ i.e. $\Delta = \Delta_r$.

Proposition 4.9. *To every simplicial complex Δ, (E, r^Δ) is a demi-matroid with*

$$r^\Delta(X) = \begin{cases} |X| & if \;\; X \in \Delta \\ |X| - 1 & if \;\; X \notin \Delta \end{cases}$$

Proof. We shall show that (E, r^Δ) is a demi-matroid, and for this we show that all three condition of Theorem 4.2 are satisfied. It is immediate that (a) is obvious.

For (b) we shall look at following cases along with if $X \subset Y$ then:

(1) When $X \in \Delta$ and $Y \in \Delta$. Then it is clear that $|X| \leqslant |Y|$, and $r^\Delta(X) \leqslant r^\Delta(Y)$.

(2) When $X \in \Delta$ and $Y \notin \Delta$. In this case Y strictly contains X i.e. $X \subsetneq Y$. Then, $|Y| \geq |X| + 1$ and $|Y| - 1 \geq (|X| + 1) - 1 = |X|$. This gives $r^{\Delta}(X) \leqslant r^{\Delta}(Y)$.

(3) When $X \notin \Delta$ and $Y \in \Delta$. This is not possible that the subset of a face of simplicial complex is not a face.

(4) When $X \notin \Delta$ and $Y \notin \Delta$, then $|X| \leqslant |Y|$ and this is same as:

$$|X| - 1 \leqslant |Y| - 1$$

and this by definition of r^{Δ} gives the desired result $r^{\Delta}(X) \leqslant r^{\Delta}(Y)$

Now we shall show that $r^{\Delta}(X \cup p) \leqslant r^{\Delta}(X) + 1$. To prove (c) we will look at following cases:

(1) If $p \notin X$ then we should look at following two cases:

(1)′ If X and $X \cup p$ are faces we have $r^{\Delta}(X) = |X|$ and $r^{\Delta}(X \cup p) = |X| + 1$, also $r^{\Delta}(X \cup p) - r^{\Delta}(X) = 1$ gives that the difference is at most 1.

(2)′ If $X \in \Delta$ and $X \cup p \notin \Delta$, then $r^{\Delta}(X) = |X|$ and $r^{\Delta}(X \cup p) = |X|$. Then $r^{\Delta}(X \cup p) - r^{\Delta}(X) = 0$.
Thus by combining $(1)', (2)'$, we get our required result i.e.
$r^{\Delta}(X \cup p) \leqslant r^{\Delta}(X) + 1$

(3)′ If $X \notin \Delta$ and $X \cup p \notin \Delta$.
Then $r^{\Delta}(X) = |X| - 1$ and $r^{\Delta}(X \cup p) = |X \cup p| - 1 = |X|$. We see that the difference between $r^{\Delta}(X \cup p) - r^{\Delta}(X) = 1$, which is at most 1. Thus, we get the same result.

(2) If $p \in X$, then $X \cup p = X$. So (c) is obvious.

□

Proposition 4.10. *If Δ is a simplicial complex and (E, r) is a demi-matroid with underlying simplicial complex Δ, then $r(X) \leqslant r^{\Delta}(X)\ \ \forall X \subset E$.*

Proof. Δ is obviously the underlying complex of r^{Δ}, since the faces of Δ are the only sets such that

$$r^{\Delta}(X) = |X|$$

Suppose that if $r(X) > r^{\Delta}(X)$ for $X \in \Delta$, then $r(X) > |X|$ but this is a contradiction with the structure of demi-matroid (E, r). So $r(X) \leqslant r^{\Delta}(X)$.

Now for $X \notin \Delta$, assume that $r(X) > r^{\Delta}(X)$. But then $r(X) = |X|$ and this implies that $X \in \Delta$ which is again a contradiction and we conclude that $r(X) \leqslant r^{\Delta}(X)$. □

Remark 4.9. We also have the sequence

$$\Delta \rightsquigarrow r_{\Delta} \rightsquigarrow \Delta_{r_{\Delta}} \rightsquigarrow r_{\Delta_{r_{\Delta}}} \cdots$$

stable in the sense that the terms number $1, 3, 5, \ldots$ are the same, and of course the terms $2, 4, 6, \ldots$ are the same also.

Moreover in the sequence

$$r \rightsquigarrow \Delta_r \rightsquigarrow r_{\Delta_r} \rightsquigarrow \Delta_{r_{\Delta_r}} \cdots$$

terms number $2, 4, 6, \ldots$ are the same, and terms $3, 5, 7, \ldots$ are the same but term 1 can be different from term 3.

