MAT-3900

MASTER'S THESIS IN MATHEMATICS

# Matroids, Demi-Matroids and Chains of Linear Codes

James Martin

November, 2010

FACULTY OF SCIENCE AND TECHNOLOGY
Department of Mathematics and Statistics
University of Tromsø

MAT-3900

MASTER'S THESIS IN MATHEMATICS

# Matroids, Demi-Matroids and Chains of Linear Codes

James Martin

November, 2010

# Acknowledgements

Firstly, I would like to express sincere thanks to my supervisor, Professor Trygve Johnsen, Head of The Dept. of Mathematics and Statistics at The University of Tromsø. His help, encouragement, expert advice and guidance throughout the composition of this thesis were and are greatly appreciated. It has been a great pleasure having him as my supervisor over the past two years.

I would also like to thank my family especially my parents for all their encouragement and support for the duration of this Masters program.

# Contents

# Introduction

The central theme of this thesis is the study of matroids and related concepts. A matroid is a combinatorial structure which can be defined in several different but, equivalent ways. We can view it as a structure that captures the essence of the notion of independence and which generalises this notion for matrices and graphs. It is an ordered pair consisting of a finite set (the ground set of the matroid) and a collection of subsets (the independent sets of the matroid) of the ground set, which satisfy certain conditions. We study matroids in connection with related phenomena like linear codes and graphs. Codes and graphs both motivate the definition of matroids and give interesting and striking examples of the relevance of the concept. Following [1] we also show how the definition of matroids can be relaxed so that other objects, namely demi-matroids, arise. In more than half of the thesis we study themes related to demi-matroids. We study how some results in coding theory are essentially consequences of results for demi-matroids.

In Chapter 1 we list the basic properties of matroids. Definitions and proofs in this chapter are taken from [6].

In Chapter 2 we list the basic properties of block codes over finite alphabets and linear codes. We describe how matroids arise from linear codes. While a large portion of this chapter is comprised of well known facts and definitions some information has been sourced [3].

In Chapter 3 we first sketch some basic properties of graphs and matroids derived from graphs. Then we describe the concepts of deletion and contraction for graphs and matroids and puncturing and shortening of linear codes. We describe how these phenomena are related to each other. Definitions, graphs and examples in this chapter have been sourced from [4], [6] and [7].

Collectively chapters 1-3 are intended to show the deep connections between graphs, codes and matroids but, we do not claim to show anything new in these chapters.

In Chapter 4 we recall the definition of demi-matroids from [1] and study associated invariants in detail.

In Chapter 5 we study higher weights of linear codes and give them a (demi-)matroid theoretical interpretation.

Chapters 4 and 5 are inspired by [1] and give a more detailed exposition of the topics treated there.

In Chapter 6 we study chains of linear codes or multi-codes. We show how they give rise to demi-matroids and describe duality.

In Chapter 7 we generalise concepts and results in [5] for pairs of codes to multi-codes and we use a demi-matroid theoretical setting.

Collectively chapters 4-7 are intended to show a connection between chains of linear codes (and chains of graphs since each graph in the chain gives rise to a matroid which is vectorial and thus can be associated with a linear code) and demi-matroids.

We end the thesis by giving a generalisation of the Singleton bound to multi-codes and a generalisation of MDS codes to optimal chains of codes.

# Chapter 1

# Matroids

Matroids were introduced by Hassler Whitney in 1935 in an effort to try to capture abstractly the essence of dependence. They are an abstraction of several combinatorial structures (such as matrices and graphs) and can be defined in several different but, equivalent ways. In this section, four definitions for a matroid will be presented along with the relationships which connect them [7].

## 1.1 Linearly Independent Sets of a Matroid

**Definition 1** *A matroid M is an ordered pair* $(E, \mathcal{I})$ *consisting of a finite set, E and a collection* $\mathcal{I}$ *of subsets of E satisfying the following three conditions*

**($\mathcal{I}$1)** $\emptyset \in \mathcal{I}$.

**($\mathcal{I}$2)** If $I \in \mathcal{I}$ and $I' \subseteq I$, *then* $I' \in \mathcal{I}$.

**($\mathcal{I}$3)** If $I_1$and $I_2$ are in $\mathcal{I}$ and $|I_1| < |I_2|$ , then there is an element $e$ of $I_2 - I_1$ such that $I_1 \cup$ $e$ $\in \mathcal{I}$.

If $M$ is the matroid *(E, $\mathcal{I}$)*, then $M$ is called a matroid on $E$. The members 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***.

## 1.2 Bases of a Matroid

Defining a matroid in terms of all the independent sets associated with it, is an unnecessarily cumbersome approach to take. If instead a matroid is described in terms of its maximal independent sets (from which all independent sets can be obtained, by **($\mathcal{I}$2)** above) a much more efficient definition of a matroid is attained.

**Definition 2** *A maximal independent set in M is called a* ***basis*** *or a* ***base*** *of M.*

**Lemma 3** *If $B_1$and $B_2$ are bases of a matroid M, then $|B_1| = |B_2|$.*

If $\mathcal{B}$ is the set of bases of a matroid M then the following axioms hold.

**(B1)** $\mathcal{B}$ is non-empty (from **($\mathcal{I}$1)**).

**(B2)** If $B_1$ and $B_2$ are members of $\mathcal{B}$ and $x \in B_1 - B_2$, then there is an element $y$ of $B_2 - B_1$ such that $(B_1 - x) \cup y \in \mathcal{B}$.

**Theorem 4** *Let E be a set and $\mathcal{B}$ be a collection of subsets of E satisfying* ***(B1)*** *and* ***(B2).*** *Let $\mathcal{I}$ be the collection of subsets of E that are contained in some members of $\mathcal{B}$. Then (E, $\mathcal{I}$) is a matroid having $\mathcal{B}$ as its collection of bases.*

## 1.3 Circuits of a Matroid

**Definition 5** *A* ***minimal dependent set*** *is one whose proper subsets are independent.*

**Definition 6** *A* ***circuit*** *of a matroid M is a minimal dependent set of M.*

A matroid M is uniquely determined by its set of circuits $\mathcal{C}$, since $\mathcal{I}$ (the set of independent sets of M) can be obtained from $\mathcal{C}$. If $\mathcal{C}$ is the set of circuits of a matroid then the following axioms hold.

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

**(C2)** If $C_1$and $C_2$ are members of $\mathcal{C}$ and $C_1 \subseteq C_2$, then $C_1 = C_2$.

**(C3)** If $C_1$and $C_2$ are distinct members of $\mathcal{C}$ and $e \in C_1 \cap C_2$, then there is a member $C_3$ of $\mathcal{C}$ such that $C_3 \subseteq (C_1 \cup C_2) - e$.

**Theorem 7** *Let E be a set and $\mathcal{C}$ be a collection of subsets of E satisfying (C1), (C2) and (C3). Let $\mathcal{I}$ be the collection of subsets of E that contain no member of $\mathcal{C}$. Then (E, $\mathcal{I}$) is a matroid having $\mathcal{C}$ as its collection of circuits.*

The set of circuits $\mathcal{C}$ and set of bases $\mathcal{B}$ of a matroid are related as follows. $\mathcal{B}$ is the collection of maximal subsets of $E$ that contain no member of $\mathcal{C}$, while $\mathcal{C}$ is the collection of minimal sets that are contained in no member of $\mathcal{B}$.

## 1.4 Rank of a Matroid

**Definition 8** *Let M = (E, $\mathcal{I}$) be a matroid, and let $X \subseteq E$.The* ***rank function*** *of M is the function $r : 2^E \to \mathbb{N}_0$ with $r(X) = \max(|I| \mid I \subseteq X, I \in \mathcal{I})$. $r(X)$ is called the* ***rank*** *of X.*

**Definition 9** *For any subsets X, Y of E, the rank function of a matroid M on E is a function $r : 2^E \to \mathbb{N}_0$ with the following properties:*

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

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

**(R3)** If $X$ and $Y$ are subsets of $E$, then $r(X \cup Y) + r(X \cap Y) \leq r(X) + r(Y)$.

**Theorem 10** *Let E be a set and let r be a function that maps $2^E \to \mathbb{N}_0$ and satisfies (R1), (R2) and (R3). Let $\mathcal{I}$ be the collection of subsets X of E for which $r(X) = |X|$. Then (E, $\mathcal{I}$) is a matroid having rank function r.*

If M is the matroid (E, $\mathcal{I}$) with rank function $r$ and $X \subseteq E$ then the following are true:

1. $X$ is an ***independent set*** iff $|X| = r(X)$.

2. $X$ is a ***basis*** iff $|X| = r(X) = r(M)$.

3. $X$ is a ***circuit*** iff $X$ is non-empty and, for all $x \in X$, $r(X - x) = |X| - 1 = r(X)$.

## 1.5 Vectorial Matroids

The most renowned examples of matroids are those obtained from the columns of a matrix over a given field. These are indeed the examples which have given rise to the name matroid, since we can concider matroids as structures, derived from matrices. To be more precise:

**Proposition 11** *If E is the list of labels of column vectors of an $m \times n$ matrix A over a field F and $\mathcal{I}$ the set of subsets of E such that the multiset of columns labelled by the subset is linearly independent over $F^m$ then (E, $\mathcal{I}$) is a matroid.*

**Proof.** Clearly $\mathcal{I}$ satisfies ($\mathcal{I}1$) and ($\mathcal{I}2$). Let $I_1$ and $I_2$ be linearly independent subsets of E such that $|I_1| < |I_2|$. Let W be the subspace of F$^m$ spanned by $I_1 \cup I_2$. Then $\dim(W)$, the dimension of W, is at least $|I_2|$ . Now suppose that $I_1 \cup e$ is linearly independent for all $e$ in $I_2 - I_1$. Then W is contained in the span of $I_1$. Thus $|I_2| \le \dim(W) \le |I_1| < |I_2|$; a contradiction. We conclude that $I_2 - I_1$ contains an element $e$ such that $I_1 \cup e \in \mathcal{I}$, that is ($\mathcal{I}3$) holds. ■

**Example 12** *Let A be the matrix*

$$\begin{array}{c} \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array} \\ \begin{bmatrix} 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix} \end{array}$$

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

*$\mathcal{I}$={∅, {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}}.*

**Definition 13** *If a matroid M is isomorphic to the vector matroid of a matrix D over a field F, then M is said to be* ***representable over F*** *or* ***F-representable****. A matroid is* ***representable*** *if it is representable over some field.*

**Definition 14** *The non-Pappus matroid is the matroid on E = {1, 2, 3, 4, 5, 6 , 7, 8, 9} whose bases are all triples except {1,2,3}, {7,8,9}, {1,4,8}, {2,4,7}, {1,5,9}, {3,5,7}, {2,6,9}, {3,6,8}.*

**Claim 15** *The non-Pappus matroid is not F-representable for a field F and is thus an example of a matroid which does not arise from a matrix.*

**Proof.** For a proof of the above claim see [6] pg173. ■

## 1.6 Dual of a Matroid

**Definition 16** *For the matroid $M$ with ground set $E$ and set of bases $\mathcal{B}$ (which we can denote as $\mathcal{B}(M)$) there exists another matroid $M^*$ with ground set $E$ and set of bases $\mathcal{B}^*$ (which we can denote as $\mathcal{B}^*(M)$) given by $\mathcal{B}^* = \{E - B \mid B \in \mathcal{B}\}$ this matroid is called **the dual** of $M$.*

Thus $\mathcal{B}(M^*) = \mathcal{B}^*(M)$ and it is clear that since $(\mathcal{B}(M^*))^* = \mathcal{B}(M)$ then $(M^*)^* = (M)$.

**Theorem 17** *If $M$ is the vector matroid of $[I_k|A] = G$, then $M^*$ (the dual matroid) is the vector matroid of $[-A^T|I_{n-k}] = H$.*

**Example 18** *Considering the matroid $M$ of Example 12. The dual matroid $M^*$ has set of bases $\mathcal{B}^*$, set of independent sets $\mathcal{I}^*$ and set of circuits $C^*$ given by:*

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

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

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

The set of bases, independent sets and circuits of $M^*$ are called the **cobases**, **coindependent sets** and **cocircuits** of $M$ respectively.

**Definition 19** *The rank function of $M^*$ is called the **corank** function of $M$.*

**Proposition 20** *For all subsets $X$ of the ground set $E$ of a matroid $M$,*

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

**Proof.** See [6] page 72. ■

## 1.7 Matroid Isomorphisms

The matroids $\mathrm{M}_1$= $(E, \mathcal{I})$ and $\mathrm{M}_2$= $(E', \mathcal{I}')$ are ***isomorphic***, if there is a bijection $\phi : E \to E'$ such that for all $X \subseteq E$, $\phi(X)$ is independent in $\mathrm{M}_2$ iff $X$ is independent in $\mathrm{M}_1$.

**Example 21** *For the matroid (E, $\mathcal{I}$) in the previous example, taking $\phi : E \to E$, such that $\phi = \begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 2 & 4 & 5 & 1 & 3\end{pmatrix}$ then the set of linearly independent sets of the matroid (E, $\mathcal{I}^{'}$ ) given by $\phi(\mathcal{I}) = \{\phi(x) \mid x \in \mathcal{I}\}$ is $\mathcal{I}^{'}$={∅, {1}, {2}, {3}, {4}, {5}, {1,3}, {1,4}, {1,5}, {2,3}, {2,4}, {2,5}, {3,4}, {3,5}, {4,5}, {1,3,4}, {1,3,5}, {1,4,5}, {2,3,4}, {2,3,5}, {2,4,5}}. In this example the matroid (E, $\mathcal{I}^{'}$ ) has the same ground set {1,2,3,4,5} as (E, $\mathcal{I}$) but, (E, $\mathcal{I}^{'}$ ) is the matroid associated with the matrix $A^{'}$obtained from A by permuting the columns of A correspondingly.*

$$\begin{array}{cc} & \begin{matrix}1 & 2 & 3 & 4 & 5\end{matrix}\\ A = & \begin{bmatrix}0 & 0 & 1 & 0 & 1\\ 0 & 1 & 0 & 1 & 0\\ 1 & 0 & 1 & 0 & 1\end{bmatrix}\end{array} \qquad \begin{array}{cc} & \begin{matrix}1 & 2 & 3 & 4 & 5\end{matrix}\\ A^{'} = & \begin{bmatrix}0 & 0 & 1 & 0 & 1\\ 1 & 0 & 0 & 1 & 0\\ 0 & 1 & 0 & 0 & 1\end{bmatrix}\end{array}$$

**Remark 22** *We observe that if $M_1 \backsimeq M_2 \Rightarrow M_1^* \backsimeq M_2^*$.*

**Remark 23** *Two isomorphic matroids have the same number of elements in their respective ground sets .i.e. $E(M) = n$. Since there exists a bijection between the bases of two isomorphic matroids they have the same rank k.*

# Chapter 2

# Coding Theory

**Definition 24** *Let A be a finite alphabet given by* $\{a_1, a_2, a_3...., a_q\}$ *where* $q \in \mathbb{N}$*. Then a* ***code word*** *over A is an element (n-tuple) of* $A^n$ *for some* $n \in \mathbb{N}_0 = \{0, 1, 2, ....\}$ *and* $A^0$ *is considered to be the empty word.*

**Example 25** *If* $A = \{a, b, c, ..., y, z, æ, ø, å\}$ *(the Norwegian alphabet) then* $c \in A$*,* $(p, å) \in A^2$*,* $(s, a, w) \in A^3$.

The set of all possible code words is given by **V**= $\overset{\infty}{\underset{n=0}{\cup}} A^n = \{\{\emptyset\} \cup A \cup A^2 \cup A^3 \cup ....\}$.

**Definition 26** *A* ***code*** *is a subset of* ***V*** *i.e.* $C \subseteq \mathbf{V}$.

**Example 27** *If A={a,b,c,.....,x,y,z} (the English alphabet) then a list of all English words is a code.*

**Definition 28** *A* ***block code*** *C is a subset of* $A^n$ *for a fixed value of* **code word length** *n i.e.* $C \subseteq A^n$*,*$n \geq 1$.

**Definition 29** *If the alphabet A is a finite field* $F_q$*, then for some fixed n, the sub vector space C of the vector space* $(F_q)^n$ *is called a* ***linear code.***

Assume C is a block code whose alphabet A is a group G, such that $C \subseteq G^n$. Let $\mathbf{g} = (g_1, g_2, ..........., g_n)$ and $\mathbf{h} = (h_1, h_2, .........., h_n) \in C$. Multiplication is defined as $\mathbf{gh} = (g_1h_1, g_2h_2, ...., g_nh_n)$ and is such that $gh \in G^n$. This operation makes $G^n$ a group.

**Definition 30** *A code $C$ is called a **group code** if:*

1. $(1, 1, ...., 1) \in C$. $1 =$ *identity element of* $G$.

2. *For* $(g_1, g_2, .........., g_n) \in C$, *then* $(g_1^{-1}, g_2^{-1}, .........., g_n^{-1}) \in C$

3. *For* $g, h \in C$, $gh \in C$.

**Example 31** *For the additive group $G$ with* $\mathbf{g} = (g_1, g_2, .........., g_n)$, $\mathbf{h} = (h_1, h_2, .........., h_n) \in G$, *if* $C \subseteq G^n$ *is a group code, then the following are true:*

1. $(0, 0, 0, ........, 0) \in C$.

2. *If* $(g_1, g_2, .........., g_n) \in C$, *then* $(-g_1, -g_2, .........., -g_n) \in C$.

3. *If* $g, h \in C$ *then* $gh = (g_1 + h_1, g_2 + h_2, .........., g_n + h_n) \in C$

If the block code alphabet is over a field F (with addition as its group operation), i.e. $C \subseteq F^n$ then the code is a **linear code** if:

1. For $\mathbf{g} = (g_1, g_2, .........., g_n) \in C$, $k(g_1, g_2, .........., g_n) \in C$ where the constant $k \in F$.

