國立交通大學

應用數學系

碩 士 論 文

組合編碼的簡介

A Survey on
Combinatorial Coding Theory

研 究 生：張景堯
指導教授：翁志文 教授

中 華 民 國 九 十 六 年 六 月

組合編碼的簡介

A Survey On Combinatorial Coding Theory

研　究　生：張景堯　　Student：Jin-yao Zhang

指導教授：翁志文　　Advisor：Chih-Wen Weng

國 立 交 通 大 學

應 用 數 學 系

碩 士 論 文

A Thesis
Submitted to Department of Applied Mathematics
College of Science
National Chiao Tung University
In Partial Fulfillment of the Requirements
For the Degree of
Master
In

Applied Mathematics

June 2007

Hsinchu, Taiwan, Republic of China

中華民國九十六年六月

組合編碼的簡介

研 究 生：張景堯　　　　　　指導教授：翁志文　教授

國 立 交 通 大 學

應 用 數 學 系

中文摘要

我們研究比較有組合性質的碼，如 super imposed codes, Reed-Muller Codes, Punctured Reed-Muller Codes, Hexacode, Extended Golay Code 和 Convolutional Codes 等。我們探討這些碼和投影空間(projective geometries), 仿射空間(affine geometries), 甚至一般的 ranked poset 的關係。

A Survey on
Combinatorial Coding Theory

Student: Jin-Yao Zhang

Department of Applied Mathematics

National Chiao Tung University

Hsinchu, Taiwan 30050

Advisor: Chih-Wen Weng

Department of Applied Mathematics

National Chiao Tung University

Hsinchu, Taiwan 30050

Abstract

We study codes with more combinatorial properties involved than algebraic properties. These include super imposed codes, Reed-Muller Codes, Punctured Reed-Muller Codes, Hexacode, Extended Golay Code and Convolutional Codes, most of them are related to the incidence structure on the projective geometries, affine geometries, or some ranked posets.

謝誌

首先感謝我的指導老師翁志文教授，花了很多的時間來指導我寫論文，從他的身上學習到一些如何思考想問題的方法，在這些過程中，讓我覺得自己處理事情的能力更進步了，除此之外，發覺老師的修養非常非常好，從沒看過他發脾氣罵人，總是不厭其煩地幫助學生學習，是個很好的學習榜樣，真的非常感謝他。

在論文的製造過程中，我也向蠻多學長、同學和學弟求助的，其中包含了黃喻培、黃皜文、余國安…等人，經過他們的幫忙或是跟他們交流討論之後，我的思考變得更加明確，把錯誤的想法修正，使得在弄這個論文會變得更得心應手。

在交大的求學過程中，我有修過的課程老師都很感謝，在應數所上的老師有翁志文、傅恆霖、黃大原、陳秋媛、黃光明、李榮耀、符麥克和王夏聲，讓我認識到更多的數學，最主要是學到思考數學的技巧和方法;還有在教程中心的老師有陳致嘉、方紫薇、彭心儀、顏貽隆、許韶玲、林珊如、孟瑛如、陳昭秀和周倩，讓我了解在教育方面的東西，最主要的是讓我了解一些心理與輔導方面的知識。

在交大也打了三年的籃球校隊，在這樣子競爭的環境之中，讓我的心理堅強了不少，除了感謝宋濤和陳忠強的技術指導，也感謝一些隊友彼此之間的想法交流討論，互相給予回饋，一起進步。

其他要感謝的就是陳宏賓、黎冠成、李秉璋、羅元勳、蔡宗翰、周俊全、卜文強、張靖尉、陳聖怡、吳春慧、黃囿芳、徐毅樺…等同儕和朋友，常常支援我一些相關資源和支援，例如:電腦、學生證、作業的交流討論…等。

總而言之，很感謝能來交大唸應數研究所，這三年讓我過得非常充實，整個人也變得更是成熟不少，不管其中過得快樂或是悲傷，到後來一切都會是很好的回憶;最後就感謝我的父母和家人，提供我經濟上的消費以及心靈上的支持，謝謝大家。

Contents

Contents

1

Introduction

Definition 1.0.1. Let S denote a set of symbols. A subset $C \subseteq S^n$ is called a *code* of length n on S. The elements in C are called *codewords*. The number of codewords in C is called the *size* of C.

The thesis is about chapter 2, chapter 3, chapter 4 and chapter 5. We introduce four conclusions of the relation between geometries and codes. The first conclusion is the relation between projective geometries and super imposed codes. The second conclusion is the relation between affine geometries and super imposed codes. The third conclusion is the relation between affine geometries and Reed-Muller codes. The last conclusion is the relation between projective geometries and punctured-Reed-Muller codes. The remaining chapters introduce the Hadamard matrices, bent functions, Hexacode, extended binary Golay code and convolutional codes.

To study codes with good properties is a fascinated work in mathematics and also has many real world applications, for examples, from wire or wireless communication, experimental designs, biological group testings etc. The propose of this thesis is to study codes with more combinatorial properties involved than algebraic properties. In fact, most of the codes introduced in the thesis are related to the projective spaces and affine spaces, or some ranked posets. All of the results in this thesis are classical.

We collect results in different places and describe them in uniform and more realizable ways. We provide examples for a definition, and list some codes explicitly, e.g. Hexacodes in Chapter 7. The thesis is organized as follows.

In chapter 2, we define b^d-super-imposed codes and disjunct matrices, which can be used to construct error-tolerable designs for non-adaptive group testing, which has applications to the screening of DNA sequence, and the corresponding decoding algorithm is efficient. In chapter 3 we introduce a class of posets, called pooling spaces, which serves as the unified frame of the construction of many pooling designs. In chapter 4 and chapter 5, we introduce the Reed-Muller codes and punctured Reed-Muller codes respectively. These are classical codes but we give the connection of them with the posets in chapter 3. In the last three chapters, we introduce Hadamard matrices and bent functions, Hexacodes and Extended Binary Golay code, and convolutional codes respectively.

The following notations are used throughout the thesis.

Definition 1.0.2. For $x = (x_1, x_2, \ldots, x_n), y = (y_1, y_2, \ldots, y_n) \in S^n$, define the *distance* $\partial(x, y)$ to be the number of different positions in x, y. That is

$$\partial(x, y) := |\{i \mid x_i \neq y_i\}|.$$

Definition 1.0.3. For $C \subseteq S^n$, the *minimum distance* of C is defined by

$$d(C) := \min\{\partial(x, y) \mid x \neq y \text{ in } C\}.$$

2

Super imposed Codes

Throughout this chapter, set S={0,1}. For x=(x_1,x_2,...,x_n), y=(y_1,y_2,...,y_n)$\in S^n$, define the Boolean sum $x \cup y$ by

$$(x \cup y)_i := \begin{cases} 0, & \text{if } x_i = y_i = 0; \\ 1, & \text{else} \end{cases} \qquad \text{for } 1 \leq i \leq n.$$

2.1 Definition

Definition 2.1.1. A code $C \subseteq \{0,1\}^n$ is b^d-*super-imposed* if for any distinct codewords x, x^1, x^2, ..., $x^b \in C$, there are at least d positions with 1 values in the codeword x and 0 values in the Boolean sum $x^1 \cup x^2 \cup \cdots \cup x^b$.

We give an example as following.

Example 2.1.2. A code $C = \{(0,1,1),(1,1,0),(1,0,1)\}$ is a 1^1-super-imposed code. Suppose we choose $x = (0,1,1)$ and $x^1 = (1,1,0)$. Then in the third position x has value 1 and x^1 has value 0. Similarly for other choices of distinct elements x and x^1 in C.

Definition 2.1.3. Let $C = \{x^1, x^2, \ldots, x^m\} \subseteq \{0,1\}^n$ and $T \subseteq \{1,2,\ldots,m\}$. We define the *output* $o(T)$ of T with respect to C is $\bigcup_{i \in T} x^i$. In convention, define $o(\emptyset) = (0,0,\ldots,0)$.

Definition 2.1.4. Let C denote a b^d-super-imposed code with codewords of length n. Set

$$\bigcup^{b} C := \{o(T) \mid T \subseteq \{1, 2, \ldots, m\} \text{ with } |T| \leq b\}.$$

With the motivation from linear algebra. We give the following definition.

Definition 2.1.5. A code $C' \subset \{0,1\}^n$ is a $b-$*union* code of *dimension* m if there exists a subset $C \subseteq C'$ of size m such that $C' = \bigcup^{b} C$ and C' has size

$$\binom{m}{0} + \binom{m}{1} + \cdots + \binom{m}{b}.$$

The set C is called a *basis* of C'. C' is called the $b-$union code spanned by C.

Theorem 2.1.6. *Let C denote a b^d-super-imposed code with codewords of length n and size m. Then $\bigcup^{b} C$ is an m-dimensional $b-$union code with the basis set C and minimum distance at least d.* □

Proof. Suppose $U \neq V$ are two subsets of $\{1, 2, \ldots, m\}$ with size at most b. Then there exists $i \in (U - V) \cup (V - U)$. Without loss of generality, say $i \in U - V$. Since C is a b^d-super-imposed code, there are d positions with 1 values in x^i and 0 values in $\bigcup_{j \in V} x^j$. Then there are at least d positions with 1 values in $\bigcup_{j \in U} x^j$ and 0 values in $\bigcup_{j \in V} x^j$. Hence $\partial(o(U), o(V)) \geq d$. □

2.2 Disjunct matrices

Sometimes it is convenient to describe a code by a matrix. So we give some definitions for the code as following.

Definition 2.2.1. An $n \times s$ 01-matrix is b^d-disjunct if the set of its columns forms a b^d-super-imposed code.

Definition 2.2.2. Suppose U, V be two families consisting of subsets of $\{1, 2, \ldots, m\}$. The *incidence matrix* M between U and V is an $|U| \times |V|$ matrix with rows and columns indexed by U, V respectively such that

$$M_{ab} := \begin{cases} 1, & \text{if } a \subseteq b; \\ 0, & \text{else} \end{cases} \quad for\ a \in\ U \text{ and } b \in\ V\ .$$

Theorem 2.2.3. *Fix three integers $1 \leq u \leq v \leq m$. Let V be the family of all the v-subsets of $\{1, 2, \ldots, m\}$, and let U be the family of all the u-subsets of $\{1, 2, \ldots, m\}$. The incidence matrix between the U and V is u^1-disjunct and $(u-1)^{v-u+1}$-disjunct with size $\binom{m}{u} \times \binom{m}{v}$.*

Proof. For $x \in V$ and any other $x^1, x^2, \ldots, x^u \in V$, choose $a_i \in x - x^i$ for each $i = 1, 2, \ldots, u$. Choose $y \in U$ such that $\{a_1, a_2, \ldots, a_u\} \subseteq y \subset x$. Because $a_i \in y$ and $a_i \notin x^i$, $y \nsubseteq x^i$ for each $i = 1, 2, \ldots, u$. This proves that M is u^1-disjunct. As the above proof, there exists a $(u-1)$-subset w such that $w \subseteq x$ and $w \nsubseteq x^i$ for $i = 1, 2, \ldots, u-1$. Observe that there are $v - u + 1$ elelments y with $w \subseteq y \subseteq x$. Because $w \subseteq y$ and $w \nsubseteq x^i$, $y \nsubseteq x^i$. This proves that M is $(u-1)^{v-u+1}$-disjunct. $\square$

2.3 Decoding

Given a $b-$union code and its basis C, we give an efficient way to determine how a codeword can be write as a boolean sum of elements in C.

Definition 2.3.1. For $x, y \in \{0,1\}^n$, define $x \dot{-} y \in \{0,1\}^n$ by

$$(x \dot{-} y)_i := \begin{cases} 1, & \text{if } x_i = 1 \text{ and } y_i = 0; \\ 0, & \text{else} \end{cases} \qquad \text{for all } 1 \leq i \leq n,$$

and define $x \subseteq y$ if

$$x_i = 1 \longrightarrow y_i = 1 \qquad \text{for all } 1 \leq i \leq n.$$

Theorem 2.3.2. *Let $C = \{C_1, C_2, \dots, C_m\} \subseteq \{0,1\}^n$ be a b^d-super-imposed code, $T \subseteq \{1, 2, \dots, m\}$ with $|T| \leq b$ and $u \in \{0,1\}^n$. Set*

$$U := \{j \mid j \in \{1, 2, \dots, m\}, \partial(C_j \dot{-} u, 0) \leq \lfloor \frac{d-1}{2} \rfloor\}.$$

Then the following (1)-(2) hold.

(1) Suppose $\partial(o(T), u) \leq \lfloor \frac{d-1}{2} \rfloor$. Then $T = U$, hence $o(T) = o(U)$.

(2) Suppose $\partial(o(T), u) \leq d-1$ and $|U| \leq b$. Then $o(T) = u$ if and only if $o(U) = u$.

Proof. (1) ($T \subseteq U$) Pick $j \in T$. Then $C_j \subseteq o(T)$. Hence

$$\begin{aligned} \partial(C_j \dot{-} u, 0) &\leq \partial(o(T) \dot{-} u, 0) \\ &\leq \partial(o(T), u) \\ &\leq \lfloor \frac{d-1}{2} \rfloor. \end{aligned}$$

Hence $j \in U$.

($T \supseteq U$) Suppose $j \notin T$. Hence $\partial(C_j \dot{-} o(T), 0) \geq d$ by the b^d-super-imposed assumption. Then

$$\begin{aligned} \partial(C_j \dot{-} u, 0) &\geq \partial(C_j \dot{-} o(T), 0) - \partial(o(T), u) \\ &\geq d - \lfloor \frac{d-1}{2} \rfloor \\ &> \frac{d-1}{2}. \end{aligned}$$

Hence $j \notin U$.

(2) Suppose $T \neq U$. Then $\partial(o(T), u) > \lfloor \frac{d-1}{2} \rfloor$ by (1). In particulur, $o(T) \neq u$. Because C is a b^d-super-imposed code with codewords of length n, then $\bigcup^b C$ has minimum distance at least d by Theorem 2.1.6. Hence $\partial(o(U), o(T)) \geq d$. Then

$$\begin{aligned} \partial(o(U), u) &\geq \partial(o(U), o(T)) - \partial(o(T), u) \\ &\geq d - (d-1) = 1. \end{aligned}$$

Hence $o(U) \neq u$. $\square$

Suppose $u=o(T)$ in Theorem 2.3.2 is the codeword in the $b-$union code spanned by C. Then $u=o(U)$ is the way to write u as a boolean sum of elements in C. Some "errors" of the codewords are also allowed.

2.4 Remarks

b-super-imposed codes were introduced in 1964 by W. H. Kautz and R. C. Singleton [9], and the concept of b^d-super-imposed codes were introduced by A. J. Macula [12]. As stated in Section 2.2 a b^d-disjunct matrix is a b^d-super-imposed code in matrix language. The b^d-disjunct matrix can be used to construct an error-tolerable design for non-adaptive group testing, which has applications to the screening of DNA sequence, and the corresponding decoding algorithm is efficient. See [3], [6] for details. A b^d-disjunct matrix is also called a *pooling design*.

The constructions of b^d-disjunct matrices were given by many authors, e.g. [11], [12], [13], [4]. Theorem 2.2.3 is a special case of [7]. The algorithm in Theorem 2.3.2 was given in [6]. See [4] for more results of this line of study.

3

Pooling spaces

We constructed disjunct matrices from the lattice of subsets of a given set in Theorem 2.2.3. We generalize the idea to poset in this chapter.