So far we have countered with demi-matroid (E, r), and obtained $\Delta_r = \{F \mid r(F) = |F|\}$. We will now obtain Δ_r in another way.

Let $D = (E, r, r^*)$ be a demi-matroid. As we know $D^* = (E, r^*, r)$ and $\overline{D} = (E, \overline{r}, r)$ are also demi-matroids. Then we have:

Proposition 4.11. *The faces of Δ_r are the zeroes of the demi-matroid function $\overline{r^*} = \overline{r}^*$.*

Proof. We look at some results. Since by definition we have

$$\overline{r^*}(X) = r^*(E) - r^*(E - X)$$

$$\overline{r^*}(X) = |E| - r(E) + r(E - E) - |E - X| + r(E) - r(X)$$

$$\overline{r^*}(X) = |E| - |E - X| - r(X)$$

$$\overline{r^*}(X) = |X| - r(X)$$

Also

$$\overline{r}^*(X) = |X| - \overline{r}(E) + \overline{r}(E - X)$$

$$\overline{r}^*(X) = |X| - r(E) + r(E - E) + r(E) - r(X)$$

$$\overline{r}^*(X) = |X| - r(X)$$

And by definition of nullity function we know $n_r(X) = |X| - r(X)$. We observe: $r(X) = 0 \Leftrightarrow \overline{r}^*(X) = |X| - r(X) = |X|$

$$X \in \Delta_r \Leftrightarrow \overline{r^*}(X) = |X|$$

$$\begin{aligned} |X| - r^*(E) + r^*(E - X) &= |X| \\ r^*(E) - r^*(E - X) &= 0 \\ \overline{r^*}(X) &= 0 \end{aligned}$$

This conclude the proof. □

Remark 4.10. Hence we see that any simplicial complex described as $\{X \subset E \mid r(X) = |X|\}$, for a demi-matroid r and also as $\{X \subset E \mid s(X) = 0\}$, for same demi-matroid r.

On the other hand all the sets $\{X \subset E \mid r(X) = 0\}$ for a demi-matroid is also $\{X$ not a subset of $E \mid r(X) = |X|\}$ for same demi-matroid s. In this case $s = \overline{r^*}$.

Proposition 4.12. *Let $E = \{1, 2, \ldots, n\}$, the following subsets of 2^E are the same:*

(1) Simplicial complexes.

(2) Zero-sets of demi-matroids.

(3) Full rank sets of demi-matroids.

Remark 4.11. The full rank set is defined as $\{X \mid r(X) = |X|\}$.

4.5 Open questions

Let Δ be a simplicial complex consisting of subsets of E. Then r_Δ is the "smallest demi-matroid" among the demi-matroids determining $\Delta(\Delta_{r_\Delta})$ in the sense of Proposition 4.6.

Look at r^*_Δ, is r^*_Δ the "smallest demi-matroid" among those determining $\Delta_{r^*_\Delta}$??

In other words: is $r_\Delta{}^* = r_{\Delta^*_r}$??

Also is $\overline{r}_\Delta = r_{\Delta_{\overline{r}}}$??

Chapter 5

Pair of Matroids

The following chapter has been inspired by [4].

Let M be a matroid on E. We recall

$$\mathcal{C}(M) = \{X \subset E \mid n(X) = 1, \text{ and } n(X - \{x\}) = 0, \forall x \in X\}$$

Definition 5.1. A cycle is a union of circuits

$$\mathcal{E}(M) = \{X \subset E \mid X \text{ is a circuit }\}$$

So; $\mathcal{C}(M) \subset \mathcal{E}(M)$.

Definition 5.2. If $\Sigma \subset \mathcal{C}(M)$, we say Σ is a non-redundant if for every $\sigma \in \Sigma$ we have:

$$\bigcup_{\tau \in \Sigma} \tau \supsetneq \bigcup_{\tau \in \Sigma - \sigma} \tau, \text{ for all } \sigma \in \Sigma$$

Definition 5.3. Let $X \subset E$. The degree of X, denoted by deg(X), is given by:

$$deg(X) = max\{|\Sigma| \mid \Sigma \text{ is non-redundant and } \bigcup_{\tau \in \Sigma} \Sigma \subset X\}$$

Remark 5.1. $n(X) = deg(X) = |X| - r(X)$

Lemma 5.1. *Let $X = C_1 \cup \ldots \cup C_k$ be a union of circuits. Then there exists a non-redundant set of circuits $\{C_1{}', \ldots, C_l{}'\}$ with $C_1{}' \cup \ldots \cup C_l{}' = X$ and $l = deg(X)$. Furthermore, if $X = C_1 \cup \ldots \cup C_m$ is a non-redundant union of circuits with $deg(C_1 \cup \ldots \cup C_m) = m$, and if $Y \subsetneq X$, then $deg(Y) < deg(X) = m$.*