2. $g, h \in C$ then $gh = (g_1 + h_1, g_2 + h_2, .........., g_n + h_n) \in C$

**Remark 32** *It is clear that requirements 1. and 2. of definition 30 for a group code are satisfied by 1. and 2. above.*

**Claim 33** *The **number of code words** $M$ in a block code $C$ is finite.*

**Proof.** **M**$=|C| \leq |A^n| = q^n$ where $q = |A|$ i.e. the number of code words in C is less than or equal to the total number of possible code words. ■

**Definition 34** *The **dimension** (or rank) $k$ of a code is defined as* $k = \log_q M$.

k will only be an integer if $M = q^k$ for some $k \in \mathbb{N}_0$.

**Remark 35** *For a linear code $C$ it is observed that* $\dim(C) = k \in \mathbb{N}_{0.}$

**Definition 36** *The **Hamming distance** between two vectors **a** and **b** of $A^n$ is the number of places in which they differ. Formally if* $\mathbf{a} = (a_1, a_2, .........., a_n)$ *and* $\mathbf{b} = (b_1, b_2, .........., b_n)$ $\in A^n$*. The Hamming Distance* $d(\mathbf{a}, \mathbf{b})$ *is given by:*

$$d(\mathbf{a}, \mathbf{b}) = |\{i|a_i \neq b_i, i = 1, 2, ....n.\}|$$

The Hamming distance satisfies the following three requirements for a metric:

1. $d(\mathbf{a}, \mathbf{b}) \geq 0$, with equality iff $\mathbf{a} = \mathbf{b}$.

2. $d(\mathbf{a}, \mathbf{b}) = d(\mathbf{b}, \mathbf{a})$.

3. $d(\mathbf{a}, \mathbf{c}) \leq d(\mathbf{a}, \mathbf{b}) + d(\mathbf{b}, \mathbf{c})$.

**Definition 37** *The **(minimum) distance** of a code, denoted d(C), is the smallest value of Hamming distance considered over all pairs of distinct code words in the code. Formally* $d(C) = \min\{d(\mathbf{a}, \mathbf{b})|\mathbf{a}, \mathbf{b} \in C, \mathbf{a} \neq \mathbf{b}\}$

**Definition 38** *The **minimum distance** d **of a linear code** C is equal to the smallest of the weights of the non-zero code words.*

**Definition 39** *Two q-ary block codes are in general called **equivalent** if one can be obtained from the other by a combination of operations of the following types:*

1. *A permutation of the positions of the code.*

2. *A permutation of the symbols appearing in a fixed position.*

**Example 40** *If (2,5,0,4,1) and (3,2,6,0,5) are two code words of a code C over $F_7$, then a permutation of positions 2 and 4 yield the code words (2,4,0,5,1) and (3,0,6,2,5) of the equivalent code Č. Č is obtained from C by applying this permutation to all code words in C. This is an example of operation 1.*

**Example 41** *If (2,5,0,4,1), (1,2,3,5,6), and (3,2,6,0,5) are three code words of a code C over $F_7$, then a permutation* $\sigma = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 2 & 5 & 0 & 1 & 4 & 3 \end{pmatrix}$ *of the symbols in position 3 yields the* *code words (2,5,6,4,1), (1,2,0,5,6) and (3,2,3,0,5) of the equivalent code $\hat{C}$. $\hat{C}$ is obtained from $C$ by applying a permutation of this type to all code words in $C$. This is an example of operation 2.*

**Remark 42** *When dealing with linear q-ary codes, we use a more restrictive version of equivalence, called* ***linear equivalence*** *where operation 2 is specified to be:*

2'. A permutation of the symbols appearing in a fixed position obtained by multiplying all of them by a fixed non-zero field element.

Since the distance between two code words is given by the number of places in which they differ, it is clear that distance of the code $d(C)$ remains unaltered by these two operations. Thus two equivalent codes have the same distance. Similarly the length of the code words $n$ remains unchanged by these permutations and equivalent codes have the same length.

**Definition 43** *The* ***Dual Code*** *of a linear code $C \subseteq (F_q)^n$ is the linear code defined by $C^{\perp} = \{x \in (F_q)^n | < x, c >= 0 \ \forall c \in C\}$ where $< x, c >= \sum_{i=1}^{n} x_i c_i$ is a scalar product. If $C$ is an $[n,k]$-code over $F_q$ then $C^{\perp}$ is a linear $[n, n-k]$ code. $(C^{\perp})^{\perp} = C$.*

**Definition 44** *Given a linear code $C$, a $(k \times n)$* ***generator matrix*** *$G$ of $C$ is a matrix whose rows generate all the elements of $C$, i.e. if $G = (r_1 r_2 ... r_k)^T$ then every code word $w$ of $C$ can be represented as a linear combination of the row vectors of $G$ in a unique way i.e. $w = c_1 r_1 + c_2 r_2 + ... + c_k r_k = \mathbf{c}G$, where $\mathbf{c} = (c_1 c_2 ... c_k)$.*

Two $k \times n$ matrices generate *equivalent linear codes* (of length $n$ and dimension $k$) over $F$ if one matrix can be obtained from the other by a sequence of operations of the following types:

(R1) Permutation of rows.

(R2) Multiplication of a row by a non-zero scalar.

(R3) Addition of a scalar multiple of one row to another.

(C1) Permutation of the columns.

(C2) Multiplication of any column by a non-zero scalar.

**Theorem 45** *Let $G$ be a generator matrix of an $[n,k]$-code. Then by performing operations of types (R1), (R2), (R3), (C1) and (C2), $G$ can be transformed to the* ***standard form*** *$[I_k|A]$ where $I_k$ is the $k \times k$ identity matrix, and $A$ is a $k \times (n-k)$ matrix.*

**Definition 46** *A **parity check matrix** $H$ of a linear code $C$ is a generator matrix of the dual code $C^{\perp}$. As such, a code word $c$ is in $C$ if and only if the product $cH^T = 0$.*

***Theorem 47*** *If $G = [I_k|A]$ is the standard form generator matrix of an $[n, k]$-code $C$, then a parity check matrix for $C$ is $H = [-A^T|I_{n-k}]$.*

If $G$ is a *generator matrix* for a code $C$ and $H$ is a *parity check matrix* for $C$, then $H$ is a *generator matrix* for $C^{\perp}$ and $G$ is a *parity check matrix* for $C^{\perp}$.

## 2.1 Matroids obtained from Linear Codes

Proposition 11 provides us with a way to relate two matroids $M_G(C)$ and $M_H(C)$ (via our generator matrix and parity check matrix respectively) to our linear code C.

Replacing the generator matrix G by another generator matrix G' gives the same matroid as for G i.e. $M_G(C) = M_{G'}(C)$. This is obvious since G' is obtained from G by a series of elementary row operations, which does not effect the columns of the matrix, whose linear independence determine the matroid.

**Definition 48** *We define $M_G(C) = M(C)$ for any generator matrix of C and $M^{\perp}(C) = M_H(C)$ for any parity check matrix of C.*

**Theorem 49** *For a linear code C, the matroids $M_G(C)$ and $M_H(C)$ are dual to each other.*

**Proof.** If G is a generator matrix for C, (with corresponding vector matroid $M_G(C)$) it can be reduced to standard form to give $G' = [I_k|A]$ and then $H = [-A^T|I_{n-k}]$ is a parity check matrix for C. Theorem 17 shows that $M_G(C)$ and $M_H(C)$ (the vector matroid associated with $H$) are dual matroids. Since $(M^*)^* = M$ the result follows. ■

**Corollary 50** *The generator matrix $G$ of a linear code $C$ is a parity check matrix for the dual code $C^{\perp}$ and the parity check matrix $H$ of $C$ is a generator matrix for $C^{\perp}$.This yields the following relationship between codes and matroids : $M^{\perp}(C) = (M(C))^*$ and $M(C^{\perp}) = (M(C))^*$*

## 2.2 Code Parameters and Matroid isomorphism Classes.

Given a linear code $C$ with generator matrix $G$. If $\dim(C) = k$ and word length is $n$, then $G$ is a $k \times n$ matrix of rank $k$. This gives that for the matroid $M_G(C)$, $E(M_G)$ has $n$ elements. The rank of $M_G(C) = k$ and the rank of $M_H(C) = n - k$, while $E(M_H) = n$.

Since all matroids isomorphic to $M_G(C)$ have ground sets $E(M)$ with the same cardinality $n$ and same rank $k$, both $n$ and $k$ are determined by properties which are only dependent on the isomorphism class of $M_G(C)$. (Similarly for $M_H(C)$).

Since the number of words in the code $M = q^k$ is determined by $k$ and $k$ in turn is determined by the isomorphism class of $M_G(C)$ then $M$ is also determined by isomorphism class of $M_G(C)$. (Similarly for $M_H(C)$).

**Theorem 51** *Suppose $C$ is a linear code of length $n$ and dimension $k$ over $F_q$ with parity check matrix $H$. The minimum distance of $C$ is $d$ if and only if any $d-1$ columns of $H$ are linearly independent but some $d$ columns are linearly dependent.*

**Proof.** The minimum distance of $C$ is equal to the smallest of the weights of the non-zero code words. Let $\mathbf{x} = x_1 x_2 .....x_n$ be a vector in $(F_q)^n$.

Then $\mathbf{x} \in \mathbf{C} \Longleftrightarrow \mathbf{x}H^T = 0 \Longleftrightarrow x_1\mathbf{H}_1 + x_2\mathbf{H}_2 + ..... + x_n\mathbf{H}_n = 0$, where $\mathbf{H}_1, \mathbf{H}_2, ....., \mathbf{H}_n$ denote the columns of $H$.

Thus corresponding to each code word $\mathbf{x}$ of weight $d$, there is a set of $d$ linearly dependent columns of $H$. On the other hand if there existed a set of $d-1$ linearly dependent columns of $H$, say $\mathbf{H}_{i_1}, \mathbf{H}_{i_2}, ....., \mathbf{H}_{i_{d-1}}$, then there would exist scalars $x_{i_1} x_{i_2} ..... x_{i_{d-1}}$, not all zero, such that $x_{i_1}\mathbf{H}_{i_1} + x_{i_2}\mathbf{H}_{i_2} + ..... + x_{i_{d-1}}\mathbf{H}_{i_{d-1}} = 0$. But then the vector $\mathbf{x} = (0...0x_{i_1}0...0x_{i_2}0.....0x_{i_{d-1}}0....0)$, having $x_{i_j}$ in the $i_j$th position for $j = 0, 1, 2, ...., d-1$, and 0s elsewhere, would satisfy $\mathbf{x}H^T = 0$ and so would be a non-zero code word of weight less than $d$. ■

From Theorem 51 we have that $d(C) =$ minimum number of linearly dependent columns of $H$ i.e. a circuit. So $d(C)$ is the smallest possible cardinality for a circuit in $M_H(C)$. Clearly the number $d(C)$ is only dependent on the isomorphism class of $M_H(C)$ and this in turn depends only on the isomorphism class of $M_H(C)$ which is only dependent on the isomorphism class of $M_G(C)$ which is dual to $M_H(C)$.

**Conclusion 52** *In summary the code parameters $n, k, d, M$ of a linear code $C$ are only dependent on the isomorphism classes of the matroids $M(C)$ (and also $M^{\perp}(C)$).*

**Remark 53** *Equivalent linear codes give isomorphic matroids. This is true since performing the row operations (R1), (R2), (R3) and column operation (C2), leaves the matroid unaltered. While using operation (C1) one permutes columns and obtains an isomorphic matroid.*

# Chapter 3

# Graph Theory

A graph consists of a non-empty set $V(G)$ of *vertices* and a multiset $E(G)$ of *edges* each of which consists of an unordered pair (possibly identical) vertices. If $e \in E(G)$ and $e = \{u, v\}$ where $u$ and $v$ are in $V(G)$, then we say that $u$ and $v$ are *neighbours* or *adjacent*, and $e$ is *incident* with $u$ and $v$. We call $V(G)$ and $E(G)$ the vertex set and edge set, respectively, of the graph G.

Figure 1 is a pictorial representation of a particular graph. The vertex and edge set of this graph are $\{v_1, v_2, .., v_5\}$ and $\{e_1, e_2, .., e_5\}$, respectively. An edge such as $e_5$, which joins a vertex to itself, is called a *loop*. Edges such as $e_2$ and $e_3$, which join the same pair of distinct vertices are called *parallel edges*. The vertex $v_5$ which does not meet any edges, is an *isolated vertex*. The *ends* of the edge $e_1$ are $v_1$ and $v_2$.

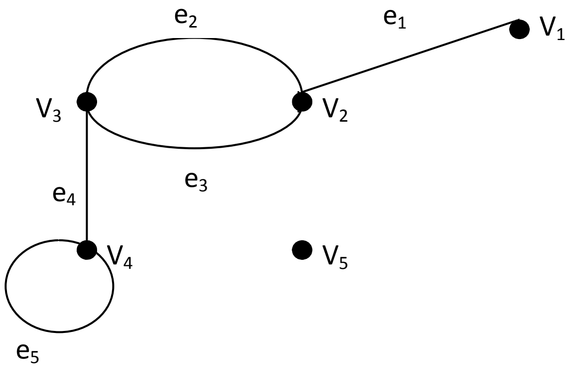


Figure 1

A graph is *simple* if it has no loops and no parallel edges.

A graph $H$ is a *subgraph* of a graph $G$ if $V(H)$ and $E(H)$ are subsets of $V(G)$ and $E(G)$, respectively. If $V'$ is a non-empty subset of $V(G)$, then $G[V']$ denotes the subgraph of $G$ whose vertex set is $V'$ and whose edge set consists of those edges of $G$ which have both endpoints in $V'$. We say that $G[V']$ is the subgraph of $G$ *induced* by $V'$. Similarly if $E'$ is a non-empty subset of $E(G)$, then $G[E']$ the subgraph of G induced by $E'$, has $E'$ as its edge set and the set of endpoints of edges in $E'$ as its vertex set.

If $G_1$ and $G_2$ are graphs, their union $G_1 \cup G_2$ is the graph with vertex set $V(G_1) \cup V(G_2)$ and edge set $E(G_1) \cup E(G_2)$. If $V(G_1)$ and $V(G_2)$ are disjoint, then so are $E(G_1)$ and $E(G_2)$ and $G_1$ and $G_2$ are called disjoint graphs.

Graphs $G$ and $H$ are isomorphic, written $G \cong H$, if there are bijections $\psi : V(G) \rightarrow V(H)$ and $\theta : E(G) \rightarrow E(H)$ such that a vertex $v$ of $G$ is incident an edge $e$ of $G$ if and only if $\psi(v)$ is incident with $\theta(e)$.

A *walk* $W$ in a graph G is a sequence $v_0e_1v_1e_2....v_{k-1}e_kv_k$ such that $v_0, v_1, ...., v_k$ are vertices and $e_1, e_2...., e_k$ are edges and each vertex or edge in the sequence, except $v_k$, is incident with its successor in the sequence. Now suppose that the vertices $v_0, v_1, ...., v_k$ are distinct, then the edges $e_1, e_2...., e_k$ are also distinct and $W$ is a *path.* The end-vertices of this path are $v_0$ and $v_k$ and the path is said to be a *$(v_0,\, v_k)$-path* or to *join* $v_0$ and $v_k$. The vertices $v_1, ...., v_{k-1}$ are the *internal vertices* of the path. The *length* of a path is the number of edges that it contains.

A graph is *connected* if each pair of distinct vertices is joined by a path. A graph that is not connected is *disconnected.* In any graph $G$, the maximal connected subgraphs are called (connected) *components.* The vertex sets of the components of $G$ partition $V(G)$. The number of these components will be denoted $\omega(G)$.

If $P$ is a $(u, v)$-path in a graph $G$ and $e$ is an edge of $G$ that joins $u$ to $v$ but, is not in $P$, then the subgraph of $G$ whose vertex set is $V(P)$ and whose edge set is $E(P) \cup e$ is called a *cycle.* A connected graph having no cycles is called a *tree*, while a union of trees is called a *forest.* A graph is a forest if and only if it has no cycles. A *spanning tree* of a connected graph $G$ is a subgraph $T$ of $G$ such that $T$ is a tree and $V(T) = V(G)$. For all trees $T$, $|E(T)| = |V(T)| - 1$. Hence if $T$ is a spanning tree of a graph $G$, then $|E(T)| = |V(G)| - 1$

## 3.1 Cycle Matroids

**Proposition 54** *Let $E$ be the set of edges of a graph $G$ and $\mathcal{C}$ be the set of edge sets of cycles of $G$. Then $\mathcal{C}$ is the set of circuits of a matroid on $E$.*

**Proof.** Clearly $\mathcal{C}$ satisfies (C1) and (C2). To prove that it satisfies (C3), let $C_1$ and $C_2$ be the edge sets of two distinct cycles of $G$ that have $e$ as a common edge. Let $u$ and $v$ be the endpoints of $e$. We now construct a cycle of $G$ whose edge set is contained in $(C_1 \cup C_2) - e$. For $i = 1, 2$, let $P_i$ be the path from $u$ to $v$ in $G$ whose edge set is $C_i - e$. Beginning at $u$, traverse $P_1$ towards $v$ letting $w$ be the first vertex at which the next edge of $P_1$ is not in $P_2$. Continue traversing $P_1$ from $w$ towards $v$ until the first time a vertex $x$ is reached that is distinct from $w$ but, also in $P_2$. Since both $P_1$ and $P_2$ end at $v$, such a vertex must exist. Now adjoin the section of $P_1$ from $w$ to $x$ to the section of $P_2$ from $x$ to $w$. The result is a cycle, the edge set of which is contained in $(C_1 \cup C_2) - e$. Hence $\mathcal{C}$ satisfies (C3). ■

**Definition 55** *The matroid derived above from the graph G is called the* ***cycle matroid*** *or* ***polygon matroid****. It is denoted by M(G). Its ground set and set of circuits are denoted by E(M) and $\mathcal{C}$(M) respectively.*

A subset $X$ of $E(G)$ the edges of a graph $G$ is *independent* in $M(G)$ if and only if $X$ does not contain the edge set of a cycle, or equivalently $G[X]$ the subgraph induced by $X$ is a forest. Thus $X$ is a *basis* of $M(G)$ precisely when $G[X]$ is a forest and for all $e \notin X$, $G[X \cup e]$ contains a cycle. It follows that when $G$ is connected that $X$ is a basis of $M(G)$ if and only if $G[X]$ is a spanning tree of $G$. In general, $X$ is a basis of $M(G)$ if and only if, for each component $H$ of $G$ having at least one non-loop edge, $H[X \cap E(H)]$ is a spanning tree of $H$.