3.1 Preliminaries

We now give the basic definitions and properties of a partially ordered set. The expert may want to skip the remaining of this section and go to the next section.

Let P denote a finite set. By a *partial order* on P, we mean a binary relation $\leq$ on P such that

(i) $x \leq x \qquad \forall\ x \in P$,

(ii) $x \leq y$ and $y \leq z \quad \longrightarrow \quad x \leq z \qquad \forall\ x, y, z \in P$,

(iii) $x \leq y$ and $y \leq x \quad \longrightarrow \quad x = y \qquad \forall\ x, y \in P$.

By a *partially ordered set* (or *poset*, for short), we mean a pair $(P, \leq)$, where P is a finite set, and where $\leq$ is a partial order on P. By abusing notation, we will suppress reference to $\leq$, and just write P instead of $(P, \leq)$.

Let P denote a poset, with partial order $\leq$, and let x and y denote any elements in P. As usual, we write $x < y$ whenever $x \leq y$ and $x \neq y$, and write $x \not< y$ whenever $x < y$ is not true. We say y *covers* x whenever $x < y$, and there is no $z \in P$ such that $x < z < y$. A poset can be described by a diagram in which the elements are corresponding to dots, and y covers x whenever dot y is placed above dot x with an edge connecting them. See Fig. 1 for the diagram of the poset with five elements $\{0, w, x, y, z\}$, and w, x covers 0; y covers w, x; z covers w, x respectively. Note $0, w, y$ is a direct chain of length 2.

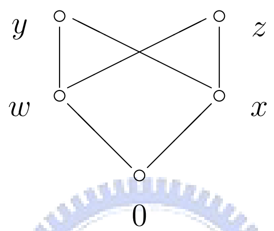

Figure 1. A poset.

An element $x \in P$ is said to be *minimal* (resp. *maximal*) whenever there is no $y \in P$ such that $y < x$ (resp. $x < y$). Let $\min(P)$ (resp. $\max(P)$) denote the set of all minimal (resp. maximal) elements in P. Whenever $\min(P)$ (resp. $\max(P)$) consists of a single element, we denote it by 0 (resp. 1), and we say P has *the least element* 0 (resp. *the greatest element* 1).

Throughout the chapter 2 we assume P is a poset with the least element 0. By an *atom* in P, we mean an element in P that covers 0. We let A_P denote the set of atoms in P. By a *rank function* on P, we mean a function rank from P to the set of nonnegative integers such that $\mathrm{rank}(0) = 0$, and such that for all $x, y \in P$, y covers x implies $\mathrm{rank}(y) - \mathrm{rank}(x) = 1$. Observe the rank function is unique if it exists. P is said to be *ranked* whenever P has a rank function. In this case, we set

$$\mathrm{rank}(P) := \max\{\mathrm{rank}(x) | x \in P\},$$

$$P_i := \{x|x \in P, \mathrm{rank}(x) = i\},$$

and observe $P_0 = \{0\}$, $P_1 = A_P$. Observed P is ranked if and only if for any $x \in P$ every direct chain from 0 to x has the same length.

Let P denote any finite poset, and let S denote any subset of P. Then there is a unique partial order on S such that for all $x, y \in S$, $x \le y$ in S if and only if $x \le y$ in P. This partial order is said to be *induced* from P. By a *subposet* of P, we mean a subset of P, together with the partial order induced from P. Pick any $x, y \in P$ such that $x \le y$. By the *interval* $[x, y]$, we mean the subposet

$$[x, y] := \{z|z \in P, x \le z \le y\}$$

of P.

P is said to be *atomic* whenever for each element x of P, x is the join of atoms in the interval $[0, x]$. Suppose P is atomic and $x < y$ are two elements in P. Observe the atoms in the interval $[0, x]$ is a proper subset of atoms in the interval $[0, y]$.

Let P denote any poset, and S be a subset of P. Fix $z \in P$. Then z is said to be an *upper bound* (resp. *lower bound*) of S, if $z \ge x$ (resp. $z \le x$) for all $x \in S$. Suppose the subposet of upper bounds (resp. lower bounds) of S has a unique minimal (resp. maximal) element. In this case we call this element *the least upper bound* or *join* (resp. *the greatest lower bound* or *meet*) of S. If $S = \{x_1, x_2, \ldots, x_t\}$ we write $x_1 \vee\ x_2 \vee \cdots \vee x_t$ for the join of S and $x_1 \wedge x_2 \wedge \cdots \wedge x_t$ for the meet of S. P is said to be *meet semi-lattice* (resp. *join semi-lattice*) whenever P is nonempty, and $x \wedge y$ (resp. $x \vee y$) exists for all $x, y \in P$. A meet semi-lattice (resp. *join semi-lattice*) has a 0 (resp. 1). A meet and join semi-lattice is called a lattice.

Suppose P is a lattice. Then P is said to be *upper semi-modular* (resp. *lower semi-modular*) whenever for all $x, y \in P$,

$$y \text{ covers } x \wedge y \quad \longrightarrow \quad x \vee y \text{ covers } x$$

$$(\text{resp. } x \vee y \text{ covers } x \quad \longrightarrow \quad y \text{ covers } x \wedge y).$$

P is said to be *modular* whenever P is upper semi-modular and lower semi-modular.

3.2 Definitions

Now we can give the main definition of the chapter as following.

Definition 3.2.1. Let P be a ranked poset. For any $w \in P$, define

$$w^+ = \{y \geq w \mid y \in P\}.$$

P is said to be a *pooling space* whenever w^+ is atomic for all $w \in P$.

In particular, a pooling space is atomic. It is immediate from the definition that if P is a pooling space, then so is w^+ for any $w \in P$. The following theorem is a generalization of Theorem 2.2.3.

Theorem 3.2.2. *Let P be a pooling space with rank $D \geq 1$. Fix an element $x \in P_D$ and fix an integer b $(1 \leq b \leq D)$. Let $T \subseteq P_D$ be a subset such that $|T| \leq b$ and $x \notin T$. Then there exists an element $y \in [0, x] \cap P_b$ such that $y \not\leq z$ for all $z \in T$.*

Proof. We prove the theorem by induction on D. If $D = 1$ then $b = 1$ and the theorem holds by setting $y = x$. In general, pick an element $z \in T$. Then $x \neq z$ by assumption. Since x is the least upper bound of $[0, x] \cap P_1$ and $x \not\leq z$, z is not an upper bound of $[0, x] \cap P_1$. Hence we can pick an element $w \in [0, x] \cap P_1$ such that $w \not\leq z$. Then $T \cap w^+$ has at most $b - 1$ elements. In the pooling space w^+, the element x and the elements of $T \cap w^+$ all have rank $D - 1$, and the elements of $w^+ \cap P_b$ have rank $b - 1$. Hence by induction, we can choose $y \in [w, x] \cap P_b$ such that $y \not\leq u$ for all $u \in T \cap w^+$. Note that clearly $y \not\leq u$ for all $u \in T \setminus w^+$. This proves the theorem. $\square$

3.3 The contractions of a graph

Many examples of pooling spaces were given in [7]. These are related the Hamming matroid, the attenuated space, and six classical polar spaces. Among these examples there is a common property: each interval is modular. In this section we will construct pooling spaces without modular intervals. Throughout the section let G denote a simple connected graph on n vertices.

Definition 3.3.1. Let $P = P(G)$ denote the set of partitions A of the vertex set $V(G)$ such that the subgraph induced by each block of A is connected. For $A, B \in P$, define

$$A \leq B \Longleftrightarrow A \text{ is a refinment of } B.$$

The poset $(P(G), \leq)$ is called the poset of *contractions* of G.

Example 3.3.2. Let G denote a graph with the vertex set $\{w, x, y, z\}$ and edge set $\{\overline{wx}, \overline{xy}, \overline{yz}, \overline{zw}\}$, i.e. G is the 4-cycle C_4. Then the poset $P(G)$ is as in Fig. 2. We delete the single element blocks in the notation of a partition. e.g. the notation 0 is used to denote the partition with four blocks $\{w\}, \{x\}, \{y\}$, $\{z\}$, and $\overline{wx}$ is used to denote the partition with three blocks $\{w, x\}$, $\{y\}$, $\{z\}$. The poset is a lattice, but not a modular lattice. This is because the join of the elements $\overline{wx}\ \overline{yz}$ and $\overline{xy}\ \overline{zw}$ is $\overline{wxyz}$, which covers $\overline{wx}\ \overline{yz}$, but $\overline{xy}\ \overline{zw}$ does not covers the element 0 which is the meet of the elements $\overline{wx}\ \overline{yz}$ and $\overline{xy}\ \overline{zw}$. Observe the subposet induced on $\overline{wx}^+$ is $P(C_3)$, the poset of contractions of a triangle.

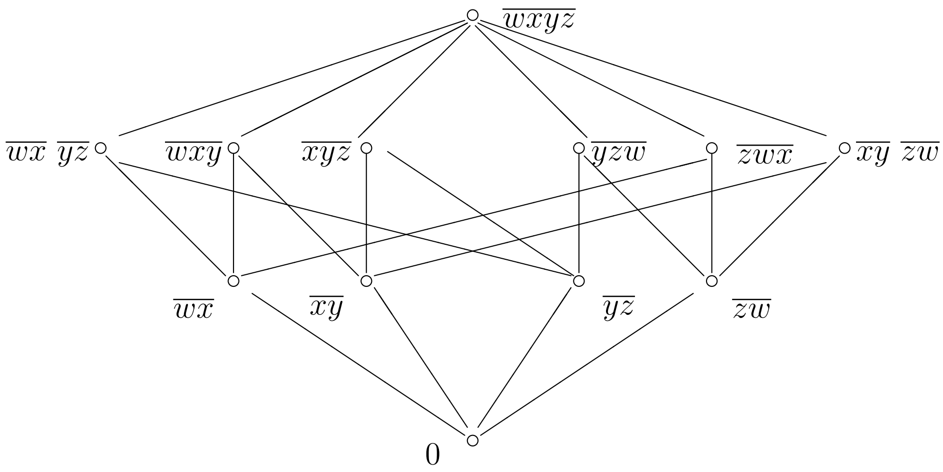

Figure 2. $P(C_4)$.

Lemma 3.3.3. *$P(G)$ is a ranked poset of rank $n-1$. The rank i elements are those elements in $P(G)$ with $n-i$ blocks for $0 \leq i \leq n-1$.*

Proof. For $D \in P(G)$ with $n-i$ blocks define the rank of D to be i, where $0 \leq i \leq n-1$. We claim this is a rank function. Suppose that B covers A and rank(A) $= i$. Since A is a proper refinement of B, rank$(B) \geq i+1$ and there are two blocks in A that are contained in the same block of B. Let C be an element in $P(G)$ that glues these two blocks of A. Then $A < C \leq B$ and rank$(C) =$ rank$(A)+1$. This shows $C = B$ and rank$(B) = i+1$. □

Theorem 3.3.4. *$P(G)$ is a pooling space of rank $n-1$.*

Proof. $P(G)$ is ranked by previous lemma. From previous lemma and the definition each atom in P(G) contains $n-1$ blocks, one block containing two adjacent vertices and each of the remaining $n-2$ blocks containing a single vertex. By identifying the atoms with the edges of G we find each element $A \in P(G)$ is the join of those edges contained in the subgraph of G induced by A. This shows that $P(G)$ is atomic. More generally, for $B \in P(G)$, the poset B^+ is also atomic. This is because the subposet B^+ is isomorphic to the poset $P(B_G)$ of contractions of B_G, where B_G is the graph with the vertex set B, and for two distinct blocks $x, y \in B$ x is adjacent to y whenever some vertex in x is adjacent to some vertex in y. □

Remark 3.3.5. Let $G = K_n$ denote the complete graph on n vertices. Then the elements in $P = P(K_n)$ are all the partitions of the vertex set of K_n. $S(n, k) := |P_k|$ is called the *Stirling number of the second kind.* It is well known that $S(n, k)$ can be solved by the recurrence relation

$$S(n, k) = S(n-1, k-1) + kS(n-1, k) \qquad \text{for } 1 \leq k \leq n-1$$

with initial condition $S(n, 0) = 0$ for $n \geq 1$, and $S(n, n) = 1$ for $n \geq 0$. See [2, Section 8.2] for details.

3.4 Finite fields

Before going farther, we need some background on finite fields. Recall that a *finite field* F_q is a set of q elements containing 0,1 with two binary relations $+$, $\cdot$, such that $(F_q\ , +\ , 0)$ and $(F_q^*\ , \cdot\ , 1)$ are abelian groups, and $+$, $\cdot$ satisfy distribute law, where $F_q^*{:=}F_q - \{0\}$.

We give some examples as following.

Example 3.4.1. $\{0, 1, 2, 3\}$ is not a finite field under ususal $+$, $\cdot$ (mod 4), since 2 does not have the multiplication inverse.

Example 3.4.2. $F_4 = \{0, 1, x, x + 1\}$ is a finite field under $+$, $\cdot$ (mod $x^2 + x + 1$).

It is well-known that the finite field F_q of q elements is unique up to isomorphism, and $q = p^r$ for some prime p. There are two ways to describe F_q:

(i) $F_q = \{a_0 + a_1x + a_2x^2 + \cdots + a_{r-1}x^{r-1} \mid a_i \in Z_p\}$,

(ii) $F_q = \{0, 1, \gamma, \gamma^2, \cdots, \gamma^{q-2}\}$.

The $+$ defined in (i) is as usual, and $\cdot$ is defined mod some irreducible polynomial $g(x) \in F_q[x]$ of degree r, e.g. $g(x) = x^2 + x + 1$ in Example 3.4.2. The $\cdot$ defined in (ii) is as usual with the condition $\gamma^{q-1} = 1$ and the $+$ is defined mod $g(x)$. γ is called a *primitive element* of F_q.

Example 3.4.3. $F_4 = \{0, 1, x, x+1\} = \{0, 1, x, x^2\} \pmod{x^2 + x + 1}$.

Example 3.4.4. $F_5 = \{0, 1, 2, 3, 4\} = \{0, 1, 2, 2^2, 2^3\} \pmod 5$.

Note 3.4.5. F_q is the set of solutions of $x(x^{q-1} - 1) = 0$.

Note 3.4.6. Suppose $q = p^r$ for some prime p. Then F_q is a vector space over F_p.

Lemma 3.4.7. *Suppose $T \subseteq F_{p^m}$ is a subspace over F_p. Then γT is a subspace over F_p for any $\gamma \in F_{p^m}$.*

Proof. This is clear for $\gamma = 0$. Suppose $\gamma \neq 0$, and suppose $\alpha_1, \alpha_2, \ldots, \alpha_k$ is a basis of T. Then $\gamma\alpha_1, \gamma\alpha_2, \ldots, \gamma\alpha_k$ is a basis of γT. □

3.5 Projective and affine geometries

We introduce two more examples of pooling spaces in this section.

Definition 3.5.1. The *projective geometry* $PG(n, q)$ is the poset consisting of all subspaces of F_q^n with order defined by inclusion. The elements in P_i are referred to the *i-subspaces* of F_q^n for $i = 0, 1, 2, \cdots, n$.

The following is from linear algebra.

Note 3.5.2. $\dim(U + V) + \dim(U \cap V) = \dim(U) + \dim(V)$ for $U, V \in PG(n, q)$.