Proof. This follows from applying [10, Lemma 2] to $M|C_1 \cup \ldots \cup C_k$. □

Lemma 5.2. *Let $\mathcal{E}'(M)$ denote the set of non-redundant unions of circuits of M. Then*

$$\mathcal{E}'(M) = \mathcal{E}(M).$$

Proof. Since every redundant union of cycles can be made non-redundant by eliminating circuits so this is obvious. □

Lemma 5.3.

$$X \in \mathcal{E}(M) \Leftrightarrow n(Y) < n(X)$$

for all $Y \subsetneq X$ and $X \neq \emptyset$

Proof. Let $X = C_1 \cup \ldots \cup C_m$ be an element of $\mathcal{E}(M)$. By Lemma 5.2 and Lemma 5.3, we may assume that $C_1 \cup \ldots \cup C_m$ is a non-redundant union and that $deg(X) = m$. By combining Lemma 5.1 and [10, Proposition 1] , we see that if $Y \subsetneq X$ then $n(Y) < n(X)$.

Conversely, assume X does not belong to $\mathcal{E}(M)$. By [10, Proposition 1] then, there is a non-redundant set $\sum \subset \mathcal{C}(M)$ such that

$$\bigcup_{\tau \in \sum} \tau \subsetneq X$$

and $n(\bigcup_{\tau \in \sum}) = n(X)$ □

Corollary 5.1.

$$\mathcal{E}(M) = \bigcup_{j \geq 0} \{X \subseteq E \mid n(X) = j, X \neq \emptyset, n(Y) \leq j, \forall Y \subsetneq X\}$$

From now on we look at two matroids M_1 and M_2, with rank functions r_1 and r_2. Moreover $M_1 \subseteq M_2$ is the sense of simplicial complexes i.e $\mathcal{I}(M_1) \subseteq \mathcal{I}(M_2)$. Also we define $\rho = r_1 - r_2$.

Definition 5.4. A demi-matroid is a pair (E, r), where E is a finite set, and $r : 2^E \longrightarrow \mathbb{Z}$ is a function satisfying, for all $X \subset Y \subset E$ and $x \in E$:

1. $0 \leqslant r(X) \leqslant |X|$
2. $r(X) \leqslant r(Y)$
3. $r(X \cup x) \leqslant r(X) + 1$

Proposition 5.1. *The pair (E, ρ) is a demi-matroid if and only if $\mathcal{E}(M2) \subseteq \mathcal{E}(M_1)$.*

Proof. When $M_1 \subseteq M_2$ then ρ satisfies the non-negative subcardinal property of Theorem 4.2. Since $r_2(X) \geq r_1(X)$ for all $X \subset E$ and also

$$\rho(X) = r_2(X) - r_1(X) \leqslant r_2(X) \leqslant |X|$$

Also for monotone rank property, if $x \in E$ then

$$\rho(X \cup x) \geq r_2(X) - r_1(X \cup x) \geq r_2(X) - r_1(X) - 1 = \rho(X) - 1$$

$$\rho(X \cup x) \leqslant r_2(X \cup x) - r_1(X) \leqslant r_2(X) + 1 - r_1(X) = \rho(X) + 1$$

such that $|\rho(X \cup x) - \rho(X)| \leqslant 1$.

Suppose first that the pair (E, ρ) is a demi-matroid, that is ρ satisfies 2. Let $X \in \mathcal{E}(M_2)$, and let $Y \subsetneq X$. Let n_1 and n_2 denote the nullity function of M_1 and M_2 respectively. Then, by Lemma 5.3, we have

$$n_2(Y) < n_2(X)$$

$$n_1(Y) - \rho(Y) < n_1(X) - \rho(X)$$

since ρ satisfies (2), thus we get

$$n_1(Y) < n_1(X)$$

and $X \in \mathcal{E}(M_1)$ by Lemma 5.3. Thus $\mathcal{E}(M_2) \subseteq \mathcal{E}(M_1)$.

Conversely suppose that ρ does not satisfy (2). Then there must exist an $X \subset E$ with $x \in X$ such that $\rho(X \backslash x) = \rho(X) + 1$. We choose X to be a minimal subset of E which possesses this property. We look at:

$$n_1(X \backslash x) - n_2(X \backslash x) = n_1(X) - n_2(X) + 1$$

$$n_2(X) - n_2(X \backslash x) = 1$$

and

$$n_1(X) - n_1(X \backslash x) = 0$$

We get from Lemma 5.3 and $n_1(X) - n_1(X \backslash x) = 0$ that $X \in \mathcal{E}(M_1)$.