Recalling that the *rank* of a matroid is given by the number of elements in a basis (i.e. the number of edges in a spanning forest). Let $M = M(G)$ where $G$ is a connected graph. Then a basis of $G$ is the set of edges of a spanning tree in $G$. For a tree $T$ we have that

$$|E(T)| = |V(G)| - 1.$$

Since $G$ is connected

$$r(M) = |V(G)| - 1.$$

Now if G has $\omega(G)$ connected components, then

$$r(M) = |V(G)| - \omega(G).$$

So, the rank of a cycle matroid is the number of vertices of the graph less the number of connected components of the graph.

It follows that if $X \subseteq E(G)$, then

$$r(X) = |V(G[X])| - \omega(G[X]).$$

**Definition 56** *A matroid that is isomorphic to the cycle matroid of a graph is called* ***graphic****.*

**Proposition 57** *Every graphic matroid is representable over every field. Thus, if G is a graph, then M(G) is representable over every field.*

$G$ is a graph whose vertices are labelled numerically and whose edges are labelled alphabetically. Applying an arrow (whose direction is arbitrarily chosen) to each of the edges, gives a directional graph $D(G)$. Let $M_{D(G)}$ denote the incidence matrix of $D(G)$, that is, $M_{D(G)}$ is the matrix $[m_{ij}]$ whose rows and columns are indexed by the vertices and edges respectively, of $D(G)$ where

$$m_{ij} \leq \begin{cases} 1 & \text{if vertex } i \text{ is the tail of non-loop arc } j; \\ -1 & \text{if vertex } i \text{ is the head of non-loop arc } j; \\ 0 & \text{otherwise.} \end{cases}$$

$M_{D(G)}$ is a matrix over $F_3$ which can be transformed to a matrix $M_{U(G)}$ over $F_2$ by replacing all "$-1$" entries by "1". The proof of Proposition 57 consists of showing that the matroid associated with the matrix $M_{D(G)}$ and also matrix $M_{U(G)}$, is the same as the graphic matroid $M(G)$. So a graphic matroid is representable over $F_2$ and thus over any field. A detailed proof of the proposition is given in [6] pg 139.

**Example 58** *The directed graph D(G) is shown in Figure 2.* $M_{D(G)}$ *the corresponding matrix over* $F_3$ *is given underneath Figure 2.*

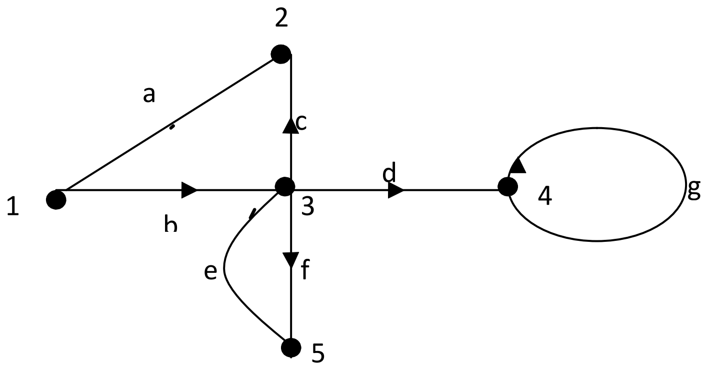


Figure 2

$$M_{D(G)} = \begin{array}{c|ccccccc|} & \mathbf{a} & \mathbf{b} & \mathbf{c} & \mathbf{d} & \mathbf{e} & \mathbf{f} & \mathbf{g} \\ \mathbf{1} & -1 & -1 & 0 & 0 & 0 & 0 & 0 \\ \mathbf{2} & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ \mathbf{3} & 0 & 1 & -1 & -1 & -1 & -1 & 0 \\ \mathbf{4} & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ \mathbf{5} & 0 & 0 & 0 & 0 & 1 & 1 & 0 \end{array}$$

Transforming this to a matrix over $F_2$ gives $M_{U(G)}$ .

$$M_{U(G)} = \begin{array}{c|ccccccc|} & \mathbf{a} & \mathbf{b} & \mathbf{c} & \mathbf{d} & \mathbf{e} & \mathbf{f} & \mathbf{g} \\ \mathbf{1} & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ \mathbf{2} & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ \mathbf{3} & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ \mathbf{4} & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ \mathbf{5} & 0 & 0 & 0 & 0 & 1 & 1 & 0 \end{array}$$

The two matrices $M_{D(G)}$ and $M_{U(G)}$ yield the same matroid.

It is clear from the way in which the matrix is constructed, that it is governed by the relation $r_1 + r_2 + ..... + r_q = 0$ where $r_i$ is the $i^{th}$ row of the matrix. This shows that the n rows are linearly dependent and we can remove any one of the rows without affecting the rank of the matrix or the corresponding vectorial matroid. Since each row corresponds to a vertex of the graph this concurs with the previously attained result regarding the rank of a cycle matroid associated with a connected graph i.e.

$$r(M) = |V(G)| - 1.$$

In fact this equation shows that the remaining $q - 1$ (in this case $5 - 1$) rows of $M_{D(G)}$ and $M_{U(G)}$ are independent, if $G$ is connected.

**Remark 59** *We observe that a circuit of* $G$ *gives a relation between the columns of* $M_{U(G)}$*. The sum of these columns is zero.*

Similarly for a disconnected graph, a matrix is constructed for each of the connected components. A single linearly dependent row can be removed from each of the matrices. Each matrix is then a sub-matrix of the matrix M from which we can regenerate our Matroid $M(G)$.

**Example 60** *If* $G$ *is a disconnected graph consisting of 3 connected components* $G_A$*,* $G_B$ *and* $G_C$ *with corresponding matrices* $A$*,* $B$ *and* $C$*, having* $n$*,* $o$ *and* $p$ *rows respectively, then the rank of the matroid* $M(G)$ *is given by* $(n + o + p) - 3$*.*

$$A = \begin{bmatrix} a_{11} & . & . & a_{1l} \\ . & & & . \\ . & & & . \\ a_{n1} & & & a_{nl} \end{bmatrix} \} n - rows \Rightarrow rank = n - 1.$$

$$B = \begin{bmatrix} b_{11} & . & . & b_{1k} \\ . & & & . \\ . & & & . \\ b_{o1} & . & . & b_{ok} \end{bmatrix} \} o - rows \Rightarrow rank = o - 1.$$

$$C = \begin{bmatrix} c_{11} & . & . & c_{1j} \\ . & & & . \\ . & & & . \\ c_{p1} & . & . & c_{pj} \end{bmatrix} \} p - rows \Rightarrow rank = p - 1.$$

$$M = \begin{bmatrix} a_{11} & . & . & a_{1l} \\ . & & & . \\ . & & & . \\ a_{n-11} & & & a_{n-1l} \\ b_{11} & . & . & b_{1k} \\ . & & & . \\ . & & & . \\ b_{o-11} & . & . & b_{o-1k} \\ c_{11} & . & . & c_{1j} \\ . & & & . \\ . & & & . \\ c_{p-11} & . & . & c_{p-1j} \end{bmatrix} \}(n+o+p)-3 \; rows \Rightarrow rank = (n+o+p)-3$$

## 3.2 Dual of a Graphic Matroid.

If $G$ is a graph, we denote the *dual of the cycle matroid* of $G$ by $M^*(G)$. This matroid is called the *bond matroid* of $G$ or the *cocycle matroid* of $G$. An arbitrary matroid that is isomorphic to the bond matroid of some graph is called *cographic.*

If $X$ is a set of edges in a graph $G$ then, $G \backslash X$ denotes the subgraph of $G$ obtained by deleting all edges in $X$. If $G \backslash X$ has more connected components than $G$, then $X$ is called an *edge cut* of $G$. An edge $e$ for which $\{e\}$ is an edge cut is called a *cut-edge.* A minimal edge cut is also called a *bond* or *cocycle* of $G$..

**Proposition 61** *The following statements are equivalent for a subset $X$ of the set edges of a graph $G$:*

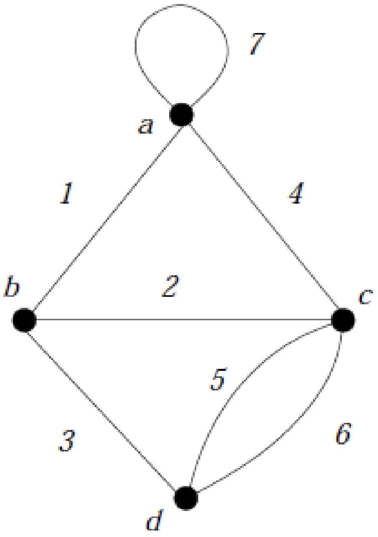
1. *$X$ is a circuit of $M^*(G)$.*

2. *$X$ is a cocircuit of $M(G)$.*

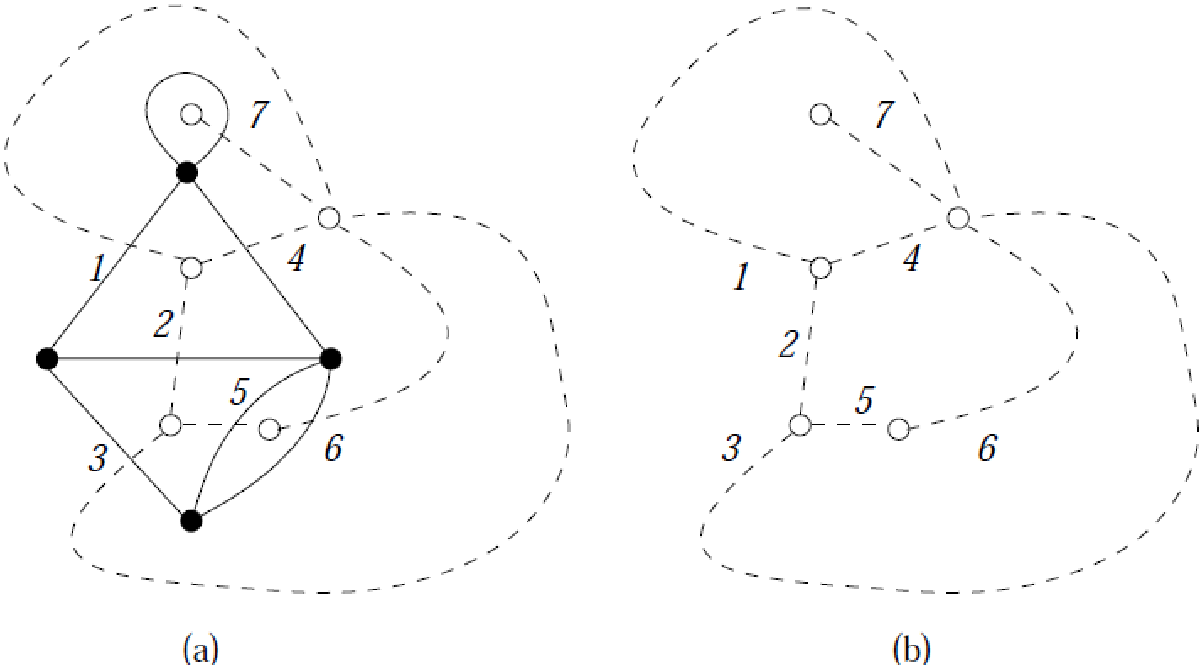
3. *$X$ is a bond of $G$.*

   *See [6] pg 89 for a proof of this proposition.*

For an arbitrary graph $G$, the circuits of $M^*(G)$ are the edge sets of bonds of $G$. If $v$ is a vertex of $G$ and $X$ is the set of edges meeting $v$, then $X$ is an edge cut. If such an $X$ is a minimal edge cut, we call it a *vertex bond* of $G$.



**The graph G** [7].



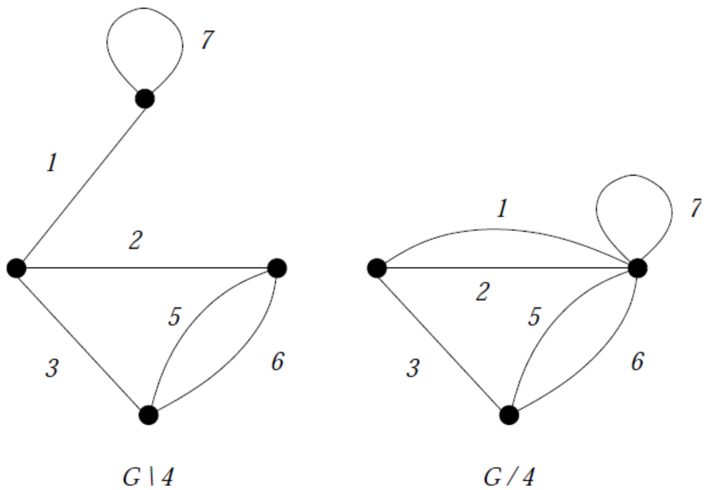
(a) **Constructing the dual $\mathbf{G}^*$ of G** (b) $\mathbf{G}^*$ [7].

## 3.3 Deletion and Contraction

### 3.3.1 Graphs

**Definition 62** *Let $G$ be a graph with edge set $E(G)$ and vertex set $V(G)$. For $e \in E$, we denote the graph obtained from $G$ by* ***deleting*** *$e$ as $G \backslash e$. This action is called* ***edge deletion****. Repeating this process for all the edges in a subset $T$ of $E(G)$ gives the graph $G \backslash T$.*

**Definition 63** *Let $G$ be a graph with edge set $E(G)$ and vertex set $V(G)$. For $e \in E$, we denote the graph obtained from $G$ by* ***contracting*** *$e$ (i.e. identifying the the ends of $e$ with one another and then deleting $e$) as $G/e$. This action is called* ***edge contraction****. Repeating this process for all the edges in a subset $T$ of $E(G)$ gives the graph $G/T$.*



$G \setminus 4$ $\qquad$ $G/4$

**Deletion and Contraction of edge** 4 **of the graph G** [7].

### 3.3.2 Matroids

**Definition 64** *Let $M$ be the matroid $(E, \mathcal{I})$ and suppose that $X \subseteq E$. Let $\mathcal{I}|X$ be $\{I \subseteq X : I \in \mathcal{I}\}$. Then it is easy to see that the pair $(X, \mathcal{I}|X)$ is a matroid. We call this matroid the* ***restriction*** *of $M$ to $X$ or the* ***deletion*** *of $E-X$ from $M$. It is denoted by $M|X$ or $M\backslash(E-X)$.*

**Remark 65** *The circuits of the matroid $M|X$ are given by $\mathcal{C}(M|X) = \{C \subseteq X : C \in \mathcal{C}(M)\}$.*

**Definition 66** *Let $M$ be a matroid on $E$ and $T$ be a subset of $E$. Let $M/T$, the* ***contraction*** *of $T$ from $M$, be given by $M/T = (M^*\backslash T)^*$.*

**Remark 67** *$M/T$ has ground set $E - T$. It is sometimes written as $M.(E - T)$ and called the* ***contraction*** *of $M$ to $E - T$.*

**Remark 68** *If $G$ is a graph and $T \subseteq E(G)$ recall that $G\backslash T$ denotes the graph obtained from $G$ by deleting the edges in $T$. Deletion for matroids extends this graph-theoretic operation, i.e.*

$$M(G\backslash T) = M(G)\backslash T$$

*Similarly for contraction*

$$M(G/T) = M(G)/T$$

**Proof.** See [6] page 111. ■

### 3.3.3 Linear codes

**Definition 69** *Let $C$ be a linear $[n, k, d]$ code over $F_q$. The action of deleting the same coordinate $i$ in each code word is called **puncturing**.*

**Remark 70** *The resulting punctured code is still linear. Its length is $n - 1$ and it is denoted $C^*$. If $G$ is a generator matrix for $C$, then a generator matrix for $C^*$ is obtained from $G$ by deleting column $i$ (and omitting a zero or duplicate row that may occur).*

**Theorem 71** *Let $C$ be a linear $[n, k, d]$ code over $F_q$, and let $C^*$ be the code $C$ punctured on the $i^{th}$ coordinate.*

1. *If $d > 1$, $C^*$ is an $[n - 1, k, d^*]$ code where $d^* = d - 1$ if $C$ has a minimum weight code word with a nonzero $i^{th}$ coordinate and $d^* = d$ otherwise.*

2. *When $d = 1$, $C^*$ is an $[n - 1, k, 1]$ code if $C$ has no code word of weight 1 whose nonzero entry is in coordinate $i$; otherwise, if $k > 1$, $C^*$ is an $[n - 1, k - 1, d^*]$ code with $d^* \geq 1$.*

**Example 72** *Let $C$ be the $[4, 2, 1]$ binary code with generator matrix*

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

*Let $C_1^*$ and $C_4^*$ be the code $C$ punctured on coordinates 1 and 4, respectively. They have generator matrices*

$$G_1^* = \begin{bmatrix} 1 & 1 & 1 \end{bmatrix} \textit{ and } G_4^* = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix}.$$