Definition 3.5.3. Consider the n-dimensional space F_q^n where q is a prime or a prime power. Let $\begin{bmatrix} n \\ k \end{bmatrix}_q$ denote the number of k-subspaces of F_q^n. In convention, define $\begin{bmatrix} n \\ k \end{bmatrix}_q = 0$, if $k > n$ or $k < 0$.

We list a few properties for $\begin{bmatrix} n \\ k \end{bmatrix}_q$.

Lemma 3.5.4.

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)} \text{ for } 0 \le k \le n.$$

Proof. We prove the statement by induction on k.

$\begin{bmatrix} n \\ 0 \end{bmatrix}_q = 1$ is clear since $\{0\}$ is the only one subspace of dimension 0, and

$$\begin{bmatrix} n \\ 1 \end{bmatrix}_q = \frac{q^n-1}{q-1}$$

since there are $q^n - 1$ nonzero vectors in F_q^n and each 1-subspace containing $q-1$ nonzero vectors.

In general, by counting the number of pairs (W, V), where $W \subseteq V$ are $(k-1)$-subspaces, k-subspaces respectively in two ways, we find

$$\begin{bmatrix} n \\ k-1 \end{bmatrix}_q \begin{bmatrix} n-k+1 \\ 1 \end{bmatrix}_q = \begin{bmatrix} n \\ k \end{bmatrix}_q \begin{bmatrix} k \\ k-1 \end{bmatrix}_q.$$

Hence

$$\begin{aligned} \begin{bmatrix} n \\ k \end{bmatrix}_q &= \frac{\begin{bmatrix} n \\ k-1 \end{bmatrix}_q \begin{bmatrix} n-k+1 \\ 1 \end{bmatrix}_q}{\begin{bmatrix} k \\ k-1 \end{bmatrix}_q} \\ &= \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)} \end{aligned}$$

by induction hypothesis. □

Lemma 3.5.5.

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \begin{bmatrix} n \\ n-k \end{bmatrix}_q \text{ for } 0 \le k \le n.$$

Proof. By Lemma 3.5.4,

$$\begin{aligned}
\begin{bmatrix} n \\ n-k \end{bmatrix}_q &= \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{k+1}-1)}{(q^{n-k}-1)(q^{n-k-1}-1)\cdots(q-1)} \cdot \frac{(q^k-1)(q^{k-1}-1)\cdots(q-1)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)} \\
&= \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-k+1}-1)}{(q^k-1)(1^{k-1}-1)\cdots(q-1)} \\
&= \begin{bmatrix} n \\ k \end{bmatrix}_q .
\end{aligned}$$

□

Lemma 3.5.6.

$$\begin{bmatrix} k \\ r \end{bmatrix}_q - \begin{bmatrix} k-1 \\ r \end{bmatrix}_q = q^{k-r} \begin{bmatrix} k-1 \\ r-1 \end{bmatrix}_q \quad \text{for } 0 \le r < k.$$

Proof.

$$\begin{aligned}
&\begin{bmatrix} k \\ r \end{bmatrix}_q - \begin{bmatrix} k-1 \\ r \end{bmatrix}_q \\
= \;& \frac{(q^k-1)(q^{k-1}-1)\cdots(q^{k-r+1}-1)}{(q^r-1)(q^{r-1}-1)\cdots(q-1)} - \frac{(q^{k-1}-1)(q^{k-2}-1)\cdots(q^{k-r}-1)}{(q^r-1)(q^{r-1}-1)\cdots(q-1)} \\
= \;& \frac{(q^k-1)-(q^{k-r}-1)}{q^r-1} \cdot \frac{(q^{k-1}-1)\cdots(q^{k-r+1}-1)}{(q^{r-1}-1)\cdots(q-1)} \\
= \;& q^{k-r} \begin{bmatrix} k-1 \\ r-1 \end{bmatrix}_q .
\end{aligned}$$

□

The following theorem will be used in the next section to construct super-imposed codes.

Theorem 3.5.7. *Fix integers $0 \le r < k \le n$. Let $A, A_1, A_2, \ldots, A_b$ be distinct k-subspaces of F_q^n. Then there are at least*

$$d := q^{k-r} \begin{bmatrix} k-1 \\ r-1 \end{bmatrix}_q - (b-1)q^{k-r-1} \begin{bmatrix} k-2 \\ r-1 \end{bmatrix}_q \tag{3.5.1}$$

r-subspaces of A which are not contained in each A_i for $i = 1, 2, \cdots, b$.

Proof. To obtain the maximum elements of r-subspaces in $A \cap A_i$, we assume $\dim(A \cap A_i) = k-1$ for all $i = 1, 2, \cdots, b$. If $A \cap A_i \neq A \cap A_j$, then $(A \cap A_i) + (A \cap A_j) = A$ and the dimension of $(A \cap A_i) \cap (A \cap A_j)$ is $k-2$. Hence there are at least

$$\begin{aligned} d &:= \begin{bmatrix} k \\ r \end{bmatrix}_q - \begin{bmatrix} k-1 \\ r \end{bmatrix}_q - (b-1)(\begin{bmatrix} k-1 \\ r \end{bmatrix}_q - \begin{bmatrix} k-2 \\ r \end{bmatrix}_q) \\ &= q^{k-r} \begin{bmatrix} k-1 \\ r-1 \end{bmatrix}_q - (b-1)q^{k-r-1} \begin{bmatrix} k-2 \\ r-1 \end{bmatrix}_q . \end{aligned}$$

r-subspaces of A which are not contained in each A_i for $i = 1, 2, \cdots, b$. $\square$

Corollary 3.5.8. *In Theorem 3.5.7. If $1 < r \leq \frac{k}{2}$, then $b = q^r + 1$ is the largest integer such that $d > 0$. If $r = 1$, then $b = q$ is the largest integer such that $d > 0$.*

Proof. Suppose $r > 1$. Then $d > 0 \Leftrightarrow$

$$\begin{aligned} b - 1 &< q \begin{bmatrix} k-1 \\ r-1 \end{bmatrix}_q \Big/ \begin{bmatrix} k-2 \\ r-1 \end{bmatrix}_q \\ &= q \cdot \frac{(q^{k-1}-1)(q^{k-2}-1)\cdots(q^{k-r+1}-1)}{(q^{k-2}-1)(q^{k-3}-1)\cdots(q^{k-r}-1)} \\ &= \frac{q(q^{k-1}-1)}{(q^{k-r}-1)} \\ &= \frac{q^k - q - q^k + q^r}{q^{k-r}-1} + q^r \\ &= \frac{q(q^{r-1}-1)}{q^{k-r}-1} + q^r . \end{aligned}$$

Since

$$r \leq \frac{k}{2},$$

$$0 < \frac{q(q^{r-1}-1)}{q^{k-r}-1} < 1.$$

Hence $b \leq q^r + 1$.

Suppose $r = 1$. Then

$$\begin{aligned} d > 0 &\iff b - 1 < q \\ &\iff b \leq q. \end{aligned}$$

$\square$

Note 3.5.9. Since $\begin{cases} b \leq q, & \text{r=1;} \\ b \leq \begin{bmatrix} 2 \\ 1 \end{bmatrix}_q = q+1, & \text{r}\geq 2 \end{cases}$, we can choose $A, A_1, A_2, \cdots, A_b$ such that $A \cap A_i \neq A \cap A_j$ for $i \neq j$, dim($A \cap A_i$)=$k-1$ for every i=1,2,$\cdots$,b and their meet is a $(k-2)-$subspace. Then there are exactly d r-subspaces of A which are not contained in any A_i for $i = 1, 2, \cdots, b$ and d is defined in (3.5.1).

Now we consider the relation of projective geometry.

Definition 3.5.10. Let F_q^n denote an n-dimensional vector space over a finite field F_q, where q is the number of elements in the field. Let $P = P(F_q^n)$ denote the poset with element set

$$P = \{u + W \mid u \in F_q^n \text{ and } W \subseteq F_q^n \text{ is a subspce}\} \cup \{\emptyset\},$$

where $\emptyset$ denote the empty set. The order is defined by inclusion. Note that P is a geometric lattice of rank $n+1$. P is called the *affine geometry* and is denoted by $AG(n, q)$. The elements in P_i are referred to the *affine* $(i-1)$-*subspaces* of F_q^n for $i = 1, 2, \cdots, n+1$. We say the affine subspaces $u + W$ and $v + W$ are *parallel* for $u, v \in F_q^n$, $W \subseteq F_q^n$ is a subspace.

We immediately have the following lemma.

Lemma 3.5.11. *Suppose $u_1, u_2 \in F_q^n$ and $W_1, W_2 \subseteq F_q^n$ are subspaces. Then $u_1 + W_1 = u_2 + W_2$ if and only if $W_1 = W_2$ and $u_1 - u_2 \in W_1$.* $\square$

Now we have a similar version of Theorem 3.5.7

Lemma 3.5.12. *Let A denote an affine k-subspaces of F_q^n. Then the number of affine r-subspaces contained in A is*

$$q^{k-r}\begin{bmatrix} k \\ r \end{bmatrix}_q,$$

where $r < k$. These affine r-subspaces in A are partitioned into

$$\begin{bmatrix} k \\ r \end{bmatrix}_q$$

classes, each class consisting of q^{k-r} parallel affine subspaces. □

Theorem 3.5.13. *Fix integers $1 \le r < k \le n$. Let $A, A_1, A_2, \ldots, A_b$ be distinct affine k-subspaces of F_q^n. Then there are at least*

$$d := q^{k-r}\begin{bmatrix} k \\ r \end{bmatrix}_q - bq^{k-r-1}\begin{bmatrix} k-1 \\ r \end{bmatrix}_q \tag{3.5.2}$$

affine r-subspaces contained in A and not contained in any of A_i for $i = 1, 2, \cdots, b$.

Proof. There are

$$q^{k-r}\begin{bmatrix} k \\ r \end{bmatrix}_q$$

affine r-subspaces contained in A, some of them in some affine subspace $A \cap A_i$ for each $i = 1, 2, \cdots, b$ to be deducted. $A \cap A_i$ takes maximal coverage of these affine r-subspaces when $A \cap A_i$ is an affine $(k-1)$-subspace, and in this situation the number of these affine r-subspaces is

$$q^{(k-1)-r}\begin{bmatrix} k-1 \\ r \end{bmatrix}_q.$$

□

Corollary 3.5.14. *In Theorem 3.5.13, if* $0 < r < \frac{k}{2}$*, then* $b = q^{r+1}$ *is the largest integer such that* $d > 0$*; if* $r = 0$*, then* $b = q-1$ *is the largest integer such that* $d > 0$*.*

Proof. $d > 0 \Longleftrightarrow$

$$\begin{aligned} b &< q \begin{bmatrix} k \\ r \end{bmatrix}_q \Big/ \begin{bmatrix} k-1 \\ r \end{bmatrix}_q \\ &= q \cdot \frac{(q^k-1)(q^{k-1}-1)\cdots(q^{k-r+1}-1)}{(q^{k-1}-1)(q^{k-2}-1)\cdots(q^{k-r}-1)} \\ &= \frac{q(q^k-1)}{(q^{k-r}-1)} \\ &= \frac{q^{k+1}-q-q^{k+1}+q^{r+1}}{q^{k-r}-1} + q^{r+1} \\ &= \frac{q(q^r-1)}{q^{k-r}-1} + q^{r+1} \end{aligned}$$

Since

$$0 < r < \frac{k}{2},$$

Then

$$\frac{q(q^r-1)}{q^{k-r}-1} < 1.$$

Hence $0 < b \le q^{r+1}$.

Suppose $r = 0$. Then

$$\begin{aligned} d > 0 &\Longleftrightarrow b < q \\ &\Longleftrightarrow b \le q-1 \end{aligned}$$

□

Note 3.5.15. Since $\begin{cases} b \le q-1, & \text{r=0;} \\ b \le q, & \text{r}\ge 1 \end{cases}$ and $k \le n$, we can choose A_i to be an affine $k-$subspace with the meet with A corresponding to each of the q parallel affine $(k-1)-$subspaces in A. Then there is exactly d affine $r-$subspaces contained in A and not contained in any of A_i for $i = 1, 2, \cdots, b$ and d is defined in (3.5.2).

3.6 Codes on projective and affine geometries

We are clearly to apply the results in the section 3.5 to construction of super-imposed codes as following.

Definition 3.6.1. Let $P_q(n, k, r)$ denote the incidence matrix of the set of r-subspaces and the set of k-subspaces in F_q^n for $1 \leq r \leq k \leq n$. The following corollary is immediate from Theorem 3.5.7, Corollary 3.5.8 and Note 3.5.9.

Corollary 3.6.2. *The columns of $P_q(n, k, r)$ form a b^d-super-imposed code, but not a b^{d+1}-super-imposed code, where b is a positive integer satisfying*

$$\begin{cases} b \leq q, & r{=}1; \\ b \leq q+1, & r{\geq}2, \end{cases}$$

$k \leq n$ and d is defined in (3.5.1).

Definition 3.6.3. Let $A_q(n+1, k+1, r+1)$ denote the incidence matrix for of the set of affine r-subspaces and the set of affine k-subspaces in F_q^n $0 \leq r \leq k \leq n$. The following Corollary is immediate from Theorem 3.5.13, Corollary 3.5.14 and Note 3.5.15.

Corollary 3.6.4. *The columns of $A_q(n+1, k+1, r+1)$ form a b^d-super-imposed code, but not a b^{d+1}-super-imposed code, when b is a positive integer satisfying*

$$\begin{cases} b \leq q-1, & r{=}0; \\ b \leq q, & r{\geq}1, \end{cases}$$

$k \leq n$ and d is defined in (3.5.2).

We set $r = 0$ and $b = q - 1$ to obtain the following result.

Corollary 3.6.5. *Let $A_q(3, 2, 1)$ be the incidence matrix of the set of affine 0-subspaces and the set of affine 1-subspaces in F_q^2. Then the columns of $A_q(3, 2, 1)$ are $(q-1)^1$-super-imposed code.* □

3.7 Sperner's theorem and EKR theorem

We list two interesting classical theorems in this section as following.