Now we assume that $X \in \mathcal{E}(M_2)$, and demonstrate that this leads to a contradiction. By Lemma 5.3 there must be a $y \in X$ such that $n_2(X) -$

$n_2(X\backslash y) = 0$ and by $n_2(X) - n_2(X\backslash x) = 1$ we know that $y \neq x$. For the sake of readability, we defer the demonstration that

$$r_2(X\backslash y) - r_2(X\backslash\{x, y\}) = 0$$

until the end of our proof.
But assume, for now that $r_2(X\backslash y) - r_2(X\backslash\{x, y\}) = 0$ holds. By our assumption that X is minimal, we have
$\rho(X\backslash y) - \rho(X\backslash\{x, y\}) \neq -1$, which is equivalent to

$$r_2(X\backslash y) - r_2(X\backslash\{x, y\}) - r_1(X\backslash y) - r_1(X\backslash\{x, y\}) \neq -1$$

$\Longrightarrow$

$$r_1(X\backslash y) - r_1(X\backslash\{x, y\}) = 0$$

We now compare

$$r_1(X) - r_1(X\backslash\{x, y\}) = r_1(X) - r_1(X\backslash x) + r_1(X\backslash x) - r_1(X\backslash\{x, y\})$$

and

$$r_1(X) - r_1(X\backslash\{x, y\}) = r_1(X) - r_1(X\backslash y) + r_1(X\backslash y) - r_1(X\backslash\{x, y\})$$

By combining above two equations we get

$$r_1(X) - r_1(X\backslash\{x, y\}) = 1$$

and the same equations then dictate

$$r_1(X\backslash x) - r_1(X\backslash\{x, y\}) = 0$$

and

$$r_1(X\backslash x) - r_1(X\backslash y) = 1$$

In conclusion we have

$$r_1(X\backslash x) = r_1(X\backslash\{x, y\})$$

$$r_1(X\backslash y) = r_1(X\backslash\{x, y\})$$

which according to [8, Lemma 1.3.3] implies

$$r_1(X) = r_1(X\backslash\{x, y\}).$$

However, from $n_2(X) - n_2(X\backslash x) = 1$ we had

$$r_1(X) = r_1(X\backslash x) + 1 = r_1(X\backslash\{x, y\}) + 1$$

and we get

$$r_1(X) - r_1(X\backslash\{x, y\}) = 1$$

which is a contradiction. We now complete our proof by showing that

$$r_2(X\backslash y) - r_2(X\backslash\{x, y\}) = 0$$

Similar to what we did for r_1, we compare

$$r_2(X) - r_2(X\backslash\{x, y\}) = r_2(X) - r_2(X\backslash x) + r_2(X\backslash x) - r_2(X\backslash\{x, y\})$$

and

$$r_2(X) - r_2(X\backslash\{x, y\}) = r_2(X) - r_2(X\backslash y) + r_2(X\backslash y) - r_2(X\backslash\{x, y\})$$

which together imply

$$r_2(X\backslash y) - r_2(X\backslash\{x, y\}) = 0$$

This completes our proof.

□

Definition 5.5. (Higher weights for a pair of matroids). Let $M_1 \subseteq M_2$ be matroids with $\mathcal{E}(M_2) \subseteq \mathcal{E}(M_1)$. We define:

$$d_i(E, \rho) = min\{|X| : X \subset E, \rho(X) = i\},$$

and call $d_i(E, \rho)$ as the i-th higher weight of the demi-matroid (E, ρ).

Remark 5.2. If $M_2 = P(E)$, so $r_2(X) = |X|$ for all $X \subset E$. Then

$$d_i(E, \rho) = min\{|X| \mid |X| - r_1(X) = i\}$$

and this is usual $d_i(M_1)$. Hence Definition 4.8 is a generalization of the usual Hamming weights.

Lemma 5.4. *Let $M_1 \subseteq M_2$ be matroids on a ground set E with the property that (E, ρ) is a demi-matroid, and let $X \subset E$ with $|X| \leqslant d_1 - 1$. Then*

$$M_1|X = M_2|X.$$

Proof. For all $Y \subset X$, we have $r_1(Y) = r_2(Y)$. □

We will now study the $\mathbb{Z}-graded$ Betti-numbers of the Stanley -Reisner rings of the matroids M_1 and M_2 appearing in the previous Chapter 3.