*So $G_1^*$ is a $[3, 1, 3]$ code and $G_4^*$ is a $[3, 2, 1]$ code.*

**Remark 73** *In general a code $C$ can be punctured on the coordinate set $T$ by deleting components indexed by the set $T$ in all code words of $C$. If $T$ has size $t$, the resulting code denoted $C^T$, is a $[n - t, k^*, \acute{d}^*]$ code with $k^* \geq k - t$ and $d^* \geq d - t$ by Theorem 71 and induction [4].*

**Definition 74** *Let $C$ be a linear $[n,k,d]$ code over $F_q$ and let $T$ be any set of $t$ coordinates. Consider the set $C(T)$ of code words which are $\mathbf{0}$ on $T$; this set is a subcode of $C$. Puncturing $C(T)$ on $T$ gives a code over $F_q$ of length $n-t$ called the code* ***shortened*** *on $T$ and denoted $C_T$.*

**Example 75** *Let $C$ be the $[6,3,2]$ binary code with generator matrix*

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

*$C^{\perp}$ is also a $[6,3,2]$ binary code with generator matrix*

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

*If the coordinates are labeled $1,2,..,6$ let $T = \{5,6\}$. Generator matrices for the shortened code $C_T$ and punctured code $C^T$ are*

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

*and*

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

*Shortening and puncturing the dual code gives the codes $(C^{\perp})_T$ and $(C^{\perp})^T$, which have generator matrices*

$$(G^{\perp})_T = \begin{bmatrix} 1 & 1 & 1 & 1 \end{bmatrix}$$

*and*

$$(G^{\perp})^T = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$$

**Remark 76** *It is clear from the above example that* $(C^{\perp})_T = (C^T)^{\perp}$ *and* $(C^{\perp})^T = (C_T)^{\perp}$*.*

**Remark 77** *If* $C$ *has parity check matrix* $G^{\perp}$*, then it is easy to see that a parity check matrix of the shortened code* $C_T$ *is obtained simply by deleting the corresponding columns of* $G^{\perp}$*.*

**Theorem 78** *Let* $C$ *be a linear* $[n, k, d]$ *code over* $F_q$ *and let* $T$ *be any set of* $t$ *coordinates. Then:*

1. $(C^{\perp})_T = (C^T)^{\perp}$ *and*
2. $(C^{\perp})^T = (C_T)^{\perp}$*, and*
3. *if* $t < d$*, then* $C^T$ *and* $(C^{\perp})_T$ *have dimensions* $k$ *and* $n - t - k$*, respectively.*
4. *if* $t = d$ *and* $T$ *is the set of coordinates where a minimum weight code word is nonzero, then* $C^T$ *and* $(C^{\perp})_T$ *have dimensions* $k - 1$ *and* $n - d - k + 1$*, respectively [4].*

**Proof.** See [4]. ■

**Remark 79** *Let* $C$ *be a linear code with generator matrix* $G$ *(with columns labeled* $1, 2, ..., n$*). The corresponding vectorial matroid obtained from* $G$ *is called* $M_C = M_G(C)$*. If* $C$ *is punctured on coordinate* $i$ *then, the generator matrix for the punctured code is given by deleting column* $i$ *from* $G$*. Since the columns of* $G$ *correspond to the elements* $E_C$ *of the matroid* $M_C$ *then deletion of columns in* $G$ *corresponds to deletion of elements in* $M_C$*.*

**Conclusion 80** *Puncturing a code corresponds to deletion in the associated vectorial matroid* $M_C$*.*

**Remark 81** *From the definition of contraction* $M/T = (M^*\backslash T)^*$*, the relationship between a linear code* $C$ *(with generator matrix* $G$ *and corresponding vectorial matroid* $M_C$*) and contraction can be explained.* $M_C^*$ *is the vectorial matroid corresponding to* $G^{\perp}$*, a parity check matrix. Deletion of* $T$ *from* $M_C^*$*, then corresponds to puncturing* $G^{\perp}$ *at* $T$*, i.e. removing the corresponding columns of* $G^{\perp}$*. So the vectorial matroid obtained from the code which has* $G^{\perp}$ *punctured at* $T$ *as generator matrix, is* $M_C^*\backslash T$*. The code which corresponds to* $(M_C^*\backslash T)^*$ *(the dual of* $M_C^*\backslash T$ *) is the dual of the code which corresponds to* $M_C^*\backslash T$*. It has just been shown that the code corresponding to* $M_C^*\backslash T$ *is the one with* $G^{\perp}$ *punctured at* $T$ *as generator matrix. Hence its dual is one having* $G^{\perp}\backslash T$ *as parity check matrix.*

**Conclusion 82** *If $C$ is linear code with $G^{\perp}$ as a parity check matrix and corresponding vectorial matroid $M_C$, then $M_C/T$ is the matroid corresponding to the code with $G^{\perp}$ minus the columns labeled by $T$ as parity check matrix.*

On the other hand Theorem 78 part 2 says:

$$(C_T)^{\perp} = (C^{\perp})^T$$

which is equivalent to:

$$C_T = ((C^{\perp})^T)^{\perp}$$

Hence we observe that the process of shortening when viewed from a matroid perspective corresponds precisely to contraction:

$$M/T = (M^{*}\backslash T)^{*}$$

**Conclusion 83** $M_C/T = M_{C_T}$.

# Chapter 4

# Demi-Matroids

The contents of this Chapter which precede "An Equivalent Characterisation of a Demi-Matroid" is a more detailed exposition of material from [1] and the definitions are taken from that article.

**Definition 84** *A* ***demi-matroid*** *is a triple $(E, s, t)$ consisting of a finite set $E$ and two functions $s, t : 2^E \to \mathbb{N}_0$, satisfying the following two conditions for all subsets $X \subseteq Y \subseteq E$ :*

***(R)*** $0 \leq s(X) \leq s(Y) \leq |Y|$ *and* $0 \leq t(X) \leq t(Y) \leq |Y|$ :

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

**Proposition 85** *If $M = (E, r)$ is a matroid with rank $r$, then, the triple $(E, r, r^*)$ where $r^*$ is the corank of $M$ is a demi-matroid.*

**Proof.** From the definition of a rank function $r$ and its dual $r^*$, **(R)** is satisfied trivially by simply equating $r$ and $r^*$ with $s$ and $t$ respectively. Let us 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 the same as

$t(X) = t(E) - |E - X| + s(E - X)\ (*)$

We know that

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

Substituting $s$ and $t$ for $r$ and $r^*$

$t(X) = |X| - s(M) + s(E - X)\ (**)$

Hence it is enough to prove that $(*)$ and $(**)$ is the same identity. This is true if

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

which in turn is true iff

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

But this holds since setting $X = \emptyset$ in **(D)** we obtain:

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

By **(R)** we have

$0 \leq t(\emptyset) \leq |\emptyset| = 0$, so $t(\emptyset) = 0$.

Hence

$t(E) = |E| - s(E)$ as desired. ■

**Remark 86** *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

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

Thus

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

or equivalently

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

Now setting $X = E - X$ in **(D)** gives

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

Adding $|E - X| + s(E)$ to both sides yields

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

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

Which gives our desired result:

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

So **(D)** $\Rightarrow$ **(D')** and by a similar argument **(D)** $\Leftarrow$ **(D'),** so **(D)** $\Leftrightarrow$ **(D').** ■

**Remark 87** *Inspired by the previous argument, we observe 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 $X = \emptyset$ :*

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

*so*

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

*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 dependent on $s$. This expression may be called $s^*$.*

**Definition 88** *$(s^*)^* = s$.*

**Proof.** The proof that $(s^*)^* = s$ is the same as for matroids.

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

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

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

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

$= s(X)$. ■

**Remark 89** *Conversely to proposition 85, 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 90** *Suppose that $E = \{a, b\}$ and define $s(X) := 0$ for $X = \emptyset, \{a\}, \{b\}$, and $s(E) := 1$. The triple $(E, s, t)$ is a demi-matroid but, $s$ is not the rank function of any matroid on $E$. In this case $t = s$ as the following simple calculation shows:*

$t(\{a\}) = |\{a\}| - s(E) + s(\{b\}) = 1 - 1 + 0 = 0.$

$t(\{b\}) = |\{b\}| - s(E) + s(\{a\}) = 1 - 1 + 0 = 0.$

$t(\{a, b\}) = |\{a, b\}| - s(E) + s(\{\emptyset\}) = 2 - 1 + 0 = 1.$

*It is clear that axiom R3 (which is a requirement for the rank function of a matroid) fails and thus $s$ is not a rank function of a matroid.*

*If $X$ and $Y$ are subsets of $E$, then $r(X \cup Y) + r(X \cap Y) \leq r(X) + r(Y)$.*

*Taking $a = X$ and $b = Y$ and rank function $s$ we get*

$s(a \cup b) + s(a \cap b) \leq s(a) + s(b)$

$s(E) + s(\emptyset) \leq s(a) + s(b)$ *but,*

$1 + 0 \nleq 0 + 0.$

**Definition 91** *The* ***dual demi-matroid*** $D = (E, r, r^*)$ *arising from the matroid* $M = (E, r)$ *is given by the demi-matroid* $D^* = (E, r^*, r)$ *which corresponds to the dual matroid* $M^* = (E, r^*)$*. In general for the demi-matroid* $D = (E, s, t)$ *the dual demi-matroid is given by* $D^* = (E, t, s)$ *and* $D = (D^*)^*$*.*

A second type of demi-matroid duality is obtained from the following involution:

**Definition 92** *For any real function* $f : 2^E \to \mathbb{R}$*, let* $\overline{f}$ *denote the function given by*

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

**Remark 93** *Since* $\overline{\overline{f}}(X) := \overline{f}(E) - \overline{f}(E - X) = f(E) - f(\emptyset) - f(E) + f(X) = f(X) - f(\emptyset)$*, it follows that if* $f(\emptyset) = 0$*, then the operation* $f \to \overline{f}$ *is an involution, i.e.* $f = \overline{\overline{f}}$*.*

**Theorem 94** *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, first note that $\overline{s}(\emptyset) = \overline{t}(\emptyset) = 0$ and that $\overline{s}(E) = s(E)$ and $\overline{t}(E) = t(E)$. Consider subsets $X \subseteq Y \subseteq E$. By **(R)** and **(D')**,

$E - Y \subseteq E - X$

$s(E - Y) \leq s(E - X)$

$-s(E - Y) \geq -s(E - X)$

$s(E) - s(E - Y) \geq s(E) - s(E - X)$

$s(E) - s(E - X) \leq s(E) - s(E - Y)$

but from (D')

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

$|X| - t(X) = s(E) - s(E - X) \Rightarrow |Y| - t(Y) = s(E) - s(E - Y)$

which gives

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

so $0 \leq \overline{s}(X) \leq \overline{s}(Y) \leq |Y|$. Similarly, it is easy to show that $0 \leq \overline{t}(X) \leq \overline{t}(Y) \leq |Y|$, so $\overline{D}$ satisfies **(R)**.

By **(D')**,

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

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

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

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

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

**Remark 95** *It has already been shown that $f = \overline{\overline{f}}$, similarly, $s = \overline{\overline{s}}$ and $t = \overline{\overline{t}}$. Thus we see that $D = (E, s, t) = (E, \overline{\overline{s}}, \overline{\overline{t}}) = \overline{\overline{D}}$.*

**Remark 96** *Note also $\overline{D^*} = \overline{(E, t, s)} = (E, \overline{t}, \overline{s}) = (E, \overline{s}, \overline{t})^* = (\overline{D})^*$.*

**Remark 97** *The supplement operation does not generally apply to matroids as the following example illustrates.*

**Example 98** *Consider the matroid $M := (E, \rho)$ where $E = \{a, b, c\}$ and $\rho(X) = 0$ for $X = \emptyset, \{a\}$ and $\rho(X) = 1$ for all other subsets $X \subseteq E$. Then $D := (E, \rho, \rho^*)$ is a demi-matroid, so $\overline{D} := (E, \overline{\rho}, \overline{\rho^*})$ is also a demi-matroid. However $(E, \overline{\rho})$ is not a matroid, since it would have rank 1 but, only contain loops i.e.*

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

$\overline{\rho}(a) = \rho(E) - \rho(\{b, c\}) = 1 - 1 = 0 \Rightarrow a$ *is a loop.*

$\overline{\rho}(b) = \rho(E) - \rho(\{a, c\}) = 1 - 1 = 0 \Rightarrow b$ *is a loop.*

$\overline{\rho}(c) = \rho(E) - \rho(\{a, b\}) = 1 - 1 = 0 \Rightarrow c$ *is a loop.*

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

*But it is impossible to have a matroid comprising of loops with rank greater than 0. Thus $(E, \overline{\rho})$ is not a matroid.*

*It is easy to see that $(E, \rho)$ is a graphical matroid consisting of a loop ($\{a\}$) and a set of parallel edges ($\{b, c\}$). It can also be verified by checking the rank axioms $R1 - R3$ are satisfied (which they are).*

## 4.1 Invariants of Demi-Matroids

**Lemma 99** *$s(X-x) \geq s(X)-1$ and $t(X-x) \geq t(X)-1$ for all $X \subseteq E$ and $x \in E$.*

**Proof.** By **(R)** and **(D)**,

$$\begin{aligned} t(X-x) &= t(E) - |E-(X-x)| + s(E-(X-x)) \\ &\geq t(E) - |E-X| - 1 + s(E-X) \\ &= t(X) - 1. \quad \blacksquare \end{aligned}$$

**Definition 100** *Define for all $i = 0, ..., k$ and $j = 0, ..., n-k$,*

$\sigma_i := \min\{|X| : X \subseteq E, s(X) \geq i\}$;

$\tau_j := \min\{|X| : X \subseteq E, t(X) \geq j\}$;

$s_i := \max\{|X| : X \subseteq E, s(X) \leq i\}$;

$t_j := \max\{|X| : X \subseteq E, t(X) \leq j\}$.

**Example 101** *If we consider the graphical matroid $M(G)$ of Figure 1. The Demi-matroid arising from this matroid has the following values for $\sigma_i, \tau_j, s_i, t_j$:*

*$k = s(E) = 3$ and $n - k = 5 - 3 = 2$.*

$\sigma_0 = |\emptyset| = 0$.

$\sigma_1 = |\{e_1\}| = |\{e_2\}| = |\{e_3\}| = |\{e_4\}| = 1$.

$\sigma_2 = |\{e_1, e_2\}| = |\{e_1, e_3\}| = |\{e_1, e_4\}| = |\{e_2, e_4\}| = |\{e_3, e_4\}| = 2$.

$\sigma_3 = |\{e_1, e_2, e_4\}| = |\{e_1, e_3, e_4\}| = 3$.

*By constructing the graph of the dual $M^*(G)$ (shown in Figure 3) we can easily determine the values of $\tau_i$. The following information may be useful in the construction and in clarifying the relationship between independent sets and both $\sigma_i$ and $\tau_j$. $E = \{e_1, e_2, e_{3,}e_4, e_5\}$, $\mathcal{B} = \{\{e_1, e_2, e_4\}\{e_1, e_3, e_4\}\} \Rightarrow \mathcal{B}^* = \{\{e_3, e_5\}, \{e_2, e_5\}\} \Rightarrow \{e_2\}, \{e_3\}, \{e_5\} \in \mathcal{I}$*

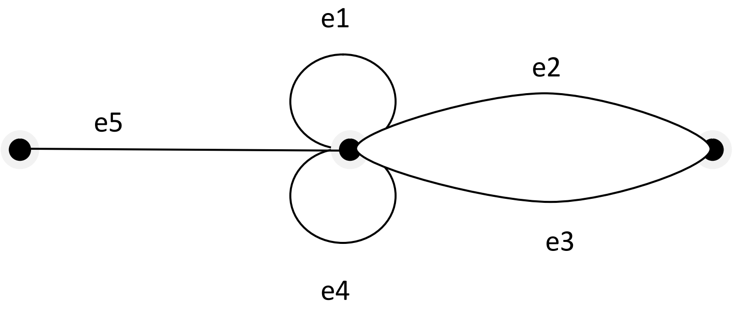


*Figure 3*

$\tau_0 = |\emptyset| = 0.$

$\tau_1 = |\{e_2\}| = |\{e_3\}| = |\{e_5\}| = 1.$

$\tau_2 = |\{e_2, e_5\}| = |\{e_3, e_5\}| = 2.$

$s_0 = (\textit{number of loops}) = |\{e_5\}| = 1.$

$s_1 = (\textit{number of loops}) + (\textit{max. number of parallel elements}) = |\{e_5\}| + |\{e_2, e_3\}| = 3.$

$s_2 = |\{e_2, e_3, e_4, e_5\}| = |\{e_1, e_2, e_3, e_5\}| = 4.$

$s_3 = |E| = 5.$

$t_0 = (\textit{number of loops}) = |\{e_1, e_4\}| = 2.$

$t_1 = (\textit{number of loops}) + (\textit{max. num. of parallel elements}) = |\{e_1, e_4\}| + |\{e_2, e_3\}| = 4.$

$t_2 = |E| = 5.$

**Remark 102** *Considering the case for invariants of a demi-matroid which is not a matroid, it can be seen that it is not necessarily true that $\sigma_i = i$ or that $\tau_j = j$.*

**Example 103** *Revisiting example 90 and using results obtained there:*

*$E = \{a, b\}$ and $s(X) := 0$ for $X = \emptyset, \{a\}, \{b\}$, and $s(E) := 1.$*

$k = 1$

$\sigma_0 = |\emptyset| = 0.$

$\sigma_1 = |\{a, b\}| = 2.$

*Using the results obtained for $t(X)$ in example 90 we get:*

$\tau_0 = |\emptyset| = 0.$

$\tau_1 = |\{a, b\}| = 2.$

*Thus we see that neither $\sigma_i = i$ nor $\tau_j = j$ for all respective $i$ and $j$.*

By **(R)** and Lemma 99, all of the numbers $\sigma_i, \tau_j, s_i$ and $t_j$ are well defined and may be given the following equivalent characterisations:

**Lemma 104** *For all $i = 0, ..., k$ and $j = 0, ..., n-k$,*

$\sigma_i = \min\{|X| : X \subseteq E, s(X) = i\}$;

$\tau_j = \min\{|X| : X \subseteq E, t(X) = j\}$;

$s_i = \max\{|X| : X \subseteq E, s(X) = i\}$;

$t_j = \max\{|X| : X \subseteq E, t(X) = j\}$.