Theorem 3.7.1. *(Sperner's Theorem)Let M be an $n \times s$ 1-disjunct matrix. Then*

$$s \leq \binom{n}{\lfloor \frac{n}{2} \rfloor}.$$

Proof. Let P be the poset consisting of subsets of $\{1, 2, \cdots, n\}$ with order defined by inclusion. For each column x of M, identify x to the element $\{i \mid x_i = 1\}$ of P. Then the set F of columns of M becomes an antichain in P. (i.e. $x \nsubseteq x'$ for any $x \neq x'$.) Set $\alpha_k := |\{x \in F \mid |x| = k\}|$ for $k = 0, 1, 2, \cdots, n$. Note $|F| = \sum_{k=0}^{n} \alpha_k$. Observe there are $n!$ maximal chains in P. Observe there are $k!(n-k)!$ maximal chains containing a fixed $x \in P$ with $|x| = k$. Observe for any chain L. $|L \cap F| \leq 1$. By counting the pairs (x, L) where $x \in F$, $x \in L$ and L is a maximal chain. We find

$$\sum_{k=0}^{n} \alpha_k k!(n-k)! \leq 1 \cdot n!.$$

Then

$$\sum_{k=0}^{n} \alpha_k \binom{n}{k}^{-1} \leq 1.$$

Hence

$$\sum_{k=0}^{n} \alpha_k \binom{n}{\lfloor \frac{n}{2} \rfloor}^{-1} \leq 1.$$

Thus,

$$s = \sum_{k=0}^{n} \alpha_k \leq \binom{n}{\lfloor \frac{n}{2} \rfloor}$$

□

Theorem 3.7.2. *(EKR-Theorem) Let A be a collection of s distinct k-subsets of $\{1, 2, \cdots, n\}$, where $k \leq \frac{n}{2}$, with the property that any two of the subsets have a* *nonempty intersection. Then*

$$s \leq \binom{n-1}{k-1}.$$

Proof. For a permutation σ of $\{1, 2, \cdots, n\}$, and $T \in A$, define $\sigma(T) := \{\sigma(x)|x \in T\}$ and $A^\sigma := \{\sigma(T)|T \in A\}$. Set $S_i := \{i, i+1, \cdots, i+k-1\}$ mod n for $i = 1, 2, \cdots, n$ and $F := \{S_1, S_2, \cdots, S_n\}$. Observe for each $S_i \in F$, there are $2k-1$ $S_j \in F$ with $S_i \cap S_j \neq \emptyset$. These are $S_{i-(k-1)}$,$S_{i-(k-2)}$,$\cdots$,S_i, S_{i+1},$\cdots$,S_{i+k-1}. Divide these into k boxes $\{S_{i-(k-1)}, S_{i+1}\}$,$\{S_{i-k-2}, S_{i+2}\}$,$\cdots$, $\{S_{i-1}, S_{i+k-1}\}$,$\{S_i\}$. Any two in the same boxes have empty intersection. Hence we can choose only one. From this observation we have $|A \cap F| \leq k$. Also $|A^\sigma \cap F| \leq k$ for any permutation σ. We count (S, T, σ) in two ways, where $S \in F$, $T \in A$, σ is a permutation with $\sigma(T) = S$, $S \in A^\sigma \cap F$ and $T = \sigma^{-1}(S)$, in the orders S,T,σ and σ,S,T to find

$$n \cdot s \cdot k!(n-k)! \leq n! \cdot k.$$

Hence

$$s \leq \frac{(n-1)!}{(k-1)!(n-k)!} = \binom{n-1}{k-1}.$$

□

Definition 3.7.3. Let P be a ranked poset of rank n and $1 \leq k \leq n$ be an integer. We say P has the k^{th} EKR property whenever any family $F \subseteq P_k$ such that for any $x, y \in F$ there exists $a \neq 0$ with $a \leq x$ and $a \leq y$, we always have $|F| \leq |w^+ \cap P_k|$ for some $w \in P_1$.

Conjecture 3.7.4. EKR property holds on a geometric lattice.

3.8 Remarks

The name pooling spaces was given in [7]. Theorem 3.3.4 was proved in [8]. Theorem 3.5.7 was given in [4] with a minor correction. Theorem 3.5.13 was given in [8].

Theorem 3.7.1 and Theorem 3.7.2 are well known and have many different proofs. We follow the proofs from [10, Chapter 6].

4

Reed-Muller Codes

For the remaining of the thesis, we consider the codes defined with more algebraic aspect, but it turns out these codes also have combinatorial meaning.

4.1 Linear Codes

Definition 4.1.1. A code $C \subseteq F_q^n$ is a $[n, k, d]$-*linear code* (or $[n, k]$-*linear code*) if C is a subspace of F_q^n with dimension k and minimum distance d.

Definition 4.1.2. For any $x \in C$, the weight $wt(x)$ of x is the number of nonzero coordinates in x. The minimum weight $wt(C)$ of C is

$$wt(C) := min\{w(x) \mid x \in C,\ x \neq 0\}.$$

In general the weight of an element in F_q^n depends on how the basis is chosen. In the above definition the weight is associated with the standard basis of F_q^n. We might choose different basis and define the weight differently. Because the distance of codewords have relation with the weight.

Note 4.1.3. The distance $\partial(x, y)$ between the codeword x and y is $wt(x - y)$ for any $x, y \in C$.

Note 4.1.4. We say C is a linear code if and only if $x - y \in C$ and $\alpha x \in C$ for any $x, y \in C$ and scalar α.

Note 4.1.5. If C is linear code, then the weight $wt(C)$ is equal to the minimum distance $d(C)$.

Note 4.1.6. The concept of weight of a code indeed depends on the chosen basis of vector space.

4.2 Reed-Muller Codes

At first, we give the definition of the codes considered in this chapter.

Definition 4.2.1. We define R_m :=$\{f \mid f : F_2^m \longrightarrow F_2$ is a function$\}$, where R_m is called the *Reed-Muller code* of order m.

The following two notes are clear.

Note 4.2.2. The Reed-Muller code is a vector space under usual $+, \cdot$ operations of functions.

Note 4.2.3. The Reed-Muller code of order m is a vector space over F_2 of dimension 2^m and $|R_m| = 2^{2^m}$.

We consider a few special functions in R_m.

Definition 4.2.4. For $1 \leq i \leq m$, we define $x_i \in R_m$ such that for any $u \in F_2^m$, $x_i(u) = 1 \Longleftrightarrow u_i = 1$, and define $1 \in R_m$ such that for any $u \in F_2^m$, $1(u) = 1$.

Definition 4.2.5. $x_{i_1} x_{i_2} \cdots x_{i_j} \in R_m$ is called a *monomial of degree j* where $1 \leq j \leq m$ and $1 \leq i_1, i_2, \cdots, i_j \leq m$ are distinct integers. 1 is called a monomial of degree 0.

We identify 0,1,2,$\cdots$,$2^m - 1$ with the elements in F_2^m by using binary expressions, e.g. $0 = (0, 0, \cdots, 0)$, $1 = (1, 0, \cdots, 0, 0)$, $2 = (0, 1, 0, \cdots, 0,)$,$\cdots$. We choose a *standard basis* $f_0, f_1, \cdots, f_{2^m-1}$ of R_m, where $f_i(j) = 1$ if and only if $j = i$ for $0 \leq i \leq 2^m - 1$. We use the standard basis to express the codeword $f \in R_m$, so the weight of f has the following meaning.

Note 4.2.6. Suppose the function $f \in R_m$. Then $f^2 = f$ and the weight $wt(f)$ is equal to $|f^{-1}(1)|$.

We consider the weight of a monomial as following note.

Note 4.2.7. Suppose $f = x_1 x_2 \cdots x_r$.Then

$$f^{-1}(1) = \{(1, 1, \cdots, 1, a_{r+1}, a_{r+2}, \cdots, a_m) \mid a_i = 0 \text{ } or \text{ } 1\}$$

is a affine $(m-r)$-subspace of F_2^m. Hence $wt(x_1 x_2 \cdots x_r) = 2^{m-r}$.

We find a basis of R_m.

Theorem 4.2.8. *The set of monomials with degree less or equal m forms a basis of the Reed-Muller code of order m.*

Proof. There are $\begin{pmatrix} m \\ 0 \end{pmatrix} + \begin{pmatrix} m \\ 1 \end{pmatrix} + \cdots + \begin{pmatrix} m \\ m \end{pmatrix} = 2^m$ monomials and $\dim(R_m) = 2^m$. It suffice to show monomials span R_m. Suppose $f \in R_m$. Observe

$$f = \sum_{a \in f^{-1}(1)} \prod_{j=1}^{m} (x_j + a_j + 1).$$

Hence f is spanned by monomials. $\square$

We consider Reed-Muller codes in the light of monomials.

Definition 4.2.9. $RM(r, m)$:=$\{f \in R_m \mid f$ is spanned by monomials of degree $\leq r\}$ where $r \leq m$. $RM(r, m)$ is called the *r-th Reed- Muller Code* of order m. Let wt_m denote the *weight function* on $RM(r, m)$.

From Theorem 4.2.8 and Definition 4.2.9, we have

Note 4.2.10. Since $RM(r,m)$ is a linear code with codewords of length 2^m, the dimension is $\dim RM(r,m) = \begin{pmatrix} m \\ 0 \end{pmatrix} + \begin{pmatrix} m \\ 1 \end{pmatrix} + \cdots + \begin{pmatrix} m \\ r \end{pmatrix}$.

Theorem 4.2.11. *The minimum distance $d(RM(r,m))$ is equal to 2^{m-r}.*

Proof. We have seen

$$wt_m(x_1x_2\cdots x_r) = 2^{m-r}.$$

Hence $d(RM(r,m)) \leq 2^{m-r}$. We prove

$$d(RM(r,m)) \geq 2^{m-r}$$

by induction on m. Suppose $m = 1$.

Case 1: $m = 1, r = 0$. $f : F_2^1 \longrightarrow F_2$(no x_i appears) and $f = 1$. Hence $f^{-1}(1) = F_2$. Then $wt_1(f) = |f^{-1}(1)| = 2 = 2^{m-r}$.

Case 2: $m = 1, r = 1$. $f \neq 0$ has $wt_1(f) \geq 1 = 2^{m-r}$.

Suppose for any $0 \neq f \in RM(r,m)$, we have $wt_m(f) \geq 2^{m-r}$. Choose any $f \in RM(r,m+1)$. Say $f = g + x_{m+1}h$ where $g \in RM(r,m+1)$ without x_{m+1} and $h \in RM(r-1,m+1)$ without x_{m+1}.

Case 1: $g = h \neq 0$. Then $f = h(x_{m+1})$ and

$$wt_{m+1}(f) = wt_m(h) \geq 2^{m-(r-1)} = 2^{m+1-r}.$$

(Using h has at most $r-1$ variables).

Case 2: $g \neq h$. Then

$$wt_{m+1}(f) = wt_m(g) + wt_m(g+h).$$

(To assign $x_{m+1} = 0$ in $wt_m(g)$ and $x_{m+1} = 1$ in $wt_m(g+h)$).

Case 2.1: $g = 0$. Hence $h \neq 0$ and

$$wt_{m+1}(f) = wt_m(h) \geq 2^{m-(r-1)} = 2^{m+1-r}.$$

Case 2.2: $g \neq 0$. Note $g + h \neq 0$, since $g \neq h$. Hence

$$wt_{m+1}(f) = wt_m(g) + wt_m(g + h) \geq 2^{m-r} + 2^{m-r} = 2^{m+1-r}.$$

$\square$

Next, our goal is to prove

$$wt_m(f_S) = 2^{m-r} \Longleftrightarrow S \text{ is affine } (m-r)-\text{subspace} \qquad (*)$$

where $S \subseteq F_2^m$, and

$$f_S(x) := \begin{cases} 1, & \text{if } x \in S; \\ 0, & \text{else} \end{cases}$$

f_S is called the *characteristic function* of S.

Remark 4.2.12. R_m=$\{f_S \mid S \subseteq F_2^m\}$.

One direction is easier.

Theorem 4.2.13. *Suppose S is an affine $(m-r)$-subspace in F_2^m. Then $wt(f_S) = 2^{m-r}$ and $f_S \in RM(r, m)$.*

Proof. Note $wt(f_S)$=$|f_S^{-1}(1)|$=$|S|$=2^{m-r}. Observe S is the solution space of a system of r linear independent equations in m variables. Hence there exist $a_{ij}, b_i \in F_2$ such that for $i = 1, 2, \cdots, r$ and $j = 1, 2, \cdots, m$ we have

$$(x_1, x_2, \cdots, x_m) \in S \Longleftrightarrow \sum_{j=1}^{m} a_{ij}x_j = b_i \text{ for } i = 1, 2, \cdots, r.$$

Observe

$$f_S = \prod_{i=1}^{r}[(\sum_{j=1}^{m} a_{ij}x_j) - b_i + 1]$$

and the degree of the monomial in the expansion of f_S is less or equal r. $\square$

To prove the other direction, we need some facts as following notes.

Note 4.2.14. An affine k-subspace is the union of 2 parallel affine $(k-1)$-subspaces by Lemma 3.5.12.

Note 4.2.15. We say the disjunct union $S_1 \dot{\cup} S_2 = S \subseteq F_2^m$ if and only if $f_S = f_{S_1} + f_{S_2}$.

Theorem 4.2.16. *The vectors in* $\{f_S \mid S \text{ is a affine } (m-r)\text{-subspace of } F_2^m\}$ *span* $RM(r,m)$.

Proof. It suffices to prove $x_{i_1}x_{i_2}\cdots x_{i_t}$ is spanned by the characteristic function of affine $(m-r)$-subspaces, where $t \leq r$. Observe $x_{i_1}x_{i_2}\cdots x_{i_t}$=$f_T$ for some affine $(m-t)$-subspace T and $f_T = f_{T_1} + f_{T_2}$ for some parallel affine $(m-(t+1))$-subspaces T_1,T_2. Keeping doing this, we find $x_{i_1}x_{i_2}\cdots x_{i_t}$ is the sum of some characteristic functions of affine $(m-r)$-subspaces. □

Definition 4.2.17. An affine $(m-1)$-subspace in F_2^m is called a *hyperplane* of F_2^m.

Theorem 4.2.18. *Suppose* $T \subseteq F_2^m$ *with* $|T| = 2^k$. *Suppose* $|T \cap S| = 0, 2^{k-1}$ *or* 2^k *for any hyperplane* S *of* F_2^m. *Then* T *is an affine* k*-subspace of* F_2^m.

Proof. We prove this by induction on m and $m = 2$ is clear. In general, we consider the following 3 cases.

Case 1: $T \subseteq S$ for some hyperplane S of F_2^m. Then $S \cong F_2^{m-1}$. Let H be a hyperplane of S. Then H is an affine $(m-2)$-subspace of F_2^m. We want to show that $|T \cap H| = 0, 2^{k-1}$ or 2^k. Observe there is an affine $(m-1)$-subspace S' such that $S \cap S' = H$. Hence $|T \cap H| = |T \cap S \cap S'| = |T \cap S'| = 0, 2^{k-1}$ or 2^k by assumption. By induction, T is an affine k-subspace in S and then in F_2^m.

Case 2: $T \cap S = \emptyset$ for some hyperplane S of F_2^m. Then $T \subseteq S'$ for the hyperplane S' of F_2^m parallel to S. So the result follows from Case 1.

Case 3: $|T \cap S| = 2^{k-1}$ for all hyperplanes S of F_2^m. Observe the case $m = k$ is clear, so suppose $m \neq k$. Then on the one hand

$$\sum_S |T\cap S|^2 = \begin{bmatrix} m \\ m-1 \end{bmatrix}_2 \cdot \frac{2^m}{2^{m-1}} \cdot 2^{2(k-1)} = (2^m-1)2^{2k-1}$$

and on the other hand

$$\begin{aligned}
\sum_S |T\cap S|^2 &= \sum_S (\sum_{a\in T} f_S(a))^2 \\
&= \sum_{a\in T}\sum_{b\in T}\sum_S f_S(a)f_S(b) \\
&= \sum_{a\in T}\sum_{b\in T, b\neq a}\sum_S f_S(a)f_S(b) + \sum_{a\in T}\sum_S f_S(a)^2 \\
&= |T|(|T|-1)\begin{bmatrix} m-1 \\ 1 \end{bmatrix}_2 + |T|\begin{bmatrix} m \\ 1 \end{bmatrix}_2 \\
&= 2^k(2^k-1)(2^{m-1}-1) + 2^k(2^m-1) \\
&= 2^k[2^{k+m-1} - 2^{m-1} - 2^k + 2^m],
\end{aligned}$$

where the summations are over all hyperplanes S in F_2^m. Hence

$$m = k,$$

a contradiction. $\square$

Now we can show the other direction in $(*)$.