Proposition 5.2. *For Stanley Reisner ring S/I_Δ, with $\Delta = \{Independent\ sets\ of\ a\ matroid\}$, the Betti numbers $\beta_i, \beta_{i,j}$ and $\beta_{i,\delta}$ are independent of the field $\mathbb{K}$.*

Proof. Let $\sigma \subset \{1, \cdots, n\}$ then

$$\beta_{i,\sigma}(I_M) = h_{|\sigma|-i-2}(M|_\sigma, \mathbb{K})$$

Now

$$\beta_{i,d}(I_M) = \sum_{|\sigma|=d} \beta_{i,\sigma}(I_M)$$

Since M is a matroid so $M|_\sigma$ is a matroid and this implies that $h_{|\sigma|-i-2}(M|_\sigma, \mathbb{K})$ is independent of $\mathbb{K}$, and $\beta_{i,d}(I_M) = \sum_{|\sigma|=d} h_{d-i-2}(M|_\sigma, \mathbb{K})$ is independent of $\mathbb{K}$ □

Proposition 5.3. *Let $M_1 \subseteq M_2$ be matroids on E with the property that (E, ρ) is a demi-matroid, and let $j \leqslant d_1 - 1$. Then*

$$\beta_{i,j}(M_1) = \beta_{i,j}(M_2)$$

for all $i \geqslant 0$.

Proof.

$$\beta_{i,j}(M_1) = \sum_{|\sigma|=j} \beta_{i,\sigma}(M_1) \tag{5.1}$$

$$= \sum_{|\sigma=j|} \widetilde{h}^{|\sigma|-i-2}(M_1|\sigma, \mathbb{K}) \tag{5.2}$$

which according to Lemma 5.4 is equal to

$$\sum_{|\sigma|=j} \widetilde{h}^{|\sigma|-i-2}(M_2|\sigma, \mathbb{K}) = \sum_{|\sigma|=j} \beta_i, \sigma(M_2) = \beta_{i,j}(M_2)$$

□

Proposition 5.4. *Let $M_1 \subsetneq M_2$ be matroids on E with the property $(E, r_2 - r_1)$ is a demi-matroid. Then*

$$\beta_{1,d_1}(M_1) \neq \beta_{1,d_1}(M_2)$$

5.1 Open questions

It is an open question in what way the higher Betti numbers of M_1 and M_2 are related to the higher $d_i(E, \rho)$.

Is it true that

$$\beta_{2,j}(M_1) = \beta_{2,j}(M_2) \text{ for } j \leqslant d_2 - 1$$

and

$$\beta_{3,j}(M_1) = \beta_{3,j}(M_2) \text{ for } j \leqslant d_3 - 1$$

Bibliography

[1] Britz., Thomas., Johnsen., Trygve., Mayhew., Dillon., Shiromoto., Keisuke., *Wei-type duality theorems for matroids*, Designs, Codes and Cryptography, 62 (March 2012), no. 3, 331–341.

[2] Gary., Gordon., *On Brylaswski's Generalized Duality*, Mathematics in Computer Science 6, (June 2012), no. 2, 135–146.

[3] Herzog, J. Hibi, T, Monomial Ideals. Graduate texts in Mathematics, 260. Springer-Verlag London Limited, 2011.

[4] Jan Nyquist Roksvold, *Pair of matroids*, Private publication, University of Tromsœ.

[5] Larsen, A.H., *Matroider og lineære koder*, Master in algebra, University of Bergen, 2005.

[6] Martin, James. *Matroid, Demi-Matroids and Chains of Linear Codes*, Masters's Thesis in mathematics, University of Tromsœ, 2010.

[7] Oxley, J., *Matroid theory*. Second edition. Oxford Graduate Texts in Mathematics, 21. Oxford University Press, Oxford, 2011.

[8] Oxley, J., *Matroid theory*. Second edition. Oxford University Press Inc, New York, 1992.

[9] Thomas Britz., Trygve Johnsen., James Martin., *Chains, Demi-Matroids, and Profiles*, IEEE Transactions on information thoery 60 (February 2014), no. 2, 986–991.

[10] Verdure, H., Trygve., Johnsen., *Hamming weights and Betti numbers of Stanley-Reisner rings associated to matroids*. Appl. Algebra Engrg. Comm. Comput. 24 (2013), no. 1, 73–93.

[11] Verdure, H., Trygve., Johnsen.,*Stanley-Reisner resolution of constant weight linear codes*, Designs, Codes and Cryptography 72 (August 2014), no. 2, 471–481

[12] Verdure, H., Trygve, Johnsen.,*Coding theory and matroid theory*, November 12, 2013.

[13] Wei, V., *Generalized Hamming weights for linear codes.* IEEE Trans. Inform. Theory 37 (1991), no. 5, 1412–1418.

UNIVERSITY OF TROMSØ