**Proof.** Let $U$ be one of the subsets $X$ which satisfies

$\sigma_i = \min\{|X| : X \subseteq E, s(X) \geq i\}$ so $s(U) \geq i$.

Now if $s(U) \geq i+1$:

Let $V = U - \{a\}$ where $a \in U$.

$s(V) \geq s(U) - 1 \geq (i+1) - 1 = i$, by Lemma 99

But, since $|V| < |U|$ and $|U| = \min\{|X| : X \subseteq E, s(X) \geq i\}$

this is a contradiction

$\Rightarrow s(U) \not> i$

$\Rightarrow s(U) = i$. A similar argument holds for $\tau_j$.

For $s_i$ we have the following:

Let $U$ be one of the subsets $X$ which satisfies

$s_i = \max\{|X| : X \subseteq E, s(X) \leq i\}$.

Now if $s(U) \leq i - 1$:

Let $V = U + \{a\}$ where $a \in (E - U)$.

$s(V) \leq s(U) + 1 \leq (i-1) + 1 = i$, by Lemma 99

But, since $|U| < |V|$ and $|U| = \max\{|X| : X \subseteq E, s(X) \leq i\}$

this is a contradiction

$\Rightarrow s(U) \not< i$

$\Rightarrow s(U) = i$. A similar argument holds for $t_j$. ■

**Remark 105** *If $M$ is a matroid on $E$ with rank function $\rho$, then the coefficients $\sigma_i$ and $\tau_j$ for the demi-matroid $D := (E, \rho, \rho^*)$ are trivial: $\sigma_i = i$ and $\tau_j = j$ for all $i, j$.*

**Proof.** Let $M = (E, \rho)$ be a matroid. Then for any subset $X \subseteq E$, $\rho(X) = i \Rightarrow |X| \geq i$. So if $|X| = i$ with $\rho(X) = i$, then $X \in \{X | \min\{|X| : X \subseteq E, s(X) \geq i\}\}$. But, the subsets which satisfy this criterion are exactly those $X \in \mathcal{I}$ such that $|X| = i$. Thus $\sigma_k = \dim(B) = k$ where $B \in \mathcal{B}$. Similarly $\sigma_{k-1} = \dim(B - \{a\}) = k - 1$ where $a \in B$ and it follows that $\sigma_i = i$. By a similar argument $\tau_j = j$. ■

**Lemma 106** *The following inequalities hold:*

$0 = \sigma_0 < \sigma_1 < \sigma_2 < \cdot\cdot\cdot\cdot < \sigma_k \leq n;$

$0 = \tau_0 < \tau_1 < \tau_2 < \cdot\cdot\cdot\cdot < \tau_{n-k} \leq n.$

**Proof.** For each $i = 1, ...., k$, let $X \subseteq E$ be a subset such that $|X| = \sigma_i$ and $s(X) \geq i$. By Lemma 99, $s(X - x) \geq i - 1$ for any $x \in X$, so $\sigma_{i-1} \leq |X - x| \leq \sigma_i$. Similarly, $\tau_{j-1} < \tau_j$ for each $j = 1, ....., n - k$. ■

**Lemma 107** *The following inequalities hold:*

$0 \leq s_0 < s_1 < s_2 < \cdot\cdot\cdot\cdot < s_k \leq n;$

$0 \leq t_0 < t_1 < t_2 < \cdot\cdot\cdot\cdot < t_{n-k} \leq n.$

**Proof.** For each $i = 1, ...., k$, let $X \subseteq E$ be a subset such that $|X| = s_i$ and $s(X) \leq i$. Let $a \in (E - X)$, then by Lemma 99, $s(X \cup \{a\}) \leq s(X) + 1 \leq i + 1$

which gives $|X \cup \{a\}| \leq s_{i+1}$ but, since $|X \cup \{a\}| = s_i + 1$ we have that $s_i + 1 \leq s_{i+1} \Rightarrow s_i < s_{i+1}$. Similarly, $t_j < t_{j+1}$ for each $j = 1, ....., n - k$. ■

The four above monotonicities each induce a generalized Singleton-type bound for demi-matroids:

**Corollary 108** *For all $i = 0, ..., k$ and $j = 0, ..., n - k$,*

$\sigma_i \leq n - k + i;$

$s_i \leq n - k + i;$

$\tau_j \leq k + j;$

$t_j \leq k + j.$

**Proof.** From Lemma 106 we have that

$0 = \sigma_0 < \sigma_1 < \sigma_2 < \cdot\cdot\cdot\cdot < \sigma_k \leq n$. Thus

$\sigma_k \leq n$

$\sigma_{k-1} \leq n-1$

$\sigma_{k-2} \leq n-2$

.

.

$\sigma_{k-a} \leq n-a$

Now letting $i = k-a$ we get:

$\sigma_i \leq n-k+i.$

A similar proof yields $\tau_j \leq k+j$. Considering Lemma 107 and applying a similar logic as in the above proof

$s_i \leq n-k+i$ and

$t_j \leq k+j$ are obtained. ■

**Notation 109** *Let the invariants $\overline{\sigma}_i$, $\overline{\tau}_j$ be defined by $\overline{s}$ and $\overline{t}$ in the same way as $\sigma_i$ and $\tau_j$ are defined from $s$ and $t$.*

**Lemma 110** *For each $i = 0, ..., k$ and $j = 0, ..., n-k$,*

$s_i = n - \overline{\sigma}_{k-i};$

$\sigma_i = n - \overline{s}_{k-i};$

$t_j = n - \overline{\tau}_{n-k-j};$

$\tau_j = n - \overline{t}_{n-k-j}.$

**Proof.** $t_j = \max\{|X| : X \subseteq E, t(X) = j\}$

$= \max\{|E-X| : X \subseteq E, t(E-X) = j\}$

$= n - \min\{|X| : X \subseteq E, t(E-X) = j\}$

$= n - \min\{|X| : X \subseteq E, \overline{t}(X) = n-k-j\}$ from $\overline{t}(X) = t(E) - t(E-X) = n-k-j$

$t_j = n - \overline{\tau}_{n-k-j}.$

Now if we observe that

$t_j = n - \overline{\tau}_{(n-k)-j}$

is the same as

$t_j = n - \overline{\tau}_{t(E)-j}$

Then we can obtain an analogous result for $s_i$

$s_i = n - \overline{\sigma}_{s(E)-i}$

$s_i = n - \overline{\sigma}_{k-i}$

Now since $\overline{s}(E) = s(E)$ we get

$\overline{s}_i = n - \overline{\overline{\sigma}}_{\overline{s}(E)-i} = n - \sigma_{k-i}$

$\sigma_{k-i} = n - \overline{s}_i \Rightarrow$

$\sigma_i = n - \overline{s}_{k-i}$

Now since $\overline{t}(E) = t(E)$ we get

$\overline{t}_j = n - \overline{\overline{\tau}}_{\overline{t}(E)-j} = n - \tau_{n-k-j}$

$\tau_{n-k-j} = n - \overline{t}_j \Rightarrow$

$\tau_j = n - \overline{t}_{n-k-j}$ ■

**Definition 111** *For each demi-matroid D, set*

$S_D := \{n - s_{k-1}, ..., n - s_1, n - s_0\}$;

$T_D := \{t_0 + 1, t_1 + 1, ..., t_{n-k-1} + 1\}$;

$U_D := \{\sigma_1, \sigma_2, ..., \sigma_k\}$;

$V_D := \{n + 1 - \tau_{n-k}, ..., n + 1 - \tau_2, n + 1 - \tau_1\}$.

Lemma 110 implies the following identities:

**Lemma 112** $S_D = U_{\overline{D}}$ *and* $T_D = V_{\overline{D}}$.

The following two fundamental duality theorems for demi-matroids generalize Wei's Duality Theorem.

**Theorem 113** $U_D \cup V_D = \{1, ..., n\}$ *and* $U_D \cap V_D = \emptyset$.

**Proof.** Assume that there are integers $i$, $j$ such that $\sigma_i = n + 1 - \tau_j$. Let $X \subseteq E$ be a subset satisfying $|X| = \tau_j$ and $t(X) \geq j$. Then $|E - X| = \sigma_i - 1$, so $s(E - X) \leq i - 1$ from Lemma 106. By **(D)**,

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

$= n - \tau_j - (n - k) + j$

$= -\tau_j + k + j \leq i - 1$ (**i**)

Similarly, $n - \sigma_i - k + i \leq j - 1$ (**ii**)

Combining (**i**) and (**ii**) gives

$-1 = n - \sigma_i - \tau_j \leq -2$, a contradiction.

This proves $U_D \cap V_D = \emptyset$.

Now $\sigma_i \geq i$ and $\tau_j \geq j$ gives $U_D \subseteq \{1, ...., n\}$ and $V_D \subseteq \{1, ...., n\}$ with $|U_D| = k$ and $|V_D| = n - k$. Since $U_D \cap V_D = \emptyset$ then, $|U_D \cup V_D| = n$ and $U_D \cup V_D = \{1, ...., n\}$. ■

**Theorem 114** *$S_D \cup T_D = \{1, ..., n\}$ and $S_D \cap T_D = \emptyset$.*

**Proof.** From Theorem 113 $U_D \cup V_D = \{1, ..., n\}$ and $U_D \cap V_D = \emptyset$ but, since this is true for all demi-matroids, it is also true for $\overline{D}$ thus, $U_{\overline{D}} \cup V_{\overline{D}} = \{1, ..., n\}$ and $U_{\overline{D}} \cap V_{\overline{D}} = \emptyset$. Applying Lemma 112 gives $S_D \cup T_D = \{1, ..., n\}$ and $S_D \cap T_D = \emptyset$. ■

## 4.2 An Equivalent Characterisation of a Demi-Matroid

The material in this subsection is not explicitly contained in [1].

A demi-matroid has previously been defined in Definition 84. This will now be used in conjunction with Lemma 99 to show that a demi-matroid is characterised by the following definition:

**Definition 115** *A **demi-matroid** is a triple $(E, s, t)$ consisting of a finite set $E$ and two functions $s, t : 2^E \to \mathbb{N}_0$, satisfying the following two conditions:*

***(R")*** *$s(\emptyset) = 0$ and $s(X) \leq s(X \cup \{e\}) \leq s(X) + 1$ for all $X \subseteq E$ and $e \in E$*

***(D")*** *$t(X) = |X| - s(E) + s(E - X)$ for all $X \subseteq E$.*

A proof showing the equivalence of Definition 84 and Definition 115 is now given:

**Proof.** (**i**) From (**D**) we have $t(X) = t(E) + s(E - X) - |E - X|$. From the proof of Proposition 85 we have that $t(E) = |E| - s(E)$. So we can write

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

$\quad = |X| - s(E) + s(E - X)$.

So (**D"**) holds.

(**ii**) Assume both (**R**) and (**D**) hold:

Let $X = Y = \emptyset$.

Thus $0 \leq s(\emptyset) \leq s(\emptyset) \leq |\emptyset| = 0$

$\Rightarrow s(\emptyset) = 0$.

Now if we set $X = X$ and $Y = X \cup \{e\}$ then from **(R)** we get $s(X) \leq s(X \cup \{e\})$.

Lemma 99 gives:

$s(A - \{e\}) \geq s(A) - 1$ for all $A \subseteq E$, and $e \in E$.

Let $X \subseteq E$ and $e \in E$. Let $A \overset{def}{=} X \cup \{e\}$.

So $A - \{e\} = (X \cup \{e\}) - \{e\} = \begin{cases} X & \text{if } e \notin X \\ X - \{e\} & \text{if } e \in X. \end{cases}$

We now prove **(R")**: $s(X \cup \{e\}) \leq s(X) + 1$.

If $e \in X$ then this is trivial since we get $s(X) \leq s(X) + 1$. So we only consider the case where $e \notin X$ and thus $A - \{e\} = X$.

Returning now to Lemma 99 which states: $s(A - \{e\}) \geq s(A) - 1$ we get the following:

$s(X) \geq s(X \cup \{e\}) - 1$ which in turn gives:

$s(X \cup \{e\}) \leq s(X) + 1$.

This shows that **(R")** holds.

**(iii)** Assume **(R")** and **(D")** hold:

From **(R")** we have that $s(\emptyset) = 0$

**(D")** gives:

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

and

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

Hence

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

and we obtain:

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

Thus **(D)** holds.

**(iv)** Assume **(R")** and **(D")** hold:

Let $X \subseteq Y \subseteq E$ and $Y - X = \{y_1, y_2, ..., y_n\}$

Now $s(X) \leq s(X \cup \{y_1\}) \leq s(X \cup \{y_1\} \cup \{y_2\}) \leq \cdots\cdots \leq s(X \cup \{y_1\} \cup \{y_2\} \cup \cdots \cup \{y_n\}) = s(Y)$.

If $Y = \{w_1, w_2, ..., w_{|Y|}\}$ then we have:

$s(\{w_1\}) \leq s(\emptyset) + 1.$

$s(\{w_1\} \cup \{w_2\}) \leq s(\{w_1\}) + 1 \leq (s(\emptyset) + 1) + 1 = s(\emptyset) + 2.$

.

.

.

$s(\{w_1\} \cup \cdot\cdot \cup \{w_{|Y|}\}) \leq s(\{w_1\} \cup \cdot\cdot \cup \{w_{|Y|-1}\}) + 1 \leq (s(\emptyset) + |Y - 1|) + 1 = s(\emptyset) + |Y| = |Y|.$

So $s(Y) \leq |Y|$.

Finally

$\emptyset \subseteq X$

so

$0 = s(\emptyset) \leq s(X)$

and **(R)** holds. ■

# Chapter 5

# Higher Weights of Linear Codes

We start this chapter by giving some standard definitions and results about higher support weights.

**Remark 116** *The* ***minimum distance*** $d$ ***of a linear code*** $C$ *was earlier defined as* $\min w(x)$, $x \neq 0$, $x \in C$ *(smallest of the weights of the non-zero code words).*

**Definition 117** *The* ***support*** *of a code word* $x$ *is defined as* $Supp(x) = \{i \in \{1, .., n\} | x_i \neq 0\}$.

**Proposition 118** $w(x) = |Supp(x)|$.

**Example 119** *If* $x = (0, 2, 1, 0, 4) \in C \subseteq (F_7)^5$ *then* $Supp(x) = \{2, 3, 4\}$ *and we see that* $w(x) = |Supp(x)| = 3$.

**Definition 120** *Let* $M \subseteq C$ *then* $Supp(M) = \underset{x \in M}{\cup} Supp(x)$ *and* $w(M) = |Supp(M)|$. *We have* $0 \leq w(M) \leq n$, *where* $n$ *is the code word length.*

**Example 121** *If* $M = \{(0, 2, 1, 0, 4), (0, 0, 0, 2, 6)\}$ *then* $Supp(M) = \{2, 3, 5\} \cup \{4, 5\} = \{2, 3, 4, 5\}$ *and* $w(M) = |Supp(M)| = 4$. *And* $0 \leq w(M) \leq 5 = n$.

**Remark 122** *If* $C \subseteq (F_q)^n$ *and* $L$ *is the one dimensional subspace of* $C$ *given by* $L = \{kx | k \in F_q\}$ *for* $x \in C$, *then* $Supp(L) = Supp(x)$ *and* $w(L) = w(x)$.

**Example 123** *If* $x = (0, 2, 1, 0, 4)$ *then* $kx = (0, 2k, k, 0, 4k)$ *and* $Supp(L) = Supp(x) = \{2, 3, 5\}$ *and* $w(L) = w(x) = 3$.

**Remark 124** *The minimum distance $d$ is then given by* $\min\{w(L)|L \subseteq C, \dim(L) = 1\}$.

**Definition 125** *The $i^{th}$* ***generalized Hamming weight*** *of $C$ is $d_i(C) \overset{def}{=} \min\{|Supp(L)| : L \subseteq C, \dim(L) = i\}$.*

**Remark 126** *For a code $C$, $d(C) = d_1$.*

**Theorem 127** *For an $[n, k]$ linear code $C$ with $k > 0$ we have $1 \leq d_1(C) < d_2(C) < \cdots < d_k(C) \leq n$.*

**Proof.** That $d_{i-1}(C) \leq d_i(C)$ is trivial; it remains to prove that strict inequalities hold. Let $D \subseteq C$ with $|Supp(D)| = d_i(C)$ and $\dim(D) = i$. Let $j \in Supp(D)$ and $D_j := \{x \in D : x_j = 0\}$. Thus $Supp(D_j)$ is obtained by removing $j$ from $Supp(D)$. Then $\dim(D_j) = i - 1$ and $d_{i-1}(C) \leq |Supp(D_j)| \leq |Supp(D)| - 1 = d_i(C) - 1$. ■

**Corollary 128** *For an $[n, k]$ linear code $C$, $d_i(C) \leq n - k + i$, for all $i = 1, 2, ...., k$. (When $i = 1$ this is the* ***Singleton bound****).*

Now we give our own proof of the following result, given in [8]. Let $C$ be a q-ary $[n, k, d]$ code, and $H$ a parity check matrix for $C$. For any $I \subseteq \{1, 2, .., n\}$ let $M(I) = \langle H_i : i \in I\rangle$ be the submatrix of $H$, consisting of the columns $H_i$, where $i \in I$.