Theorem 4.2.19. *Let $f \in RM(r,m)$ be the minimum weight vector. Then $f = f_S$ for some affine $(m-r)$-subspace S in F_2^m.*

Proof. By Theorem 4.2.11, $wt(f) = 2^{m-r}$. Then $f = f_S$ for some $S \subseteq F_2^m$ with $|S| = 2^{m-r}$. We want to show that S is an affine $(m-r)$-subspace. Let H be a hyperplane in F_2^m. We want to show

$$|S\cap H| = 0, 2^{m-r-1} \text{ or } 2^{m-r},$$

and then apply Theorem 4.2.18 to say S is an affine $(m-r)$-subspace. Observe $F_2^m = H \cup H'$ where H' is parallel to H. Observe $f_H, f_{H'} \in RM(1,m)$ by Theorem

4.2.16 and $1 = f_H + f_{H'}$, since $H \cap H' = \emptyset$. Hence $ff_H, ff_{H'} \in RM(r+1, m)$. By Theorem 4.2.11,

$$wt(ff_H) = 0 \text{ or } \geq 2^{m-(r+1)}$$

and

$$wt(ff_{H'}) = 0 \text{ or } \geq 2^{m-(r+1)}.$$

Since

$$\begin{aligned} 2^{m-r} &= wt(f) \\ &= wt(ff_H + ff_{H'}) \\ &= wt(ff_H) + wt(ff_{H'}), \end{aligned}$$

We have $wt(ff_H) = 0, 2^{m-r-1}$ or 2^{m-r}. Hence

$$|S \cap H| = 0, 2^{m-r-1} \text{ or } 2^{m-r}.$$

□

4.3 Decoding

We study the decoding of Reed-Muller codes in this section, we need the following notation.

Definition 4.3.1. $S_\sigma := \{(c_1, c_2, \cdots, c_m) \mid c_i = 1, i \in \sigma\}$ is an affine $(m-|\sigma|)-$subspace and $x_\sigma = \prod_{i\in\sigma} x_i$ is a monomial, where $\sigma \subseteq [m] = \{1, 2, \cdots, m\}$. Hence

$$S_\sigma = x_\sigma^{-1}(1).$$

Definition 4.3.2. $\overline{\sigma} = [m] - \sigma$ is called the complement of σ, where $\sigma \subseteq [m]$

We give an example as following.

Example 4.3.3. Suppose $m = 6, \sigma = \{1, 2, 3\}$. Since $x_\sigma = x_1x_2x_3$ and $x_{\overline{\sigma}} = x_4x_5x_6$, we obtain $S_\sigma = \{(1, 1, 1, a, b, c) \mid a, b, c \in F_2\}$ and $S_{\overline{\sigma}} = \{(d, e, f, 1, 1, 1) \mid d, e, f \in F_2\}$.

By Definition 4.2.9, we have

Note 4.3.4. Suppose $f \in RM(r,m)$. Then $f = \sum_{|\sigma| \le r, \sigma \subseteq [m]} f_\sigma x_\sigma$ for some $f_\sigma \in F_2$.

Lemma 4.3.5. *Suppose $u \in F_2^m$ and $\tau = \{i \mid u_i = 1\}$. Then for $\sigma, \rho \subseteq [m]$, we have*

$$|S_\sigma \cap (u + S_\rho)| = \begin{cases} 2^{m-|\rho \cup \sigma|}, & \text{if } \sigma \cap \rho \cap \tau = \emptyset; \\ 0, & \text{else}. \end{cases}$$

Proof. Observe

$$u + S_\rho = \{(c_1, c_2, \cdots, c_m) \mid c_i = 1 \text{ if } i \in \rho \cap \overline{\tau},\ c_i = 0 \text{ if } i \in \rho \cap \tau\}$$

and

$$S_\sigma = \{(c_1, c_2, \cdots, c_m) \mid c_i = 1 \text{ if } i \in \sigma\}.$$

Hence if $\sigma \cap \rho \cap \tau = \emptyset$, we have

$$S_\sigma \cap (u + S_\rho) = \{(c_1, c_2, \cdots, c_m) \mid c_i = 1 \text{ if } i \in \sigma \cup (\rho \cap \overline{\tau}),\ c_i = 0 \text{ if } i \in \overline{\sigma} \cap \rho \cap \tau\}.$$

Then

$$|S_\sigma \cap (u + S_\rho)| = 2^{m-|\rho \cup \sigma|}$$

when

$$\sigma \cap \rho \cap \tau = \emptyset.$$

Note

$$|S_\sigma \cap (u + S_\rho)| = 0$$

when

$$\sigma \cap \rho \cap \tau \neq \emptyset.$$

□

Since this is not trivial, we give two examples as following for improving the sense about Lemma 4.3.5.

Example 4.3.6. Suppose $u = 0, m = 5$, $\sigma = \{1,2\}$ and $\rho = \{3,4\}$. We obtain $S_\sigma = \{(1,1,c_3,c_4,c_5) \mid c_i \in F_2\}$ and $u + S_\rho = \{(c_1,c_2,1,1,c_5) \mid c_i \in F_2\}$. Hence

$$S_\sigma \cap (u + S_\rho) = \{(1,1,1,1,c_5) \mid c_5 \in F_2\}$$

has cardinality $2 = 2^{m-|\sigma\cup\rho|}$.

Example 4.3.7. Suppose $u = (1,0,0), m = 3$, $\sigma = \{1,2\}$ and $\rho = \{1\}$. We obtain $S_\sigma = \{(1,1,c_3) \mid c_3 \in F_2\}$ and $u + S_\rho = \{(0,c_2,c_3) \mid c_2,c_3 \in F_2\}$. Hence

$$S_\sigma \cap (u + S_\rho) = \emptyset.$$

The following theorem is essentially a decoding of $RM(r,m)$. This will be clear later.

Theorem 4.3.8. *Suppose* $f = \sum_{|\rho|\le r, \rho\subseteq[m]} f_\rho x_\rho \in RM(r,m)$ *for* $f_\rho \in F_2$*. Fix* $\sigma \subseteq [m]$ *with* $|\sigma| = r$*. Then*

$$f_\sigma = \sum_{w\in u+S_{\overline{\sigma}}} f(w) \text{ for all } u \in F_2^m. \tag{$*$}$$

Proof.

$$\begin{aligned}
\sum_{w\in u+S_{\overline{\sigma}}} f(w) &= \sum_{w\in u+S_{\overline{\sigma}}} \sum_{|\rho|\le r} f_\rho x_\rho(w) \\
&= \sum_{|\rho|\le r} f_\rho \sum_{w\in u+S_{\overline{\sigma}}} x_\rho(w) \\
&= \sum_{|\rho|\le r} f_\rho |S_\rho \cap (u + S_{\overline{\sigma}})| \\
&= f_\sigma,
\end{aligned}$$

since $|S_\rho \cap (u + S_{\overline{\sigma}})|$ is even except $\rho = \sigma$ by Lemma 4.3.5. $\square$

Note 4.3.9. The size of $u + S_{\overline{\sigma}}$ is $|\{u + S_{\overline{\sigma}} \mid u \in F_2^m\}| = \dfrac{2^m}{2^{m-|\overline{\sigma}|}} = \dfrac{2^m}{2^r} = 2^{m-r}$ for the σ, u in Theorem 4.3.8. $(*)$ contains 2^m equations, one for each $u \in F_2^m$. Some of them are identical. There are 2^{m-r} different equations.

Note 4.3.10. For $|\sigma| = r-1$, the Theorem 4.3.8 does not hold.

We show how Theorem 4.3.8 is used in the decoding process as following.

Application 4.3.11. (Encoding and Decoding Processes)

$$
\begin{aligned}
& f = \sum_{|\rho|\leq r, \rho\subseteq[m]} f_\rho x_\rho \in RM(r,m) \qquad \text{(original message)} \\
\longrightarrow\ & (f(0), f(1), f(2), \cdots, f(2^m-1)) \qquad \text{(encoding } f \text{ into a string of } 0,1) \\
\longrightarrow\ & (f'(0), f'(1), f'(2), \cdots, f'(2^m-1))
\end{aligned}
$$

(f is sending via a noisy channel to become f')

$\longrightarrow$ Compute $f'_\sigma = \sum_{t\in u+S_{\overline{\sigma}}} f'(t)$ for each $|\sigma| = r$ and each $u + S_{\overline{\sigma}}$.

There are 2^{m-r} such f'_σ according to different cosets $u + S_{\overline{\sigma}}$,

and we use majority to determine f_σ

(Assume the number of errors $\leq \lfloor \frac{2^{m-r}-1}{2} \rfloor$ in the sending).

$\longrightarrow$ Set new f as $f - \sum_{|\sigma|=r} f_\sigma x_\sigma$ and new f' as $f' - \sum_{|\sigma|=r} f_\sigma x_\sigma$

and go to the previous step to determine those f_σ for $|\sigma| = r-1$.

Keep doing this untill we get $f_\emptyset$.

We also present an example of the decoding process for improving the sense about the encoding and decoding processes.

Example 4.3.12. In $RM(1,3)$, suppose the receiving codeword

$$(f'(0), f'(1), f'(2), \cdots, f'(7)) = (1,1,0,0,0,1,0,0).$$

Assume the number of errors $\leq \lfloor \frac{2^{m-r}-1}{2} \rfloor = 1$.

(i) We can find f_σ for $|\sigma| = 1$ by the following steps.

Suppose $\sigma = \{1\}, \overline{\sigma} = \{2,3\}$. First step is to find all $u + S_{\{2,3\}}$ for $u \in F_2^3$. We find

$$S_{\{2,3\}} = \{(0,1,1),(1,1,1)\}$$

Then

$$\begin{aligned}\{u+S_{\{2,3\}} \mid u \in F_2^3\} &= \{\{(0,1,1),(1,1,1)\},\{(0,0,1),(1,0,1)\}\\ &\quad ,\{(0,1,0),(1,1,0)\},\{(0,0,0),(1,0,0)\}\}\\ &= \{\{6,7\},\{4,5\},\{2,3\},\{0,1\}\}.\end{aligned}$$

Second step is to compute the possible values of $f_{\{1\}}$ and use majority to determine $f_{\{1\}}$. Since

$$f'_{\{1\}} = \sum_{t \in u+S_{\{2,3\}}} f'(t),$$

the possible values of $f_{\{1\}}$ are

$$f'(6)+f'(7)=0+0=0,\ \ f'(4)+f'(5)=0+1=1,$$

$$f'(2)+f'(3)=0+0=0 \text{ or } f'(0)+f'(1)=1+1=0.$$

Third step is to use majority to determine that

$$f_{\{1\}}=0.$$

In the same way, we find that $f_{\{2\}}=1$ and $f_{\{3\}}=0$.
(ii) Since

$$f = \sum_{|\rho|\leq 1, \rho\subseteq[m]} f_\rho x_\rho,$$

$$\begin{aligned} f_\emptyset &= f - f_{\{1\}}x_1 - f_{\{2\}}x_2 - f_{\{3\}}x_3\\ &= f + x_2 \in RM(0,3).\end{aligned}$$

Hence the new receiving codeword

$$\begin{aligned} & (f''(0), f''(1), f''(2), \cdots, f''(7))\\ =\ & (1,1,0,0,0,1,0,0)+(0,0,1,1,0,0,1,1)\\ =\ & (1,1,1,1,0,1,1,1).\end{aligned}$$

(iii) Go to previous step to find $f_{\emptyset}$. Since $\sigma = \emptyset$, then

$$\{u + S_{\overline{\sigma}} \mid u \in F_2^3\} = \{\{0\}, \{1\}, \{2\}, \{3\}, \{4\}, \{5\}, \{6\}, \{7\}\},$$

then the possible values of $f_{\emptyset}$ are

$$f''(0) = 1,\ f''(1) = 1,\ f''(2) = 1,\ f''(3) = 1,$$

$$f''(4) = 0,\ f''(5) = 1,\ f''(6) = 1 \text{ or } f''(7) = 1.$$

By using majority to determine that

$$f_{\emptyset} = 1.$$

Hence

$$f = f_{\emptyset} + f_{\{1\}}x_1 + f_{\{2\}}x_2 + f_{\{3\}}x_3 = 1 + x_2,$$

and

$$(f(0), f(1), f(2), \cdots, f(7)) = (1, 1, 0, 0, 1, 1, 0, 0),$$

the 5th bit is error in the sending.

4.4 Recursive construction of $RM(1, m)$

We give another description of $RM(1, m)$ as appeared in [10, Chapter 18] in this section. We identity each function in $RM(1, m)$ with its coordinates in the standard basis.

Example 4.4.1. Suppose $RM(1, 1)$ is the 1-th Reed-Muller code of order 1. Then

$$\begin{aligned} RM(1,1) &= \{0, 1, x_1, 1 + x_1\} \\ &= \{(0,0), (1,1), (0,1), (1,0)\}. \end{aligned}$$

Example 4.4.2. Suppose $RM(1, 2)$ is the 1-th Reed-Muller code of order 2. Then

$$\begin{aligned} RM(1,2) &= \{0, 1, x_1, 1 + x_1, x_2, 1 + x_2, x_1 + x_2, 1 + x_1 + x_2\} \\ &= \{(0,0,0,0), (1,1,1,1), (0,1,0,1), (1,0,1,0), \\ &\quad (0,0,1,1), (1,1,0,0), (0,1,1,0), (1,0,0,1)\}. \end{aligned}$$

Since we observe the rule between Example 4.4.1 and Example 4.4.2, we get the general rule is as following.

Example 4.4.3. Suppose $RM(1, m+1)$ is the 1-th Reed-Muller code of order $m+1$. Then

$$\begin{aligned} & RM(1, m+1) \\ = \ & \{f \mid \ f \text{ does not have } x_{m+1}\} \cup \{f \mid f \ \text{ has } x_{m+1}\} \\ = \ & \{(c, c) \mid c \in RM(1, m)\} \cup \{(c, \overline{c}) \mid c \in RM(1, m)\} \\ = \ & \{(d, d, d, d), (d, \overline{d}, d, \overline{d}), (d, d, \overline{d}, \overline{d}), (d, \overline{d}, \overline{d}, d) \mid d \in RM(1, m-1)\}, \end{aligned}$$

where $\overline{c}$ is a vector obtained from c by switching 0 and 1.

4.5 Covering radius

We give the definition of covering radius of a code in this section and determine the lower bound of the covering radius of $RM(r, m)$.

Definition 4.5.1. For $C \subseteq F_2^n$, we define $d(x, C)$:=min$\{d(x, y) \mid y \in C\}$ where $x \in F_2^n$ and $\rho(C)$ =max$\{d(x, C) \mid x \in F_2^n\}$ is called the *covering radius* of C.

Example 4.5.2. Suppose $C = \{(0, 0, 0), (1, 1, 1)\}$. Then the covering radius of C is $\rho(C) = 1$.

The following notes show why the name covering radius is chosen.

Note 4.5.3. Suppose $\rho(C)$ is the covering radius of C. Then $\bigcup\limits_{x \in C} B_{\rho(C)+1}(x) = F_2^n$ where $B_i(x) := \{y \mid d(x, y) < i\}$.

Note 4.5.4. The covering radius $\rho(C)$ is minimum i such that $\bigcup\limits_{x \in C} B_{i+1}(x) = F_2^n$.

Theorem 4.5.5. $\rho(RM(1, m)) \geq 2^{m-1} - 2^{\lceil \frac{m}{2} \rceil - 1}$.

Proof. Induction on m.

If $m = 1$, then $2^{m-1} - 2^{\lceil \frac{m}{2} \rceil - 1} = 1 - 1 = 0$ and clearly $\rho(RM(1,1)) \geq 0$.

If $m = 2$, then $2^{m-1} - 2^{\lceil \frac{m}{2} \rceil - 1} = 2 - 1 = 1$. Since $RM(1,2) \neq RM(2,2)$, we have $\rho(RM(1,2)) \geq 1$. In general, consider in $RM(1, m+1)$. Choose $u \in R_{m-1}$ such that

$$d(u, RM(1, m-1)) \geq 2^{m-2} - 2^{\lceil \frac{m-1}{2} \rceil - 1}.$$

Set $v = (u, u, u, \overline{u}) \in R_{m+1}$. It remains to show

$$d(v, RM(1, m+1)) \geq 2^{m} - 2^{\lceil \frac{m+1}{2} \rceil - 1}.$$

There are 4 cases of codewords in $RM(1, m+1)$.

Case 1:$(c, c, c, c) \in RM(1, m+1)$ for $c \in RM(1, m-1)$.

$$\begin{aligned} & d(v, (c, c, c, c)) \\ = \;& 3d(u, c) + d(\overline{u}, c) \\ = \;& 3d(u, c) + 2^{m-1} - d(u, c) \\ = \;& 2^{m-1} + 2d(u, c) \\ \geq \;& 2^{m-1} + 2(2^{m-2} - 2^{\lceil \frac{m-1}{2} \rceil - 1}) \\ = \;& 2^{m} - 2^{\lceil \frac{m-1}{2} \rceil} \\ = \;& 2^{m} - 2^{\lceil \frac{m+1}{2} \rceil - 1}. \end{aligned}$$

Case 2:$(c, c, \overline{c}, \overline{c}) \in RM(1, m+1)$ for $c \in RM(1, m-1)$.

$$\begin{aligned} & d(v, (c, c, \overline{c}, \overline{c})) \\ = \;& 2d(u, c) + d(u, \overline{c}) + d(\overline{u}, \overline{c}) \\ = \;& 3d(u, c) + d(\overline{u}, c) \qquad (\text{by } d(u, \overline{c}) = d(\overline{u}, c) \text{ and } d(\overline{u}, \overline{c}) = d(u, c)) \\ \geq \;& 2^{m} - 2^{\lceil \frac{m+1}{2} \rceil - 1} \end{aligned}$$

as in the Case 1.

Similar for the remaining two cases $(c, \overline{c}, c, \overline{c}), (c, \overline{c}, \overline{c}, c) \in RM(1, m+1)$ for $c \in RM(1, m-1)$.

$\square$

Here we announced that we will know $\rho(RM(1, m))$ when m is even in section 6.1.

5

Punctured Reed-Muller Codes

A punctured Reed-Muller code is a obtain from a Reed-Muller code by puncturing the first position of each codeword. Since we use different language to define it, this will not be clear at the first look.

5.1 Definition

Definition 5.1.1. Let $F_2[\lambda]$ denote the set of polynomials over F_2 with a variable λ. Fix a primitive element $\gamma \in F_{2^m}^* := F_{2^m} - \{0\}$. For $f \in F_2[\lambda]$, define

$$T_f := \{\gamma^i \mid \text{the coefficient of } \lambda^i \text{ in } f(\lambda) \text{ is } 1\}.$$

$$\begin{aligned} PRM(r,m) := \ & \text{Span}\{f(\lambda) \in F_2[\lambda] \mid T_f \text{ is an affine } (m-r)-\text{subspace} \\ & \text{of } F_{2^m} \text{ over } F_2 \text{ or } T_f \cup \{0\} \text{ is an } (m-r)-\text{subspace} \\ & \text{of } F_{2^m} \text{ over } F_2\ \}/ < \lambda^{2^m-1} - 1 > \end{aligned}$$

is called the r-th *punctured Reed-Muller code* of order m with codewords of length $2^m - 1$. For $f(\lambda) \in PRM(r,m)$, the weight of f is defined by

$$wt(f) := |\{\ i \mid \text{the coefficient of } \lambda^i \text{ in } f \text{ is } 1\}|.$$

Of course, T_f depends on the choice of a primitive element $\gamma \in F_{2^m}$. We omit the mention of γ if no confusion occurs. We refer the reader to Theorem 4.2.16 for the name $PRM(r, m)$ to be chosen. Here we give an example for correspondence relation between $RM(r, m)$ and $PRM(r, m)$.

Example 5.1.2. Suppose $F_{2^3} = \{0, 1, \gamma, \gamma^2, \ldots, \gamma^6\}$, where γ is primitive element satisfying $\gamma^3 + \gamma + 1 = 0$. Then $\gamma^3 = 1 + \gamma$, $\gamma^4 = \gamma + \gamma^2$, $\gamma^5 = 1 + \gamma + \gamma^2$, and $\gamma^6 = 1 + \gamma^2$. This gives an one to one correspondence between $F_{2^3}^*$ and $F_2^3 - \{0\}$. The following processes (a)-(e) provide an example of the map from $f \in RM(1, 3)$ onto $f^* \in PRM(1, 3)$.

(a) $f = x_1 + x_2 \in RM(1, 3)$;

(b)

$$\begin{array}{cccccccccc}
f & = & (0, & 1, & 1, & 0, & 0, & 1, & 1, & 0) \\
 & & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow \\
1 & x_1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
\gamma & x_2 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
\gamma^2 & x_3 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
 & & & 1 & \gamma & \gamma^3 & \gamma^2 & \gamma^6 & \gamma^4 & \gamma^5
\end{array}$$

(encoding f into a string of $0, 1$ as in Application 4.3.11, the positions are indexed correspondence to the binary number of F_2^3. The last row shows the way to index the positions by elements in $F_{2^3}^*$);

(c) $f^* = (1, 1, 0, 0, 1, 1, 0)$

(delete the first position)

(d)

$$\begin{array}{ccccccccc}
f^* & = & (1, & 1, & 0, & 0, & 1, & 0, & 1) \\
 & & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow \\
 & & 1 & \gamma & \gamma^2 & \gamma^3 & \gamma^4 & \gamma^5 & \gamma^6
\end{array}$$

(reorder the string by the new index corresponding to $F^*_{2^3}$);

(e) $f^* = 1 + \lambda + \lambda^4 + \lambda^6$

(write the string in polynomial form).

Observe

$$\begin{aligned} T_{f^*} &= \{1, \gamma, \gamma^4, \gamma^6\} \\ &= \{1, \gamma, \gamma + \gamma^2, 1 + \gamma^2\} \\ &= \{(1,0,0), (0,1,0), (0,1,1), (1,0,1)\} \\ &= (1,0,0) + \{(0,0,0), (1,1,0), (1,1,1), (0,0,1)\} \end{aligned}$$

is an affine 2-subspace. Hence $f^* \in PRM(1,3)$.

In Example 5.1.2, we will have a complete correspondence between $RM(1,3)$ and $PRM(1,3)$.

Lemma 5.1.3. *The minimum distance $d(PRM(r,m))$ is equal to $2^{m-r} - 1$.*

Proof. This is immediate from Theorem 4.2.11 and Theorem 4.2.19. □

5.2 Cyclic Codes

We will show a punctured Reed-Muller code is cyclic. First we need a definition as following.

Definition 5.2.1. A code $C \subseteq F_2^n$ is cyclic if

$$(c_0, c_1, \cdots, c_{n-1}) \in C \Longrightarrow (c_{n-1}, c_0, c_1, \cdots, c_{n-2}) \in C.$$

We give four examples as following.

Example 5.2.2. $\{0\}$ is cyclic.

Example 5.2.3. $\{(0,0,0,0),(1,1,1,1)\} \subseteq F_2^4$ is cyclic.

Example 5.2.4. F_2^n is cyclic.

Example 5.2.5. $\{(0,0,0,0,0,0,0),(1,1,1,0,1,0,0),(0,1,1,1,0,1,0),$ $(0,0,1,1,1,0,1),(1,0,0,1,1,1,0),(0,1,0,0,1,1,1),(1,0,1,0,0,1,1),$ $(1,1,0,1,0,0,1)\}$ is cyclic. This code is not linear!

It is not easy to find a nontrivial code that are both linear and cyclic. We introduce a way by polynomials. Usually we identity an element $(a_0, a_1, \cdots, a_{n-1}) \in F_2^n$ with the polynomial $a_0 + a_1\lambda + \cdots + a_{n-1}\lambda^{n-1}$.

Note 5.2.6. A linear code $C \subseteq F_2^n$ is cyclic if and only if $\lambda f(\lambda) \in C \bmod (\lambda^n - 1)$ for any $f(\lambda) \in C$. $\square$

Lemma 5.2.7. *A linear code $C \subseteq F_2^n$ is cyclic if and only if there exists a function $g(\lambda)|\lambda^n - 1$ such that $C = \{g(\lambda)h(\lambda) \mid h(\lambda) \in F_2[\lambda], \deg(h(\lambda)) \leq n - \deg(g(\lambda)) - 1\}$.*

We skip the proof of the above lemma. It can be found in any standard textbook of coding theory, for examples [14],[1]. Lemma 5.2.7 says a linear code $C \subseteq F_2^n$ is cyclic if and only if C is a *principle idea ring* in $F_2[\lambda]/ < \lambda^n - 1 >$.

Note 5.2.8. By Lemma 5.2.7, we obtain that $\dim(C) = n - \deg(g(\lambda))$.

Note 5.2.9. As the notation in Definition 5.1.1, $T_{\lambda f(\lambda)} = \gamma T_{f(\lambda)}$ and $T_{\lambda f(\lambda)} \cup \{0\} = \gamma(T_{f(\lambda)} \cup \{0\})$.

The following is the main theorem of the section.

Theorem 5.2.10. *$PRM(r,m)$ is cyclic when the coordinates are indexed by*

$$1, \gamma, \gamma^2, \cdots, \gamma^{2^m-2}.$$

Proof. We need to prove

$$f(\lambda) \in PRM(r,m) \Longrightarrow \lambda f(\lambda) \in PRM(r,m) \bmod (\lambda^{2^m-1} - 1).$$

It suffices to assume $T_{f(\lambda)}$ or $T_{f(\lambda)} \cup \{0\}$ is an affine $(m-r)$-subspace and show $\gamma T_{f(\lambda)} = T_{\lambda f(\lambda)}$ or $\gamma(T_{f(\lambda)} \cup \{0\}) = T_{\lambda f(\lambda)} \cup \{0\}$ is an $(m-r)$-subspace. This follows from Lemma 3.4.7. $\square$

Example 5.2.11. We complete the Example 5.1.2 by a table.

$RM(1,3)$	$RM(1,3)$	$PRM(1,3)$	$PRM(1,3)$
0	$(0,0,0,0,0,0,0,0)$	$(0,0,0,0,0,0,0)$	0
1	$(1,1,1,1,1,1,1,1)$	$(1,1,1,1,1,1,1)$	$1+\lambda+\cdots+\lambda^6$
$1+x_3$	$(1,1,1,1,0,0,0,0)$	$(1,1,0,1,0,0,0)$	$1+\lambda+\lambda^3$
$1+x_1$	$(1,0,1,0,1,0,1,0)$	$(0,1,1,0,1,0,0)$	$\lambda+\lambda^2+\lambda^4$
$1+x_1+x_2$	$(1,0,0,1,1,0,0,1)$	$(0,0,1,1,0,1,0)$	$\lambda^2+\lambda^3+\lambda^5$
$1+x_1+x_2+x_3$	$(1,0,0,1,0,1,1,0)$	$(0,0,0,1,1,0,1)$	$\lambda^3+\lambda^4+\lambda^6$
$1+x_2+x_3$	$(1,1,0,0,0,0,1,1)$	$(1,0,0,0,1,1,0)$	$1+\lambda^4+\lambda^5$
$1+x_1+x_3$	$(1,0,1,0,0,1,0,1)$	$(0,1,0,0,0,1,1)$	$\lambda+\lambda^5+\lambda^6$
$1+x_2$	$(1,1,0,0,1,1,0,0)$	$(1,0,1,0,0,0,1)$	$1+\lambda^2+\lambda^6$
x_1	$(0,1,0,1,0,1,0,1)$	$(1,0,0,1,0,1,1)$	$1+\lambda^3+\lambda^5+\lambda^6$
x_1+x_2	$(0,1,1,0,0,1,1,0)$	$(1,1,0,0,1,0,1)$	$1+\lambda+\lambda^4+\lambda^6$
$x_1+x_2+x_3$	$(0,1,1,0,1,0,0,1)$	$(1,1,1,0,0,1,0)$	$1+\lambda+\lambda^2+\lambda^5$
x_2+x_3	$(0,0,1,1,1,1,0,0)$	$(0,1,1,1,0,0,1)$	$\lambda+\lambda^2+\lambda^3+\lambda^6$
x_1+x_3	$(0,1,0,1,1,0,1,0)$	$(1,0,1,1,1,0,0)$	$1+\lambda^2+\lambda^3+\lambda^4$
x_2	$(0,0,1,1,0,0,1,1)$	$(0,1,0,1,1,1,0)$	$\lambda+\lambda^3+\lambda^4+\lambda^5$
x_3	$(0,0,0,0,1,1,1,1)$	$(0,0,1,0,1,1,1)$	$\lambda^2+\lambda^4+\lambda^5+\lambda^6$

The codewords in the third column is obtained by truncating the codewords in the second column and then reordering the coordinates by the the way switching the positions $(3,4)$ and permuting positions $(4,6,5)$ as escribed in Example 5.1.1. Observe from the table that if we set $g(\lambda) := 1+\lambda+\lambda^3$ then

$$PRM(1,3) = \{g(\lambda)h(\lambda) \mid h(\lambda) \in F_2[\lambda],\ \deg(h(\lambda)) \leq 3\}.$$

Note that $PRM(1,3)$ does not decrease in number from $RM(1,3)$. This is true for any $PRM(r,m)$. However this is not easy to show.

5.3 Lucas Theorem

In the following two sections, we give some background information in order to find the dimension of $PRM(r,m)$ is section 5.5.

Lemma 5.3.1. *(Lucas Theorem 1878) If p is a prime and $0 \leq a, b < p$ are integers, then for n,$k \in \mathbb{N}$*

$$\binom{np+a}{kp+b} = \binom{n}{k}\binom{a}{b} \ \textit{mod } p.$$

Proof. By binomial theorem,

$$\begin{aligned}
\sum_{i=0}^{np+a}\binom{np+a}{i}\lambda^i &= (\lambda+1)^{np+a} \\
&= (\lambda+1)^{np}(\lambda+1)^a \\
&= (\sum_{i=0}^{p}\binom{p}{i}\lambda^i)^n(\lambda+1)^a \\
&\equiv (\lambda^p+1)^n(\lambda+1)^a \bmod p \\
&= \sum_{j=0}^{n}\binom{n}{j}\lambda^{pj}\sum_{s=0}^{a}\binom{a}{s}\lambda^s.
\end{aligned}$$

Comparing the coefficients of λ^{kp+b} in both sides, we find

$$\binom{np+a}{kp+b} = \binom{n}{k}\binom{a}{b} \bmod p.$$

□

Corollary 5.3.2. *If p is a prime and $0 \leq n_0, k_0 < p$ are integers, then*

$$\binom{n_0+n_1p+n_2p^2+\cdots n_tp^t}{k_0+k_1p+k_2p^2+\cdots k_tp^t} = \binom{n_o}{k_0}\binom{n_1}{k_1}\binom{n_2}{k_2}\cdots\binom{n_t}{k_t} \ \textit{mod } p$$

for $n_i, k_i \in \mathbb{N}$ and $i = 0, 1, 2, \cdots, t$.