**Theorem 129** *$d_r(C) = \min\{|I| : |I| - rank(M(I)) \geq r\}$ where $I \subset \{1, 2, .., n\}$.*

**Proof.** For any $I \subset \{1, 2, .., n\}$, let $S(I)$ be the column space spanned by $\{H_i : i \in I\}$, where $H_i$ is column number $i$ of $H$, so $S(I)$ is the column space of $M(I)$. Let $S^{\perp}(I) := \{\mathbf{x} : x_i = 0$ for $i \notin I$, and $\sum\limits_{i \in I} x_i H_i = 0\}$. By the Dimension Theorem for Linear Transformations we have that $rank(M(I)) + nullity(M(I)) = |I|$, or equivalently $\dim(\mathrm{col}(M(I))) + \dim(\ker(M(I))) = |I| \Rightarrow \dim(S(I)) + \dim(S^{\perp}(I)) = |I|$.

Let $d = \min\{|I| : |I| - rank(M(I)) \geq r\}$. But we have $\min\{|I| : |I| - rank(M(I)) \geq r\} = \min\{|I| : |I| - rank(M(I)) = r\}$. This follows from Proposition 130 below in addition to Lemma 104. Let $I \subset \{1, 2, .., n\}$ be such that $|I| - \dim(S(I) = r$, and $|I| = d$. Then $\dim(S^{\perp}(I)) = r$, and $S^{\perp}(I)$ is a subcode of $C$, and $d_r(C) \leq |Supp(S^{\perp}(I))| = |I| = d$. So $d_r(C) \leq \min\{|I| : |I| - rank(M(I)) \geq r\}$. The inequality in the other direction remains to be established. Let $D \subset C$ with $\dim(D) = r$ and $|Supp(D)| = d_r(C)$. Let $I = Supp(D)$, the $D \subset S^{\perp}(I\dot{)}$. Given $d_r(C)$, we choose $I$ such that$|I| = |Supp(D)| = d_{r'}(C)$ and $\dim(S(I)) \geq r$ but, this entails that $d$, which is the smallest cardinality to an $I$ such that $|I| - \dim(S(I)) \geq r$ is less than or equal to the $I$ we have initially chosen i.e. $d \leq d_r(C)$. ■

Let $(E, s, t)$ be the demi-matroid derived from the matroid $M_C = (E, s)$ where $E = \{1, 2, ...., n\}$ and $s$ is the rank function of the matroid. Recall Definition 100 and Notation 109 for $\overline{\sigma}_r$ and $\overline{\tau}_r$. This motivates the two next propositions, which are taken from [1] and which we prove in detail here.

**Proposition 130** $d_r = \overline{\sigma}_r$.

**Proof.** Let the generator and parity check matrices corresponding to $M_C$ be $G$ and $H$ respectively.

Applying Theorem 129 to the demi-matroid $(E, s, t)$ we get:

$$\begin{aligned} d_r(C) &= \min\{|X| : |X| - rank(M(X)) \geq r\} \\ &= \min\{|X| : |X| - t(X) \geq r\} \\ &= \min\{|X| : s(E) - s(E - X) \geq r\} \\ &= \min\{|X| : \overline{s}(X) \geq r\} \\ &= \overline{\sigma}_r. \end{aligned}$$ ■

**Definition 131** $d_{r^{\perp}} \overset{def}{=} d_r(C^{\perp})$

**Proposition 132** $d_{r^{\perp}} = \overline{\tau}_r$.

**Proof.** Let $(E, s, t)$ be the demi-matroid derived from the matroid $M_C = (E, s)$ where $E = \{1, 2, ...., n\}$ and $s$ is the rank function of the matroid. Let the generator and parity check matrices corresponding to $M_C$ be $G$ and $H$ respectively. Let $N(I) = \langle G_i : i \in I \rangle$ be the submatrix of $G$, consisting of the columns $G_i$, where $i \in I$

Applying Theorem 129 to the demi-matroid $(E, s, t)$ we get:

$$\begin{aligned} d_{r^{\perp}} = d_r(C^{\perp}) &= \min\{|X| : |X| - rank(N(X)) \geq r\} \\ &= \min\{|X| : |X| - s(X) \geq r\} \\ &= \min\{|X| : t(E) - t(E - X) \geq r\} \\ &= \min\{|X| : \overline{t}(X) \geq r\} \end{aligned}$$

$= \overline{\tau}_r$. ■

**Theorem 133** *Let $C$ be a $[n, k]$ code. Then $\{d_r(C) : 1 \leq r \leq k\} \cup \{n+1-d_{r^\perp} : 1 \leq r \leq n-k\} = \{1, 2, ...., n\}$.*

**Theorem 134** *Let $C$ be a $[n, k]$ code. Then $\{d_r(C) : 1 \leq r \leq k\} \cap \{n+1-d_{r^\perp} : 1 \leq r \leq n-k\} = \emptyset$.*

**Proof.** It has been shown that $d_r = \overline{\sigma}_r$ and $d_{r^\perp} = \overline{\tau}_r$. Thus $\{d_r : 1 \leq r \leq k\} = \{\overline{\sigma}_r : 1 \leq r \leq k\} = U_{\overline{D}} = S_D$ by Lemma 112, and $\{n+1-d_{r^\perp} : 1 \leq r \leq n-k\} = \{n+1-\overline{\tau}_r : 1 \leq r \leq n-k\} = V_{\overline{D}} = T_D$ by Lemma 112. Furthermore by Theorem 114, $S_D \cup T_D = \{1, ..., n\}$ and $S_D \cap T_D = \emptyset$, so $\{d_r(C) : 1 \leq r \leq k\} \cup \{n+1-d_{r^\perp} : 1 \leq r \leq n-k\} = \{1, 2, ...., n\}$ and $\{d_r(C) : 1 \leq r \leq k\} \cap \{n+1-d_{r^\perp} : 1 \leq r \leq n-k\} = \emptyset$. ■

# Chapter 6

# Demi-Matroids obtained from Multi-Codes (Chains of Codes).

The material in this chapter is new. We begin by considering a chain of subcodes $C_m \subseteq C_{m-1} \subseteq \cdot \cdot \cdot\cdot \subseteq C_2 \subseteq C_1$ of length $n$. Each $C_i$ has generator matrix $G_i$ and corresponding matroid $M_{C_i} = M[G_i]$ and associated rank function $\rho_i : 2^E \to \mathbb{N} \cup \{\emptyset\}$ where $E = \{1, 2, ...., n\}$. So for each $X \subseteq E, \rho_i : X \mapsto \rho_i(X)$.

**Definition 135** *We introduce new functions*

$$s_m(X) = \rho_1(X) - \rho_2(X) + \rho_3(X) - \rho_4(X) + \cdot\cdot\cdot\cdot + (-1)^{m+1}\rho_m(X)$$

*and*

$$t_m(X) = n - k - |E - X| + s_m(E - X)$$

*where*

$$k \overset{def}{=} s_m(E) = \sum(-1)^{i+1}\rho_i(E) = \sum(-1)^{i+1}k_i$$

*so*

$$k_i = \rho_i(E) = rank(G_i).$$

The following is the main result of this chapter:

**Theorem 136** *$(E, s_m, t_m)$ is a demi-matroid.*

**Proof.** To prove Theorem 136 axioms **(R)** and **(D)** for a demi-matroid must be satisfied. If $X \subseteq Y \subseteq E$:

**(R)** **(i)** $0 \leq s_m(X) \leq s_m(Y) \leq |Y|$ and **(ii)** $0 \leq t_m(X) \leq t_m(Y) \leq |Y|$ :

**(D)**$|E - X| - s_m(E - X) = t_m(E) - t_m(X)$.

We rewrite $s_m(X)$ as

$$s_m(X) = [\rho_1(X) - \rho_2(X)] + [\rho_3(X) - \rho_4(X)] + \cdot \cdot \cdot \cdot + [\rho_{m-1}(X) - \rho_m(X)]$$

when $m$ is even and similarly as

$$s_m(X) = [\rho_1(X) - \rho_2(X)] + [\rho_3(X) - \rho_4(X)] + \cdot \cdot \cdot \cdot + [\rho_{m-2}(X) - \rho_{m-1}(X)] + \rho_m(X)$$

when $m$ is odd.

We see that $\rho_i(X) \geq 0 \ \forall i$, and since $C_i \subset C_{i-1}$, then $\rho_{i-1}(X) - \rho_i(X) \geq 0 \ \forall i$. This implies that $0 \leq s_m(X)$.

Now we rewrite $s_m(Y)$ as

$$s_m(Y) = \rho_1(Y) - [\rho_2(Y) - \rho_3(Y) + \rho_4(Y) - \cdot \cdot \cdot \cdot - (-1)^{m+1}\rho_m(Y)] = \rho_1(Y) - [R_{m-1}(Y)] \leq |Y| - 0 = |Y|.$$

Here

$$R_{m-1}(Y) = \rho_2(Y) - \rho_3(Y) + \rho_4(Y) - \cdot \cdot \cdot \cdot - (-1)^{m+1}\rho_m(Y)$$

is obtained from the chain of subcodes

$$C_m \subseteq C_{m-1} \subseteq \cdot \cdot \cdot \subseteq C_2$$

and the argument in the previous paragraph gives $R_{m-1}(Y) \geq 0$. Thus we have shown $s_m(Y) \leq |Y|$.

Next we show $s_m(X) \leq s_m(Y)$ by proving $s_m(Y) - s_m(X) \leq 0$. In the case where $m$ is even we get:

$$s_m(Y) - s_m(X) = [\rho_1(Y) - \rho_2(Y)] + [\rho_3(Y) - \rho_4(Y)] + \cdots + [\rho_{m-1}(Y) - \rho_m(Y)]$$

$$-[\rho_1(X) - \rho_2(X)] - [\rho_3(X) - \rho_4(X)] - \cdots - [\rho_{m-1}(X) - \rho_m(X)]$$

In the case where $m$ is odd we get:

$$s_m(Y) - s_m(X) = [\rho_1(Y) - \rho_2(Y)] + [\rho_3(Y) - \rho_4(Y)] + \cdots + [\rho_{m-2}(Y) - \rho_{m-1}(Y)] + \rho_m(Y)$$

$$-[\rho_1(X) - \rho_2(X)] - [\rho_3(X) - \rho_4(X)] - \cdots - [\rho_{m-2}(X) - \rho_{m-1}(X)] - \rho_m(X)$$

Now since $\rho_m(Y) \geq \rho_m(X)$ the situation for $m$ odd and even amount to the same problem. This in turn reduces to the solving for $m = 2$.

We define the projection

$$\phi : (F_q)^{\rho_1(E)} \to (F_q)^{\rho_2(E)}$$

which maps

$$X|_{C_1} \to X|_{C_2}$$

Now

$$s_2(Y) = \rho_1(Y) - \rho_2(Y) = \dim(\ker(\phi|_Y))$$

and similarly

$$s_2(X) = \rho_1(X) - \rho_2(X) = \dim(\ker(\phi|_X)).$$

But, since $X \subseteq Y$ it must be true that

$$\dim(\ker(\phi|_Y)) \geq \dim(\ker(\phi|_X))$$

so

$$s_2(Y) - s_2(X) \geq 0$$

and

$$s_2(Y) \geq s_2(X)$$

Thus **(R) (i)** is proved.

From $t_m(X) = n - k - |E - X| + s_m(E - X)$ we get

$$t_m(E) = n - k \text{ so } t_m(X) = t_m(E) - |E - X| + s_m(E - X)$$

and rewriting gives

$$|E - X| - s_m(E - X) = t_m(E) - t_m(X)$$

so **(D)** is proved.

Now returning to **(R) (ii);** we have the following sequence of equivalences

$$t_m(Y) \leq |Y|$$

$$\Leftrightarrow n - k - |E - Y| + s_m(E - Y) \leq |Y|$$

$$\Leftrightarrow n - k - (n - |Y|) + s_m(E - Y) \leq |Y|$$

$$\Leftrightarrow -k + s_m(E - Y) \leq 0 \Leftrightarrow -k + s_m(E - Y) \leq 0$$

$$\Leftrightarrow s_m(E - Y) \leq k = s_m(E).$$

The last statement follows from **(R) (i)**. Hence the first statement $t_m(Y) \leq |Y|$ is also true.

Next we show that for $X \subseteq Y$ we have

$$t_m(X) \leq t_m(Y).$$

If this is the case then since $\emptyset \subseteq X$ we have that

$$t_m(\emptyset) \leq t_m(X).$$

where

$$t_m(\emptyset) = n - k - |E - \emptyset| + s_m(E - \emptyset) = n - k - n + k = 0$$

Hence the statement

$$0 \leq t_m(X)$$

follows from

$$t_m(X) \leq t_m(Y)$$

if $X \subseteq Y$ and it is sufficient to show that. Now we have the sequence of equivalences

$$t_m(X) \leq t_m(Y)$$

$$\Leftrightarrow \; n - k - |E - X| + s_m(E - X) \leq n - k - |E - Y| + s_m(E - Y)$$

$$\Leftrightarrow s_m(E - X) - s_m(E - Y) \leq |E - X| - |E - Y|$$

We now simplify our notation by letting $E - X = X'$ and $E - Y = Y'$ and get

$$s_m(X') - s_m(Y') \leq |X'| - |Y'|.$$

$$s_m(X') - s_m(Y') = \rho_1(X') - [\rho_2(X') - \rho_3(X') + \rho_4(X') - \cdots - (-1)^{m+1}\rho_m(X')]$$

$$-\rho_1(Y') + [\rho_2(Y') - \rho_3(Y') + \rho_4(Y') - \cdots - (-1)^{m+1}\rho_m(Y')]$$

$$= [\rho_1(X') - \rho_1(Y')] - [R_{m-1}(X') - R_{m-1}(Y')] \leq |X'| - |Y'|.$$

We recall the definition

$$R_{m-1}(Y) = \rho_2(Y) - \rho_3(Y) + \rho_4(Y) - \cdots - (-1)^{m+1}\rho_m(Y),$$

Thus **(R) (ii)** has been proven. ■

## 6.1 Duality

For the chain of subcodes

$$C_m \subseteq C_{m-1} \subseteq \cdots \subseteq C_2 \subseteq C_1 \qquad (*)$$

we consider the special case:

$$C_{2m} \subseteq C_{2m-1} \subseteq \cdots \subseteq C_2 \subseteq C_1$$

Since

$$C_i^{\perp} = \{\overrightarrow{y} | \overrightarrow{x}.\overrightarrow{y} = 0 \forall \overrightarrow{x} \in C_i\} \subseteq C_{i+1}^{\perp} = \{\overrightarrow{y} | \overrightarrow{x}.\overrightarrow{y} = 0 \forall \overrightarrow{x} \in C_{i+1}\}$$

we get

$$C_{2m}^{\perp} \supseteq C_{2m-1}^{\perp} \cdots \supseteq C_2^{\perp} \supseteq C_1^{\perp} \qquad (**)$$

For the chain of subcodes in $(*)$ we have for all $X \subseteq E$ the associated function

$$s_{2m}(X) = \rho_1(X) - \rho_2(X) + \rho_3(X) \cdots + \rho_{2m-1}(X) - \rho_{2m}(X)$$

Similarly for the chain of subcodes in $(**)$ we have for all $X \subseteq E$ the associated function

$$\rho_{2m}^*(X) - \rho_{2m-1}^*(X) + \cdots + \rho_2^*(X) - \rho_1^*(X)$$

Now rewriting gives

$$[|X| - \rho_1^*(X)] - [|X| - \rho_2^*(X)] +$$
$$[|X| - \rho_3^*(X)] - [|X| - \rho_4^*(X)] +$$
$$.$$
$$.$$
$$.$$
$$[|X| - \rho_{2m-1}^*(X)] - [|X| - \rho_{2m}^*(X)]$$

and applying $s(E) - s(E - X) = |X| - t(X)$ gives

$$[\rho_1(E) - \rho_1(E - X)]$$
$$-[\rho_2(E) - \rho_2(E - X)]$$
$$.$$
$$.$$
$$.$$
$$+[\rho_{2m-1}(E) - \rho_{2m-1}(E - X)]$$
$$-[\rho_{2m}(E) - \rho_{2m}(E - X)]$$

$$= [\rho_1(E) - \rho_2(E) + \rho_3(E) \cdot \cdots + \rho_{2m-1}(E) - \rho_{2m}(E)]$$
$$-[\rho_1(E - X) - \rho_2(E - X) + \rho_3(E - X) \cdot \cdots + \rho_{2m-1}(E - X) - \rho_{2m}(E - X)]$$

$$= s_{2m}(E) - s_{2m}(E - X) = \overline{s}_{2m}(X)$$

For the case where we have an uneven number of subcodes in our chain i.e.

$$C_{2m-1} \subseteq C_{2m-2} \subseteq \cdot \cdot \cdot \subseteq C_2 \subseteq C_1$$

we simply introduce a dummy code $C_{2m} = \mathbf{0}$; which is perfectly valid since the zero code is a subcode of all linear codes. Thus we get

$$C_{2m} \subseteq C_{2m-1} \subseteq \cdot \cdot \cdot \subseteq C_2 \subseteq C_1$$

as before with $\rho_{2m}(X) \triangleq 0$ and can use our previously attained formulae for an even number of subcodes.

# Chapter 7

# Generalisation of results in [5]

The results of this chapter are new unless otherwise specified. They are inspired by results in [2] for simple codes and [5] for pairs of codes. We prove corresponding results for multi-codes and use to a great extent demi-matroid techniques.

**Definition 137** *Let $X \subseteq E = \{1, ..., n\}$, for an $[n, k]$ linear code $C$, its subcode $C_X$ is defined as $\{(a_1, a_2, a_3...., a_n) \in C | a_t = 0 \text{ for } t \notin X\}$. Its projection $P_X(C)$ is defined as $\{P_X(\mathbf{a}) | \mathbf{a} = (a_1, a_2, a_3...., a_n) \in C\}$ where $P_X(\mathbf{a})$ is a vector of length $n$ and the $t^{th}$ component of $P_X(\mathbf{a})$ is given by $a_t$ if $t \in X$ and given by $0$ if $t \notin X$.*

What follows is called The First Duality Lemma [2]:

**Lemma 138** *For an $[n, k]$ linear code $C$ and a set $X \subseteq E = \{1, ..., n\}$*
$\dim[P_X(C)] + \dim(C_{E-X}) = k.$

**Proof.** $C_X$ is effectively a mapping $\phi : (F_q)^n \to (F_q)^{\dim P_X(C)}$. For example if $X = \{i_1, i_2, i_3\}$, then $\phi : (a_1, a_2, a_3...., a_n) \mapsto (0, a_{i_1}, 0, ..., a_{i_2}, 0, ....0, a_{i_3}, 0..0)$ which clearly illustrates that the subcode given by $\{\mathbf{a} = (0, a_{i_1}, 0, ..., a_{i_2}, 0, ....0, a_{i_3}, 0..0)\}$ has dimension $P_X(C)$. The kernel of $\phi$ is given by $\ker \phi = \{\mathbf{a} | a_{i_1} = a_{i_2} = a_{i_3} = 0\} = C_{E-X}$. Now by The Dimension Theorem we have:

$$\dim C = \dim(\ker \phi) + \dim(image(\phi))$$

$$\Rightarrow k = \dim(C_{E-X}) + \dim(P_X(C)).$$

■

We note that $\dim[P_X(C)] = \rho(C)$ where $\rho$ is the rank function associated with the matroid $M_C$.

We denote $\dim[P_X(C)]$ by $\rho(X)$ and consider the demi-matroid $(E, \rho, \rho^*)$. For this demi-matroid we have:

**Lemma 139** $\overline{\rho}(X) = \dim(C_X)$

**Proof.** From Lemma 138 we have that:

$$\rho(X) + \dim(C_{E-X}) = k = \rho(E).$$

So

$$\dim(C_{E-X}) = \rho(E) - \rho(X).$$

Now substituting for $X = E - X$ we get

$$\dim(C_X) = \rho(E) - \rho(E - X) = \overline{\rho}(X).$$

Thus the lemma is proved. ■

We now look at the multi-code case where we have:

$$C_m \subseteq C_{m-1} \subseteq \cdot \cdot \cdot \cdot \subseteq C_2 \subseteq C_1$$

We set

$$s_m(X) = \rho_1(X) - \rho_2(X) + \rho_3(X) - \rho_4(X) + \cdot \cdot \cdot \cdot + (-1)^{m+1}\rho_m(X)$$

where

$$\rho_i(X) = \dim[P_X(C_i)] \text{ which we denote } \dim[P_X(C^i)]$$

Then we consider the demi-matroid $(E, s_m, t_m)$ introduced in Definition 135. For this demi-matroid we have:

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

$$= [\rho_1(E) - \rho_2(E) + \cdots\cdot + (-1)^{m+1}\rho_m(E)] - [\rho_1(E-X) - \rho_2(E-X) + \cdots\cdot + (-1)^{m+1}\rho_m(E-X)]$$

$$\begin{array}{c} [\rho_1(E) - \rho_1(E-X)] \\ -[\rho_2(E) - \rho_2(E-X)] \\ . \\ . \\ . \\ +(-1)^{m+1}[\rho_m(E) - \rho_m(E-X)] \end{array}$$

$$= \overline{\rho}_1(X) - \overline{\rho}_2(X) + \cdots\cdot + (-1)^{m+1}\overline{\rho}_m(X)$$
$$= \dim(C_X^1) - \dim(C_X^2) + \cdots\cdot + (-1)^{m+1}\dim(C_X^m)$$

**Conclusion 140** *If*

$$s_m(X) \overset{def}{=} \dim[P_X(C^1)] - \dim[P_X(C^2)] + \cdots\cdot + (-1)^{m+1}\dim[P_X(C^m)]$$

*then*

$$\overline{s}_m(X) = \dim(C_X^1) - \dim(C_X^2) + \cdots\cdot + (-1)^{m+1}\dim(C_X^m)$$

For any demi-matroid $(E, s, t)$, we define $K_i$ and $\widetilde{K}_i$ as follows:

**Definition 141** $K_i \overset{def}{=} \max\{\overline{s}(X) \mid |X| = i\}$ *and* $\widetilde{K}_i \overset{def}{=} \min\{s(X) \mid |X| = i\}$

**Remark 142** *We observe in the article [**5**] with $m = 2$ that we have he following situation:*

$$K_i(C^1, C^2) = \max(\dim(C_X^1) - \dim(C_X^2) : |X| = i)$$

*and that corresponds to the situation where*

$$\overline{s}(X) = \overline{s_2}(X) = \dim(C_X^1) - \dim(C_X^2) = \overline{\rho}_1(X) - \overline{\rho}_2(X)$$

$$\widetilde{K}_i(C^1, C^2) = \min(\dim[P_X(C^1)] - \dim[P_X(C^2)] : |X| = i)$$

*and*

$$s(X) = s_2(X) = \dim[P_X(C^1)] - \dim[P_X(C^2)] = \rho_1(X) - \rho_2(X)$$

*For the multi-code case we have*

$$C_m \subseteq C_{m-1} \subseteq \cdots \subseteq C_2 \subseteq C_1$$

*with demi-matroid*

$$(E, s_m, t_m)$$

*and*

$$s(X) \overset{def}{=} s_m(X) \text{ and } \overline{s}(X) = \overline{s}_m(X)$$

*Then*

$$K_i = \max\{\overline{s}(X)||X| = i\}$$

$$= \max(\dim(C^1_X) - \dim(C^2_X) + \cdots + (-1)^{m+1}\dim(C^m_X) : |X| = i)$$

$$= \max(\overline{\rho}_1(X) - \overline{\rho}_2(X) + \cdots + (-1)^{m+1}\overline{\rho}_m(X) : |X| = i)$$

*and*

$$s(X) \overset{def}{=} s_m(X)$$

*so*

$$\widetilde{K}_i = \min\{s(X)||X| = i\}$$

$$= \min\{\dim[P_X(C^1)] - \dim[P_X(C^2)] + \cdots + (-1)^{m+1}\dim[P_X(C^m)] : |X| = i\}$$

$$= \min\{\rho_1(X) - \rho_2(X) + \cdots + (-1)^{m+1}\rho_m(X) : |X| = i\}$$

**Remark 143** *In [5] it is proven that:*

$$K_i(C^1, C^2) = (a_1 - a_2) - \widetilde{K}_{n-i}(C^1, C^2),$$

*where* $a_i = \dim(C^i)$*, for* $i = 1, 2$.

*This result is analogous to that obtained for a demi-matroid given in the next theorem.*

**Theorem 144** *For any demi-matroid* $(E, s, t)$*, we have*

$$K_i = s(E) - \widetilde{K}_{n-i}$$

*where* $n = |E|$*.*

**Proof.**

$$\widetilde{K}_i = \min\{s(X)||X| = i\}$$

$$= \min\{s(E) - \overline{s}(E - X)||X| = i\}$$

$$= \min\{s(E) - \overline{s}(X)||X| = n - i\}$$

$$= s(E) + \min\{-\overline{s}(X)||X| = n - i\}$$

$$= s(E) - \max\{\overline{s}(X)||X| = n - i\}$$

$$= s(E) - K_{n-i}$$

so

$$\widetilde{K}_i = s(E) - K_{n-i}$$

replacing $i$ by $n - i$ gives

$$\widetilde{K}_{n-i} = s(E) - K_i$$

■

**Corollary 145** *Theorem 144 also holds for the multi-code case:*

*For*

$$C_m \subseteq C_{m-1} \subseteq \cdots \subseteq C_2 \subseteq C_1$$

*we have*

$$K_i = s_m(E) - \widetilde{K}_{n-i}$$

*where $s_m(X)$ is as defined earlier.*

**Remark 146** *In [5] it is proven in Proposition 1 that for $m = 2$:*

$$0 \leq K_{i+1}(C^1, C^2) - K_i(C^1, C^2) \leq 1$$

*and*

$$0 \leq \widetilde{K}_{i+1}(C^1, C^2) - \widetilde{K}_i(C^1, C^2) \leq 1$$

*and*

$$K_0(C^1, C^2) = \widetilde{K}_0(C^1, C^2) = 0$$

*and*

$$K_n(C^1, C^2) = \widetilde{K}_n(C^1, C^2) = \dim C^1 - \dim C^2.$$

*It will now be shown that this is also essentially a result about demi-matroids in general. In other words:*

**Proposition 147** *For a demi-matroid $(E, s, t)$ we have:*

$$0 \leq K_{i+1} - K_i \leq 1$$

$$0 \leq \widetilde{K}_{i+1} - \widetilde{K}_i \leq 1$$

*for $i \leq n - 1$ where $n = |E|$.*

**Proof.** We have

$$K_i = \max\{\overline{s}(X) || X| = i\}$$

and

$$K_{i+1} = \max\{\overline{s}(X) | |X| = i + 1\}$$

Let $X_0 \subseteq E$ be such that

$$|X_0| = i$$

and

$$\overline{s}(X_0) = K_i.$$

Let $y \in (E - X_0)$ and set

$$X_1 = X_0 \cup \{y\}.$$

Then

$$|X_1| = i + 1.$$

Furthermore

$$K_i = \overline{s}(X_0) \leq \overline{s}(X_1) \leq \max\{\overline{s}(X) | |X| = i + 1\} = K_{i+1}$$

So

$$0 \leq K_{i+1} - K_i.$$

Next we choose $Y_0 \subseteq E$ such that

$$|Y_0| = i + 1$$

and

$$\overline{s}(Y_0) = K_{i+1}.$$

Pick $y \in Y_0$ and set

$$Y_1 = Y_0 - \{y\}.$$

Then

$$|Y_1| = i$$

and

$$K_i \geq \overline{s}(Y_1) \geq \overline{s}(Y_0) - 1 = K_{i+1} - 1$$

so

$$1 \geq K_{i+1} - K_i.$$

Furthermore

$$\widetilde{K}_i = s(E) - K_{n-i}$$

$$\widetilde{K}_{i+1} - \widetilde{K}_i = (s(E) - K_{n-i-1}) - (s(E) - K_{n-i}) = K_{n-i} - K_{(n-i)-1} = K_{i'+1} - K_{i'}$$

So the proof also holds for $\widetilde{K}_{i+1}$ and $\widetilde{K}_i$. ■

**Remark 148** *It will now be shown that* $K_{0'} = \widetilde{K}_0 = 0$ *and that* $K_{n'} = \widetilde{K}_n = s(E)$.

**Proof.** We have that

$$K_i = \max\{\overline{s}(X) | |X| = i\}$$

so

$$K_0 = \max\{\overline{s}(X) | |X| = 0\}$$

$$= s(\emptyset) = 0$$

We also have that

$$K_n = \max\{\overline{s}(X) | |X| = n\}$$

$$= s(E)$$

Now from Theorem 144 we have that

$$K_i = s(E) - \widetilde{K}_{n-i}$$

which gives

$$K_0 = s(E) - \widetilde{K}_n$$

$$0 = s(E) - \widetilde{K}_n$$

$$\Rightarrow \widetilde{K}_n = s(E)$$

Returning to Theorem 144 we have

$$\widetilde{K}_i = s(E) - K_{n-i}$$

$$\widetilde{K}_0 = s(E) - K_n$$

$$\widetilde{K}_0 = s(E) - s(E)$$

$$\Rightarrow \widetilde{K}_0 = 0$$

■

**Remark 149** *For linear codes we recall that*

$$d_i = \overline{\sigma}_i$$

*For a general demi-matroid we use the expression*

$$M_i \overset{def}{=} \overline{\sigma}_i \overset{def}{=} \min\{|X| : \overline{s}(X) \geq i\}.$$

*We have simultaneously*

$$K_i = \max\{\overline{s}(X)||X| = i\}$$

*For demi-matroids we have that the $M_j$ are determined by the $K_i$, and the $K_i$ are determined by the $M_i$, in the following explicit way:*

**Theorem 150**

$$M_j = \min\{i|K_i \geq j\}$$

$$K_i = \max\{j|M_j \leq i\}$$

*where $0 \leq i \leq n$ and $0 \leq j \leq s(E)$.*

**Proof.**

$$\min\{i : K_i \geq j\}$$

$$= \min\{i : \exists|X| = i \text{ such that } \overline{s}(X) \geq j\}$$

$$= \min\{|X| : \overline{s}(X) \geq j\} = M_j.$$

and

$$\max\{j | M_j \leq i\}$$

$$= \max\{j : \exists |X| \leq i \text{ such that } \overline{s}(X) \geq j\}$$

$$= \max\{\overline{s}(X) : |X| \leq i\} = K_i.$$

■

**Proposition 151** *Given a demi-matroid $(E, s, t)$ then*

$$M_{j+1} > M_j$$

*for all $j = 0, ., s(E) - 1$. Moreover, $M_o = 0$ and*

$$M_j = \min\{i | K_i = j\}$$

$$= \min\{|X| : \overline{s}(X) = j\}$$

*for $0 \leq j \leq s(E)$.*

**Proof.** Clearly $M_j \leq M_{j+1}$. Assume

$$M_j = M_{j+1}.$$

We know that

$$M_j = \min\{i | K_i \geq j\}.$$

This implies

$$K_{M_{j-1}} \leq j - 1.$$

If $M_j = M_{j+1}$ then

$$K_{M_j} \geq j + 1.$$

Hence .

$$K_{M_j} - K_{M_{j-1}} \geq (j+1) - (j-1) = 2.$$

This is a contradiction. Hence

$$M_j < M_{j+1}.$$

Obviously $M_0 = 0$ which comes from the fact that

$$M_0 = \min\{|X| : \overline{s}(X) \geq j\} = 0$$

since

$$\overline{s}(\emptyset) = 0.$$

We now show

$$M_j = \min\{i|K_i = j\}.$$

We know

$$M_j = \min\{i|K_i \geq j\}$$

this implies

$$K_{M_{j-1}} \leq j - 1$$

hence

$$K_{M_j} \leq K_{M_{j-1}} + 1 \leq (j - 1 + 1) = j$$

but, since

$$K_{M_j} \geq j$$

we have that

$$K_{M_j} = j$$

Hence

$$M_j = \min\{i|K_i = j\}$$

Next we show

$$M_j = \min\{|X| : \overline{s}(X) = j\}.$$

We know that

$$M_j = \min\{|X| : \overline{s}(X) \geq j\}.$$

We choose $X$, such that

$$|X| = M_j, \text{ and } \overline{s}(X) \geq j$$

We now consider $Y = X - \{x_0\}$ where $x_0 \in X$. Then

$$|Y| = M_j - 1$$

and hence

$$\overline{s}(Y) \leq j - 1.$$

If

$$\overline{s}(X) > j + 1,$$

then

$$\overline{s}(X) - \overline{s}(X - \{x_0\}) \geq 2$$

which by Lemma 99 is a contradiction. Hence

$$\overline{s}(X) = j$$

and

$$M_j = |X| = \min\{|X| : \overline{s}(X) = j\}.$$

■

**Remark 152** *We will now generalise Section IV of* **[5],** *(which is itself takes the Singleton bound for single code and generalises it to the pair of codes case.), to the multi-code case. The Singleton bound was defined in Corollary128 for linear codes $C$..*

*We have seen earlier that for the matroid $M[C]$, we have $d_i = M_i$, $k = s(E)$ with $\widetilde{K}_i$ and $K_i$ being determined by $M_i$, and visa versa. In terms of $M_i$,$\widetilde{K}_i$ and $K_i$ the Singleton bound reads as follows:*

$$M_j \leq \begin{cases} 0 & \textit{for } \; j\text{= } 0. \\ n-k+j & \textit{for } j=1,....,k. \end{cases}$$

$$K_i \geq \begin{cases} 0 & \textit{for } i=0,1,.....,n-k. \\ i-(n-k)=i-n+k & \textit{for } i=n-k,....,n. \end{cases}$$

*and*

$$\widetilde{K}_i \leq \begin{cases} i & \textit{for } i=0,..............,k. \\ k & \textit{for } i=k,..............,n. \end{cases}$$

*We have in fact equality in the inequality for all $i \Leftrightarrow C$ is an MDS code $\Leftrightarrow M[C]$ is a uniform matroid.*

These bounds are now generalised to the case of demi-matroids which have been obtained from multi-codes. We start with the $\widetilde{K}_i$ :

**Proposition 153** *First we observe that $\widetilde{K}_{\rho_{2h}} = 0$ where $\rho_i \overset{def}{=} \rho_i(E)$ for all $i$.The generalised lower bound for the $\widetilde{K_i}$ is given by:*

$$\widetilde{K_i} \leq \begin{cases} 0 & \textit{for } i \leq \rho_{2h} \\ i\text{–}\rho_{2h} & \textit{for } \rho_{2h} \leq i \leq \rho_{2h} + s_{2h}(E) = s_{2h-1}(E). \\ s_{2h}(E) & \textit{for } i \geq s_{2h-1}(E) \end{cases} \quad .$$