Proof. By Lemma 5.3.1, then

$$\begin{aligned}
\binom{n_0 + n_1 p + n_2 p^2 + \cdots n_t p^t}{k_0 + k_1 p + k_2 p^2 + \cdots k_t p^t} &= \binom{n_0 + (n_1 + n_2 p + \cdots + n_t p^{t-1})p}{k_0 + (k_1 + k_2 p + \cdots + k_t p^{t-1})p} \\
&\equiv \binom{n_0}{k_0} \binom{n_1 + n_2 p + \cdots + n_t p^{t-1}}{k_1 + k_2 p + \cdots + k_t p^{t-1}} \mod p \\
&\;\;\vdots \\
&\equiv \binom{n_0}{k_0} \binom{n_1}{k_1} \binom{n_2}{k_2} \cdots \binom{n_t}{k_t} \mod p.
\end{aligned}$$

□

Note 5.3.3. By Corollary 5.3.2,

$$\binom{n}{k} = \binom{n_0}{k_0} \binom{n_1}{k_1} \binom{n_2}{k_2} \cdots \binom{n_t}{k_t} \mod 2$$

for $n = \sum_{i=0}^{t} 2^i n_i$ and $k = \sum_{i=0}^{t} 2^i k_i$, where $n_i, k_i \in \{0, 1\}$.

We give a summary as following.

Note 5.3.4. Suppose $n = \sum_{i=0}^{t} 2^i n_i$ and $k = \sum_{i=0}^{t} 2^i k_i$, where $n_i, k_i \in \{0, 1\}$. Then the following $(1) - (4)$ are equivalent by Note 5.3.3.

(1) $\binom{n}{k} \equiv 1 \mod 2$.

(2) $\binom{n_i}{k_i} \equiv 1 \mod 2$ for all $i = 0, 1, 2, \cdots, t$

(3) $k_i \leq n_i$ $(n_i - k_i \leq n_i)$ for all $i = 0, 1, 2, \cdots, t$.

(4) There is no overflowing in compute $n = k + (n - k)$ in binary system.

More generally, we have the following.

Note 5.3.5. Suppose $n = j_1 + j_2 + \cdots + j_k$. Then $\dfrac{n!}{j_1!j_2!\cdots j_k!} \equiv 1 \bmod 2$ if and only if there is no overflowing in compute $n = j_1 + j_2 + \cdots + j_k$ in binary system.

Example 5.3.6. Let $k = (0,0,1,1,1,1,0)_2 = 4{+}8{+}16{+}32 = 60$, $n = (1,0,0,0,0,0,1)_2 = 1 + 64 = 65$ and $n - k = (1,0,1,0,0,0,0)_2 = 1 + 4 = 5$. Since there is overflowing over the summation $n = k + (n-k)$ in binary system, we have $\begin{pmatrix} n \\ k \end{pmatrix} = \begin{pmatrix} 65 \\ 60 \end{pmatrix} \equiv 0$ mod 2.

5.4 Evaluation $f(a)$ for $f \in PRM(r,m)$

We give a theorem without proof. This is a generalization of Theorem 4.2.8.

Theorem 5.4.1. *If $V = \{F \mid F : F_q^k \longrightarrow F_q$ is a function$\}$, where $q = 2^m$, then the set $\{x_1^{j_1}x_2^{j_2}\cdots x_k^{j_k} \mid 0 \le j_i \le q-1\}$ is a basis of V over F_q.* $\square$

Definition 5.4.2. For each $s \in \{1, 2, 3, \cdots, 2^m - 1\}$ and $k \le m$, we define a polynomial function F_S in V as

$$F_s(x_1, x_2, \cdots, x_k) := \sum_{\substack{j_1+j_2+\cdots+j_k=s \\ j_i \ge 1}} \begin{pmatrix} s \\ j_1 j_2 \cdots j_k \end{pmatrix} x_1^{j_1}x_2^{j_2}\cdots x_k^{j_k},$$

where $\begin{pmatrix} s \\ j_1 j_2 \cdots j_k \end{pmatrix} = \dfrac{s!}{j_1!j_2!\cdots j_k!} = \begin{cases} 1, & \text{if } \begin{pmatrix} s \\ j_1 j_2 \cdots j_k \end{pmatrix} \text{ is odd;} \\ 0, & \text{else} \end{cases}.$

Note 5.4.3. $F_s(x_1, x_2, \cdots, x_k) \ne (x_1 + x_2 + \cdots + x_k)^s$.

Lemma 5.4.4. *$F_s(x_1, x_2, \cdots, x_k) = 0$ if and only if there are at most $(k-1)$ 1's in the binary expression of s.*

Proof. ($\Longrightarrow$)Since $\{x_1^{j_1}x_2^{j_2}\cdots x_k^{j_k} \mid 0 \le j_i \le 2^m - 1\}$ is a linear independent set over F_{2^m} and then over F_2, we find $\dfrac{s!}{j_1!j_2!\cdots j_k!} = 0$ in F_2 for all $j_1 + j_2 + \cdots + j_k = s$.

Hence the binary expression of s has at most $k-1$ 1's by Note 5.3.5.

($\Longleftarrow$)By Note 5.3.5, s can not be written as the sum of k positive integers without overflowing in the binary expression. Hence each coefficient $\begin{pmatrix} s \\ j_1 j_2 \cdots j_k \end{pmatrix} \equiv 0$ in $(*)$.

Hence $F_s(x_1, x_2, \cdots x_k) = 0$. □

Lemma 5.4.5. *$F_s(x_1, x_2, \cdots, x_k) = \sum (b_1x_1 + b_2x_2 + \cdots + b_kx_k)^s$, where the summation is over all $b = (b_1, b_2, \cdots, b_k) \in F_2^k$.*

Proof. We prove by induction on k. For $k = 1$, observe $F_s(x_1) = x_1^s$ and

$$\sum_{b_1 \in F_2} (b_1x_1)^s = x_1^s.$$

Before showing the general case we do the case $k = 2$ first for clarity. Observe

$$\begin{aligned} F_s(x_1, x_2) &= \begin{pmatrix} s \\ 1 \end{pmatrix} x_1 x_2^{s-1} + \begin{pmatrix} s \\ 2 \end{pmatrix} x_1^2 x_2^{s-2} + \cdots + \begin{pmatrix} s \\ s-1 \end{pmatrix} x_1^{s-1} x_2 \\ &= \sum_{i=1}^{s-1} \begin{pmatrix} s \\ i \end{pmatrix} x_1^i x_2^{s-i} \end{aligned}$$

and

$$\begin{aligned} & \sum_{(b_1,b_2) \in F_2^2} (b_1x_1 + b_2x_2)^s \\ = & \sum_{b_2 \in F_2} (b_2x_2)^s + \sum_{b_2 \in F_2} (x_1 + b_2x_2)^s \qquad \text{(according to } b_1 = 0 \text{ or } 1) \\ = & \sum_{b_2 \in F_2} (b_2x_2)^s + \sum_{b_2 \in F_2} \sum_{i=0}^{s} \begin{pmatrix} s \\ i \end{pmatrix} x_1^i (b_2x_2)^{s-i} \\ = & \; x_2^s + (\sum_{i=1}^{s-1} [\sum_{b_2 \in F_2} b_2^{s-i}] \begin{pmatrix} s \\ i \end{pmatrix} x_1^i x_2^{s-i}) + x_2^s + \sum_{b_2 \in F_2} x_1^s \\ = & \sum_{i=1}^{s-1} [\sum_{b_2 \in F_2} b_2^{s-i}] \begin{pmatrix} s \\ i \end{pmatrix} x_1^i x_2^{s-i} \\ = & \sum_{i=1}^{s-1} \begin{pmatrix} s \\ i \end{pmatrix} x_1^i x_2^{s-i}. \end{aligned}$$

In general,

$$
\begin{aligned}
& \sum_{b\in F_2^k}(b_1x_1+b_2x_2+\cdots+b_kx_k)^s \\
= & \sum_{(b_2,b_3,\cdots,b_k)\in F_2^{k-1}}(b_2x_2+b_3x_3+\cdots+b_kx_k)^s \\
& + \sum_{(b_2,b_3,\cdots,b_k)\in F_2^{k-1}}(x_1+b_2x_2+b_3x_3+\cdots+b_kx_k)^s \\
= & \sum_{j_1=1}^{s-1}\sum_{(b_1,b_2,\cdots,b_k)\in F_2^{k-1}}\binom{s}{j_1}x_1^{j_1}(b_2x_2+b_3x_3+\cdots+b_kx_k)^{s-j_1} \\
& \qquad \text{(the term is 0 when } j_1=0, \text{ or } s) \\
= & \sum_{j_1=1}^{s-1}\binom{s}{j_1}x_1^{j_1}F_{s-j_1}(x_2,x_3,\cdots,x_k) \qquad \text{(by induction)} \\
= & \sum_{j_1=1}^{s-1}\binom{s}{j_1}x^{j_1}\sum_{\substack{j_2+j_3+\cdots+j_k=s-j_1\\ j_i\geq 1}}\frac{(s-j_1)!}{j_2!j_3!\cdots j_k!}x_2^{j_2}x_3^{j_3}\cdots x_k^{j_k} \\
= & F_s(x_1,x_2,\cdots,x_k).
\end{aligned}
$$

□

Lemma 5.4.6. *Let $\alpha_1,\alpha_2,\cdots,\alpha_k\in F_{2^m}$ be linear dependent vectors over F_2. Then*

$$F_s(\alpha_1,\alpha_2,\cdots,\alpha_k)=0$$

for $s\in\{1,2,\cdots,2^m-1\}$.

Proof. Suppose $\alpha_1,\alpha_2,\cdots,\alpha_k$ are linear dependent over F_2. We say $\alpha_k=\sum_{i=1}^{k-1}a_i\alpha_i$ for some $a_i \in F_2$. Then

$$
\begin{aligned}
& F_s(\alpha_1, \alpha_2, \cdots, \alpha_k) \\
= & \sum_{b \in F_2^k} (b_1\alpha_1 + b_2\alpha_2 + \cdots + b_k\alpha_k)^s \\
= & \sum_{(b_1, b_2, \cdots, b_{k-1}) \in F_2^{k-1}} (b_1\alpha_1 + b_2\alpha_2 + \cdots + b_{k-1}\alpha_{k-1})^s \\
+ & \sum_{(b_1, b_2, \cdots, b_{k-1}) \in F_2^{k-1}} [(a_1 + b_1)\alpha_1 + (a_2 + b_2)\alpha_2 + \cdots + (a_{k-1} + b_{k-1})\alpha_{k-1}]^s \\
= & 2F_s(\alpha_1, \alpha_2, \cdots, \alpha_{k-1}) \\
= & 0.
\end{aligned}
$$

□

Lemma 5.4.7. *Suppose $f(\lambda) \in PRM(r, m)$ such that $T_f \cup \{0\} \subseteq F_{2^m}$ is a subspace of dimension $k := m - r$ over F_2. Then*

$$f(\gamma^s) = F_s(\alpha_1, \alpha_2, \cdots, \alpha_k)$$

where γ is a primitive element of F_2^m, $1 \leq s \leq 2^m - 1$ and $\alpha_1, \alpha_2, \cdots, \alpha_k$ is a basis of $T_f \cup \{0\}$ over F_2.

Proof. Suppose $f = \lambda^{d_1} + \lambda^{d_2} + \cdots + \lambda^{d_{2^k-1}}$. Then $T_f \cup \{0\} = \{\gamma^{d_1}, \gamma^{d_2}, \ldots, \gamma^{d_{2^k-1}}, 0\}$ run through all possible linear combinations of $\alpha_1, \alpha_2, \cdots, \alpha_k$. Then by Lemma 5.4.5,

$$
\begin{aligned}
f(\gamma^s) &= (\gamma^s)^{d_1} + (\gamma^s)^{d_2} + \cdots + (\gamma^s)^{d_{2^k-1}} + 0 \\
&= \sum_{b \in F_{2^k}} (b_1\alpha_1 + b_2\alpha_2 + \cdots + b_k\alpha_k)^s \\
&= F_s(\alpha_1, \alpha_2, \cdots, \alpha_k).
\end{aligned}
$$

□

Corollary 5.4.8. *Let $\gamma \in F_{2^m}$ be a primitive element and $1 \leq s \leq 2^m - 1$. Then $f(\gamma^s) = 0$ for all $f \in PRM(r, m)$ with $T_f \cup \{0\}$ is a subspace of dimension $k = m - r$ over F_2 if and only if there are at most $(k-1)$ $1's$ in the binary expression of s.*

Proof. ($\Longleftarrow$) This is clear from Lemma 5.4.4 and Lemma 5.4.7.

($\Longrightarrow$) By Lemma 5.4.4, it suffices to show $F_s(\alpha_1, \alpha_2, \cdots, \alpha_k) = 0$ for any $\alpha_1, \alpha_2, \cdots \alpha_k \in F_{2^m}$. But the result is clear from Lemma 5.4.6 and Lemma 5.4.7. $\square$

5.5 The dimension of $PRM(r, m)$

Theorem 5.5.1.

$PRM(r,m) = span\{f(\lambda) \mid T_f \cup \{0\}$ is an $(m-r)-$subspace over $F_2\}/ < \lambda^{2^m-1} - 1 >$

and

$$\dim(PRM(r,m)) = \binom{m}{0} + \binom{m}{1} + \cdots + \binom{m}{r}.$$

Proof. Set

$$C = \text{ span } \{ \ f(\lambda) \ \mid \ T_f \cup \{0\} \ \text{ is an } (m-r) - \text{subspace of } F_2^m \text{ over } F_2 \ \}.$$

Clearly $C \subseteq PRM(r,m)$ by Definition 5.1.1. We have known that the $PRM(r,m)$ is essentially the codewords obtained by puncturing the first coordinate of the codewords in $RM(r,m)$. Hence

$$\dim(PRM(r,m)) \leq \dim(RM(r,m)) = \binom{m}{0} + \binom{m}{1} + \cdots + \binom{m}{r}.$$

To prove the theorem, it suffices to prove

$$\dim(C) \geq \binom{m}{0} + \binom{m}{1} + \cdots + \binom{m}{r}.$$

Similar to the proof of Theorem 5.2.10, we find C is cyclic. Hence

$$C = \{g(\lambda)h(\lambda) \mid \deg(h(\lambda)) \leq \dim(C) - 1)\},$$

where $g(\lambda)|\lambda^{2^m-1} - 1$. Since C is cyclic, we always can find a polynomial of degree $2^m - 2$ in C. Hence $\dim(C) \geq 2^m - 1 - \deg(g(\lambda))$. We need to prove

$$\deg(g(\lambda)) \leq 2^m - 1 - [\binom{m}{0} + \binom{m}{1} + \cdots + \binom{m}{r}].$$

This is equivalent to prove $\lambda^{2^m-1}-1$ has at least

$$\ell := \binom{m}{0} + \binom{m}{1} + \cdots + \binom{m}{r}$$

zero roots which are not zero roots of $g(\lambda)$. We need to check the number of γ^s with $g(\gamma^s) \neq 0$ is at least ℓ. Since $g(\lambda) \in C$ it suffices to show that there are at least ℓ elements of the form γ^s with $f(\gamma^s) \neq 0$ for any $f \in C$ such that $T_f \cup \{0\}$ is an $(m-r)$-subspace of F_2^m over F_2. By Corollary 5.4.8, if the binary expression of s contains at least $m-r$ 1's then we must have $f(\gamma^s) \neq 0$. The proof is finished since number of such s is

$$\binom{m}{m-r} + \binom{m}{m-r+1} + \cdots + \binom{m}{m} = \binom{m}{r} + \binom{m}{r-1} + \cdots + \binom{m}{0}.$$

$\square$

To end this section, we give some observations which are the main part of the thesis.