**Proof.** Since

$$\dim(C_{2h}) = \rho_{2h}, \exists\, \mathcal{I} \subseteq \{1,...,n\} \textit{ with } |\mathcal{I}| = \rho_{2h},$$

and

$$\dim[P_{\mathcal{I}}(C_{2h})] = \rho_{2h}.$$

This gives:

$$\dim[P_{\mathcal{I}}(C_i)] = \rho_i \text{ for all } i.$$

Now

$$s_{2h}(\mathcal{I}) = \sum(-1)^{i+1}\rho_i(\mathcal{I}) = \sum(-1)^{i+1}\rho_i(\mathcal{I}) = \dim[P_{\mathcal{I}}(C_i)] = \sum_{i=1}^{2h}(-1)^{i+1}\rho_{2h} = 0.$$

But

$$\widetilde{K}_i = \min\{s(X)||X| = i\}$$

so

$$\widetilde{K}_{\rho_{2h}} = \min\{s(X)||X| = \rho_{2h}\}.$$

Choose $X = \mathcal{I}$ and we get

$$s_{2h}(\mathcal{I}) = 0.$$

Hence

$$\widetilde{K}_{\rho_{2h}} = 0$$

and

$$\widetilde{K}_i = 0,\ \forall i \leq \rho_{2h}.$$

Furthermore

$$\widetilde{K}_{i+1} - \widetilde{K}_i \leq 1\ \forall i.$$

Thus

$$\widetilde{K}_i \leq i - \rho_{2h},\ for\ i = \rho_{2h}, \rho_{2h+1}, ..., \rho_{2h} + s_{2h}(E)$$

Now look at the range

$$i \geq \rho_{2h} + s_{2h}(E)$$

$$= \rho_1(E) - \rho_2(E) + ... + \rho_{2h-1}(E) - \rho_{2h}(E) + \rho_{2h}(E)$$

$$= \rho_1(E) - \rho_2(E) + ... + \rho_{2h-1}(E)$$

$$= s_{2h-1}(E).$$

Then we have

$$\widetilde{K}_i \leq s_{2h}(E)$$

This is clear since

$$\widetilde{K}_i \overset{def}{=} \min\{s_{2h}(X)||X| = i\}$$

For all $X$, we have that

$$s_{2h}(X) \leq s_{2h}(E)$$

clearly

$$\widetilde{K}_i \leq s_{2h}(E); \forall i.$$

We end up with the generalised Singleton bound :

$$\widetilde{K_i} \leq \begin{cases} 0 & \text{for } i \leq \rho_{2h} \\ i - \rho_{2h} & \text{for } \rho_{2h} \leq i \leq \rho_{2h} + s_{2h}(E) = s_{2h-1}(E). \\ s_{2h}(E) & \text{for } i \geq s_{2h-1}(E) \end{cases}$$

■

**Proposition 154** *The generalised upper bound for the $K_i$ is given by:*

$$K_i \geq \begin{cases} s_{2h}(E) - s_{2h}(E) = 0 & \textit{for } i \leq n - s_{2h-1} \\ i - (n - s_{2h-1}(E)) = i - n + s_{2h-1}(E) & \textit{for } n - s_{2h-1}(E) \leq i \leq n - \rho_{2h}(E). \\ s_{2h}(E) & \textit{for } n - \rho_{2h-1}(E) \leq i \leq n. \end{cases}$$

**Proof.** We use the formula

$$K_i = s_{2h}(E) - \widetilde{K}_i$$

to derive the lower bound for the $K_i$. We get:

$$K_i \geq \begin{cases} s_{2h}(E) - s_{2h}(E) = 0 & \text{for } i \leq n - s_{2h-1} \\ i - (n - s_{2h-1}(E)) = i - n + s_{2h-1}(E) & \text{for } n - s_{2h-1}(E) \leq i \leq n - \rho_{2h}(E). \\ s_{2h}(E) & \text{for } n - \rho_{2h-1}(E) \leq i \leq n. \end{cases}$$

■

**Proposition 155** *The generalised lower bound for the $M_j$ is given by:*

$$M_j \leq \begin{cases} 0 & \textit{for } j = 0 \\ n - \rho_{2h} - s_{2h}(E) + j & \textit{for } j = 1, 2, ...., s_{2h}(E). \end{cases}$$

**Proof.** We have from Theorem 150 that

$$M_j = \min\{i | K_i \geq j\}.$$

Set

$$n - \rho_{2h} - s_{2h}(E) = a$$

and

$$n - \rho_{2h} = b.$$

We see that

$$M_0 \leq 0$$

$$M_1 \leq a + 1$$

$$M_2 \leq a + 2$$

$$.$$

$$.$$

$$.$$

$$M_{s_{2h}(E)} \leq b = a + s_{2h}(E)$$

We get:

$$M_j \leq \begin{cases} 0 & \text{for } j = 0 \\ n - \rho_{2h} - s_{2h}(E) + j & \text{for } j = 1, 2, ...., s_{2h}(E). \end{cases}$$

■

**Remark 156** *We now check our generalisation for the cases where we have pairs of codes $C_2 \subseteq C_1$ and individual codes $C_1$.*

**Solution 157** *Assume $h = 1$, so $C_2 \subseteq C_1$ are the only codes. We get: $M_0 = 0$, $M_j = n - \rho_2 - s_2(E) + j = n - s_2(E) + j = n - (\rho_1 - \rho_2) + j$ which is the bound given in Section IV of **[5]**. For the case of individual codes with $\dim(C_1) \overset{def}{=} k = \rho_1$, we examine the case where $C_2 = \{\emptyset\}$, and get: $d_j = M_j \leq n - \rho_1 + j = n - k + j$. Which is the usual Singleton bound.*

**Definition 158** *A multi-code, $C_{2h} \subseteq \cdots \subseteq C_1$ is **optimal** if there is equality in the Singleton bound for all i, i.e.*

$$M_i = \begin{cases} 0 & \textit{for } i = 0 \\ n - \rho_{2h} - s_{2h}(E) + i & \textit{for } i = 1, 2, ...., s_{2h}(E). \end{cases}$$

*equivalently*

$$K_i = \begin{cases} s_{2h}(E) - s_{2h}(E) = 0 & \textit{for } i \leq n - s_{2h-1} \\ i-(n - s_{2h-1}(E)) = i-n + s_{2h-1}(E) & \textit{for } n - s_{2h-1}(E) \leq i \leq n - \rho_{2h}(E). \\ s_{2h}(E) & \textit{for } n - \rho_{2h-1}(E) \leq i \leq n. \end{cases}$$

*equivalently*

$$\widetilde{K_i} = \begin{cases} 0 & \textit{for } i \leq \rho_{2h} \\ i-\rho_{2h} & \textit{for } \rho_{2h} \leq i \leq \rho_{2h} + s_{2h}(E) = s_{2h-1}(E). \\ s_{2h}(E) & \textit{for } i \geq s_{2h-1}(E) \end{cases}$$

**Proposition 159** *The code is optimal if:*

$$\widetilde{K}_{\rho_{2h}+s_{2h}(E)} = s_{2h}(E)$$

*equivalently*

$$K_{n-s_{2h-1}(E)} = 0 \ \ (K_a = 0)$$

*equivalently*

$$M_1 = a + 1$$

*where*

$$a = n - (s_{2h}(E) + \rho_{2h}) \ as \ before.$$

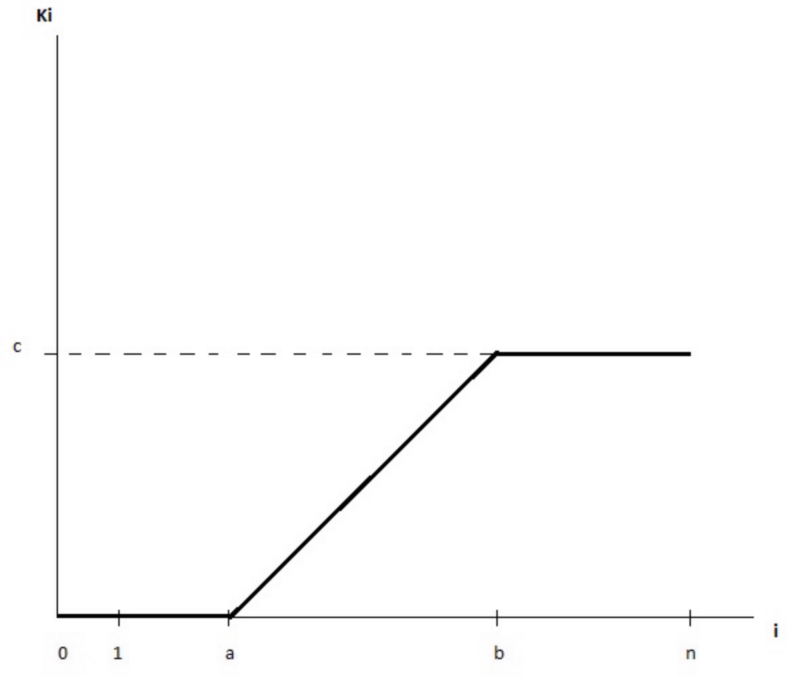


Figure 4

**Proof.** We will first prove that if $K_a = 0$, then $K_i$ is equal the specified values of Definition 158 for all $i$. These values are indicated in Figure 4. And $c = s_{2h}(E)$. If $i \leq a$, then $K_i \leq K_a$ (which follows directly from Proposition 147). We also have $K_i \geq 0$, so then $K_i = 0$ for these $i$. For $a \leq i \leq b$, we have the Singleton bound.: $K_i \geq i - a$. This means that the points $(i, K_i)$ are not below the sloped section of the graph. On the other hand: $K_{i+1} - K_i \leq 1$, for all $i$, so

$$K_{a+1} \leq K_a + 1 = 0 + 1 = 1.$$

$$K_{a+2} \leq K_{a+1} + 1 \leq 1 + 1 = 2.$$

and so on. Hence the points $(i, K_i)$ are not above the sloped section of the graph for $a \leq i \leq b$. So the points $(i, K_i)$ lie on the sloped section of the graph for $a \leq i \leq b$. For $i \geq b$ the Singleton bound gives $K_i \geq s_{2h}(E)$, hence we are not below the upper horizontal line. On the other hand: $K_i$ is trivially at most $s_{2h}(E)$ by Definition 141 (since $\overline{s}_{2h}(X) \leq \overline{s}_{2h}(E) = s_{2h}(E)$). ■

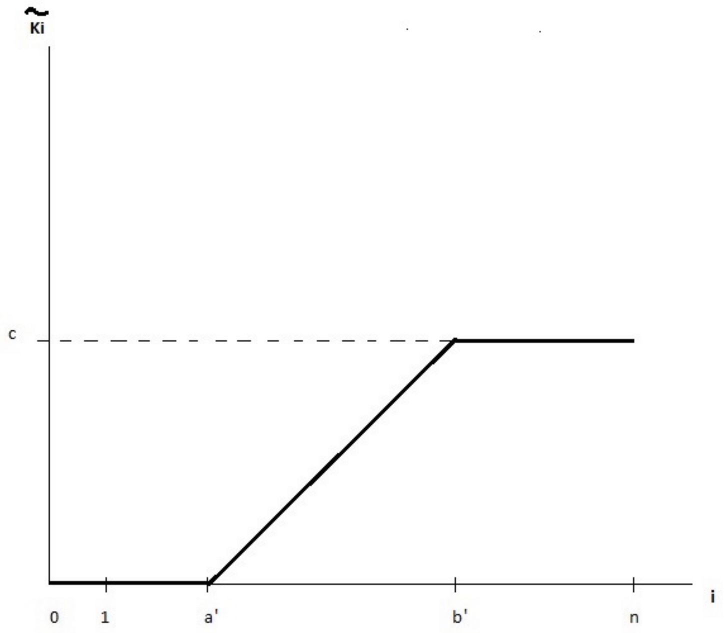


Figure 5

We now prove the second part of the Proposition 159 while referring to Figure 5:

**Proof.** Since $\widetilde{K}_{a'} \leq 0$, (Singleton bound), we must have $\widetilde{K}_{a'} = 0$ since $\widetilde{K}_i$ is non negative. Moreover $\widetilde{K}_i = 0$, for all $i \leq a'$, since $\widetilde{K}_i$ is non decreasing in $i$. Further $\widetilde{K}_i \leq s_{2h}(E)$ for all $i$, including $i \geq b'$. But since $\widetilde{K}_{b'} = s_{2h}(E)$, we have that $\widetilde{K}_i \geq \widetilde{K}_{b'} = s_{2h}(E)$ for $i \geq b'$, since the $\widetilde{K}_i$ are non-decreasing in $i$. Hence $\widetilde{K}_i = s_{2h}(E)$, for $i \geq b'$. For $a' \leq i \leq b'$ we have $\widetilde{K}_i \leq i - a'$ by the Singleton bound. But $\widetilde{K}_{b'-1} \geq \widetilde{K}_{b'} - 1$ by Remark 146. In the same way

$$\widetilde{K}_{b'-2} \geq \widetilde{K}_{b'-1} - 1 \geq (\widetilde{K}_{b'} - 1) - 1 = \widetilde{K}_{b'} - 2$$

$$\widetilde{K}_{b'-3} \geq \widetilde{K}_{b'-2} - 1 \geq (\widetilde{K}_{b'} - 2) - 1 = \widetilde{K}_{b'} - 3$$

and so on.

Hence

$$\widetilde{K}_{b'-j} \geq \widetilde{K}_{b'} - j = s_{2h}(E) - j \text{ for all positive } j$$

$$\widetilde{K}_i = \widetilde{K}_{b'-(b'-i)} \geq s_{2h}(E) - (b' - i)$$

$$= s_{2h}(E) - b' + i$$

$$= i - (b' - s_{2h}(E))$$

$$= i - (s_{2h-1}(E) - s_{2h}(E))$$

$$= i - \rho_{2h}$$

where

$$j = b' - i.$$

■

We now prove the third part of the Proposition 159 while referring to Figure 6:

**Proof.** We will prove that if $M_i = a + 1$, then the $M_i$ are equal to the specified values from of Definition 158 for all $i$. Firstly we have

$$M_0 = 0$$

since

$$M_0 \overset{def}{=} \min\{|X| : \overline{s}(X) \geq 0\}.$$

But,

$$s(\emptyset) = 0,$$

so

$$M_0 = 0.$$

Moreover, the Singleton bound gives:

$$M_i \leq a + i$$

for all $i$, so the points $(i, M_i)$ are not above the slope of the curve for $i \geq 1$.

In addition

$$M_{i+1} \geq M_i + 1$$

for all $1 \leq i \leq s_{2h}(E) - 1$.

Hence

$$M_2 \geq M_1 + 1 = (a+1) + 1 = a + 2.$$

$$M_3 \geq M_2 + 1 \geq (a+2) + 1 = a + 3.$$

and so on.

Hence $M_i \geq a + i$ for all of these $i$. ■

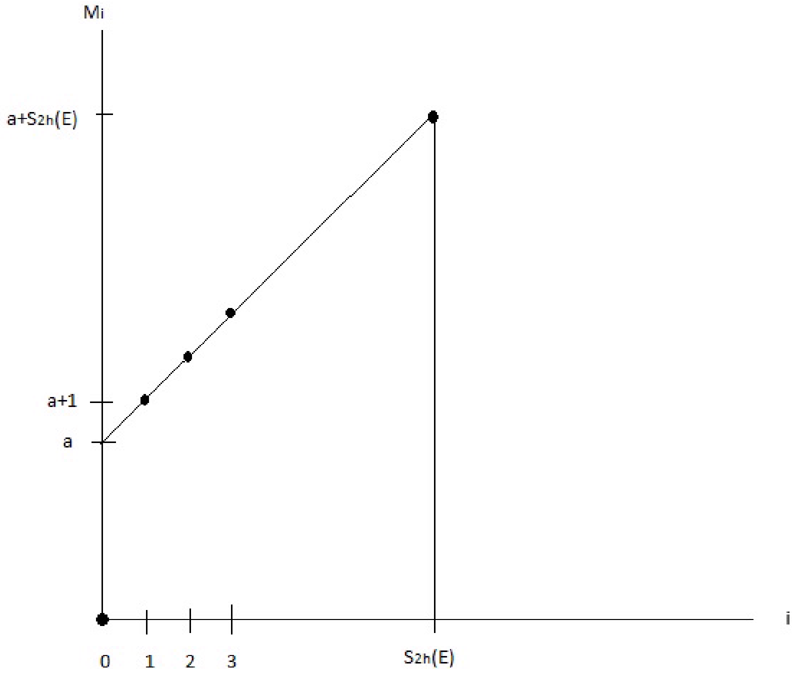


Figure 6

# Chapter 8

# Bibliography

[1] T. Britz, B. Heiseldal, T. Johnsen, D. Mayhew & K. Shiromoto, *Generalizations of Wei's Duality Theorem*, arXiv: 0910.2099, cs.IT (2009).

[2] G. D. Forney, *Dimension/length profiles and trellis complexity of linear block codes*, IEEE Transactions on Information Theory, Vol. 40, No. 6, pg. 1741-1752 (1994).

[3] R. Hill, *A First Course in Coding Theory*, Oxford University Press (1986).

[4] W. C. Huffman & V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press (2003).

[5] Y. Luo, C. Mitrpant, A. J. Han Vinck & K. Chen, *Some New Characters on the Wire-Tap Channel of Type II*, IEEE Transactions on Information Theory, Vol. 51, No. 3, pg. 1222-1229 (2005).

[6] J. Oxley, *Matroid Theory*, Oxford University Press (1992).

[7] J. Oxley, *What is a Matroid?* (revised version of 2003 paper that appeared in Cubo 5), prepared for presentation at the Workshop on Combinatorics and its Applications (Auckland 2004), www.math.lsu.edu/~oxley/survey4.pdf.

[8] V. K. Wei, *Generalized Hamming Weights for Linear Codes*, IEEE Transactions on Information Theory, Vol. 37, No. 5, pg. 1412-1418 (1991).