Note 5.5.2. The map $a \to \{0, a\}$ gives a $1-1$ correspondence between $F_2^m - \{0\}$ and the $1-$subspaces of F_2^m.

Note 5.5.3. From Theorem 5.5.1 and Note 5.5.2, $PRM(r,m)$ can be realized as the span of the columns of the incidence matrix of 1-subspaces and $(m-r)-$subspaces of F_2^m.

Note 5.5.4. By Theorem 4.2.16, $RM(r,m)$ can be realized as the span of the columns of the incidence matrix of affine 0-subspaces(points) and affine $(m-r)$-subspaces of F_2^m.

The following definition generalize $PRM(r,m)$ and $RM(r,m)$.

Definition 5.5.5. The *projective geometric codes of order k* over F_{q^m} is spanned by the columns of the incidence matrix of 1-subspaces of F_{q^m} and k-subspaces of F_{q^m}.

The *Euclidean geometric codes of order* k over F_q^m is spanned by the columns of the incidence matrix of points in F_q^m and affine k-subspaces of F_q^m.

By the above definition, $PRM(r, m)$ is a projective geometric code of order $m-r$ over $F_{2^m}^*$ and $RM(r, m)$ is an Euclidean geometric code of order $m-r$ over F_2^m.

5.6 Remarks

In view of Section 3.5 and Note 5.5.3, Note 5.5.4, it is interesting to ask what the linear span of a super-imposed code can be, and how to find a super-imposed subcode of a given linear code?

6

Hadamard matrices and bent functions

We introduce Hadamard matrices and bent functions in this chapter and show their links.

6.1 Hadamard matrices

Recall: $R_m := \{f \mid f : F_2^m \longrightarrow F_2 \text{ is a function }\}$.

Definition 6.1.1. For $f \in R_m$, we define the function $F : F_2^m \longrightarrow \mathbb{R}$ by $F(u) = \sum\limits_{v \in F_2^m} (-1)^{u \circ v + f(v)}$ where $u \circ v := u_1v_1 + u_2v_2 + \cdots + u_mv_m$ and $f(v) \in \{0, 1\}$ is viewed as real numbers. F is called the *Hadamard transform* of $\hat{f}$, where $\hat{f}(v) = (-1)^{f(v)}$ for all $v \in F_2^m$.

Hence f has value in F_2, $\hat{f}$ has value in $\{-1, 1\}$ and F has value in $\mathbb{R}$.

Note 6.1.2. In matrix forms, $H_m = \Big[\ (-1)^{u \circ v} \ \Big]_{2^m \times 2^m}$ and $\hat{f} = \Big[\ (-1)^{f(v)} \ \Big]_{2^m \times 1}$ $\Longrightarrow F = H_m\hat{f}$ is a matrix of size $2^m \times 1$.

Note 6.1.3. H_m is symmetric.

We give the first three H_m.

Example 6.1.4. $H_1 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}_{2\times 2}$

Example 6.1.5. $H_2 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}_{4\times 4} = H_1 \otimes H_1.$

Example 6.1.6.

$$
\begin{aligned}
H_3 &= \begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\
1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\
1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\
1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\
1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\
1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\
1 & -1 & -1 & 1 & -1 & 1 & 1 & -1
\end{pmatrix}_{8\times 8} \\
&= H_2 \otimes H_1 \\
&= H_1 \otimes H_2 \\
&= H_1 \otimes H_1 \otimes H_1.
\end{aligned}
$$

Definition 6.1.7. An $n \times n$ matrix H is a *Hadamard matrix* if $H^t H = nI$.

Lemma 6.1.8. *H_m is a Hadamard matrix.*

Proof.

$$\begin{aligned}
(H_m^t H_m)_{uv} &= \sum_{w\in F_2^m} (H_m^t)_{uw}(H_m)_{wv} \\
&= \sum_{w\in F_2^m} (H_m)_{wu}(H_m)_{wv} \\
&= \sum_{w\in F_2^m} (-1)^{w\circ(u+v)} \\
&= \begin{cases} 2^m, & \text{if } u=v; \\ 0, & \text{if } u\neq v, \end{cases}
\end{aligned}$$

where $u, v \in F_2^m$. $\square$

We use the Hadamard transform of $\hat{f}$ to determine the distance from f to $RM(1,m)$.

Theorem 6.1.9. *$d(f, RM(1,m)) = min\{\frac{2^m \pm F(u)}{2} \mid u \in F_2^m\}$ for all $f \in R_m$.*

Proof. Suppose a is the number of $(x_1, x_2, \cdots, x_m)$ such that $f-(u_1x_1+u_2x_2+\cdots+u_mx_m) = 1$ and b is the number of $(x_1, x_2, \cdots, x_m)$ such that $f-(u_1x_1+u_2x_2+\cdots+u_mx_m) = 0$, where $u_i, x_i \in F_2$ for $i \leq i \leq m$. Note $a+b = 2^m$. Observe for any $u = (u_1, u_2, \cdots, u_m) \in F_2^m$,

$$\begin{aligned}
& d(f, u_1x_1+u_2x_2+\cdots+u_mx_m) \\
= \; & d(f-(u_1x_1+u_2x_2+\cdots+u_mx_m), 0) \\
= \; & a \\
= \; & \frac{a+2^m-b}{2} \\
= \; & \frac{2^m - \sum_{(x_1,x_2,\cdots,x_m)\in F_2^m} (-1)^{f-(u_1x_1+u_2x_2+\cdots+u_mx_m)}}{2} \\
= \; & \frac{2^m - F(u)}{2},
\end{aligned}$$

and

$$
\begin{aligned}
& d(f, 1+u_1x_1+u_2x_2+\cdots+u_mx_m) \\
= \; & 2^m - d(f, u_1x_1+u_2x_2+\cdots+u_mx_m) \\
= \; & \frac{2^m+F(u)}{2}.
\end{aligned}
$$

The theorem follows from this. $\square$

Theorem 6.1.10. *$\rho(RM(1,m)) \leq 2^{m-1}-2^{\frac{m}{2}-1}$ and equality holds if and only if there exists $f \in R_m$ with $|F(u)| = \frac{m}{2}$ for all $u \in F_2^m$.*

Proof. Fix $f \in R_m$. Then

$$
\begin{aligned}
\sum_{u \in F_2^m} F(u)^2 &= F^tF \qquad (\text{ in matrix form}) \\
&= (H_m\hat{f})^t(H_m\hat{f}) \\
&= (\hat{f})^t {H_m}^t H_m \hat{f} \\
&= 2^m \hat{f}^t \hat{f} \\
&= 2^m \sum_{u \in F_2^m} (-1)^{2f(u)} \\
&= 2^{2m}.
\end{aligned}
$$

Hence there exists $u \in F_2^m$ such that $F(u)^2 \geq 2^m$. Hence $|F(u)| \geq 2^{\frac{m}{2}}$. Thus, $d(f, RM(1,m)) \leq \dfrac{2^m-2^{\frac{m}{2}}}{2}$ by Theorem 6.1.9. Hence

$$
\rho(RM(1,m)) = \max\{d(f,RM(1,m)) \mid f \in R_m\} \leq 2^{m-1}-2^{\frac{m}{2}-1}.
$$

The remaining is clear. $\square$

Corollary 6.1.11. *$\rho(RM(1,m)) = 2^{m-1}-2^{\frac{m}{2}-1}$ where m is even.*

Proof. This is clear from Theorem 4.5.5 and Theorem 6.1.10. $\square$

6.2 Bent functions

We introduce bent functions in this section and study their properties.

Definition 6.2.1. $f \in R_m$ is a bent function if $d(f, RM(1,m)) = 2^{m-1} - 2^{\frac{m}{2}-1}$.

From Theorem 6.1.10, we have the following two properties.

Note 6.2.2. $f \in R_m$ is a bent function if and only if $|F(u)| = 2^{\frac{m}{2}}$ for all $u \in F_2^m$.

Note 6.2.3. f is the farthest from the linear functions if $f \in R_m$ is a bent function.

Note 6.2.4. By Corollary 6.1.11, we obtain $\rho(RM(1,2)) = 1$.

We give an example as following.

Example 6.2.5. Consider the codewords of $RM(1,2)$ in Example 4.4.2. We obtain $0 = (0,0,0,0)$, $1 = (1,1,1,1)$, $x_1 = (0,1,0,1)$, $x_2 = (0,0,1,1)$, $1 + x_1 = (1,0,1,0)$, $1 + x_2 = (1,1,0,0)$, $x_1 + x_2 = (0,1,1,0)$ and $1 + x_1 + x_2 = (1,0,0,1)$. Any $f \in R_2 - RM(1,2)$ is a bent function in R_2.

The following theorem characterizes bent functions by using Hadamard matrices.

Theorem 6.2.6. *$f \in R_m$ is bent if and only if the $2^m \times 2^m$ matrix K with rows and columns indexed by F_2^m and uv-entry $K_{uv} := (-1)^{f(u+v)}$ is a Hadamard matrix.*

Proof. Observe

$$
\begin{aligned}
& (K^t K)_{uv} \\
= & \sum_{w \in F_2^m} K^t_{uw} K_{wv} \\
= & \sum_{w \in F_2^m} (-1)^{f(u+w)} \cdot (-1)^{f(w+v)} \\
= & \sum_{w \in F_2^m} \widehat{f}(u+w) \widehat{f}(w+v) \\
= & \frac{1}{2^{2m}} \sum_{w \in F_2^m} (H_m F)_{u+w} \cdot (H_m F)_{w+v} \quad (F = H_m \widehat{f} \text{ and } H_m H_m = 2^m I) \\
= & \frac{1}{2^{2m}} \sum_{w \in F_2^m} \Big(\sum_{x \in F_2^m} (H_m)_{u+w,x} F_x \Big) \Big(\sum_{y \in F_2^m} (H_m)_{w+v,y} F_y \Big) \\
= & \frac{1}{2^{2m}} \sum_{w \in F_2^m} \Big(\sum_{x \in F_2^m} (-1)^{(u+w)\circ x} F_x \Big) \Big(\sum_{y \in F_2^m} (-1)^{(w+v)\circ y} F_y \Big) \\
= & \frac{1}{2^{2m}} \sum_{x \in F_2^m} \sum_{y \in F_2^m} \Big(\sum_{w \in F_2^m} (-1)^{w \circ (x+y)} \Big) (-1)^{u \circ x + v \circ y} F_x F_y \\
= & \frac{2^m}{2^{2m}} \sum_{x \in F_2^m} (-1)^{(u+v)\circ x} |F_x|^2, \qquad (6.2.1)
\end{aligned}
$$

where $u, v \in F_2^m$.

($\Longrightarrow$) Suppose f is a bent function. Then $|F(x)|^2 = 2^m$ for all $x \in F_2^m$. Hence by 6.2.1

$$
\begin{aligned}
& (K^t K)_{uv} \\
= & \sum_{x \in F_2^m} (-1)^{(u+v)\circ x} \\
= & \begin{cases} 2^m, & u = v; \\ 0, & u \neq v, \end{cases}
\end{aligned}
$$

where $u, v \in F_2^m$.

($\Longleftarrow$) By Lemma 6.1.8, we obtain $K^tK = 2^mI$. Setting $u = 0$ in 6.2.1, we find

$$\begin{aligned}(K^tK)_{0v} &= \frac{1}{2^m}\sum_{x\in F_2^m}(-1)^{v\circ x}|F_x|^2 \\ &= \frac{1}{2^m}\sum_{x\in F_2^m}(H_m)_{vx}T_x \\ &= \frac{1}{2^m}(H_mT)_v,\end{aligned}$$

where T is a column vector with columns indexed by F_2^m and entry $|F_x|^2$ for each $x \in F_2^m$. Then

$$T = 2^mH_m^{-1}\begin{pmatrix}2^m\\0\\0\\\vdots\\0\end{pmatrix}_{2^m\times 1} = H_m\begin{pmatrix}2^m\\0\\0\\\vdots\\0\end{pmatrix}_{2^m\times 1} = \begin{pmatrix}2^m\\2^m\\\vdots\\2^m\end{pmatrix}_{2^m\times 1},$$

since the first column in H_m has all 1's entries. Hence $|F_x|^2 = 2^m$ for all $x \in F_2^m$. Then $|F_x| = 2^{\frac{m}{2}}$ for all $x \in F_2^m$. By Note 6.2.2, f is a bent function. $\square$

Our next goal is to prove that if $f \in R_m$ is a bent function, then $\deg(f) \le \frac{m}{2}$ with only exception $m = 2$.

Lemma 6.2.7. *Suppose $f(x_1, x_2, \cdots, x_m) \in R_m$ and $g(y_1, y_2, \cdots, y_n) \in R_n$ are bent functions. Then*

$$k(x_1, x_2, \cdots, x_m, y_1, y_2, \cdots, y_n) := f(x_1, x_2, \cdots, x_m) + g(y_1, y_2, \cdots, y_n) \in R_{m+n}$$

is a bent function.

Proof. View $w \in F_2^{m+n}$ as $w = (w_1, w_2)$ where $w_1 \in F_2^m$ and $w_2 \in F_2^n$. Then

$$\begin{aligned}
K(w) &:= \sum_{v=(v_1,v_2)\in F_2^{m+n}} (-1)^{w\circ v+k(v)} \\
&= \sum_{v_1\in F_2^m, v_2\in F_2^n} (-1)^{w_1\circ v_1+w_2\circ v_2+f(v_1)+g(v_2)} \\
&= (\sum_{v_1\in F_2^m} (-1)^{w_1\circ v_1+f(v_1)})(\sum_{v_2\in F_2^n} (-1)^{w_2\circ v_2+g(v_2)}) \\
&= F(w_1)G(w_2) \\
&= (\pm 2^{\frac{m}{2}})(\pm 2^{\frac{n}{2}}) \\
&= \pm 2^{\frac{m+n}{2}}
\end{aligned}$$

for all $w \in F_2^{m+n}$. Hence k is a bent function. □

Definition 6.2.8. For a linear code $C \subseteq F_2^m$, we define

$C^\perp := \{(t_1, t_2, \cdots, t_m) \mid t_1c_1 + t_2c_2 + \cdots + t_mc_m = 0$ for any $c = (c_1, c_2, \cdots, c_m) \in C\}$.

The following is from linear algebra.

Note 6.2.9. $\dim(C^\perp) = m - \dim(C)$ for $C \subseteq F_2^m$.

We give an example that $C \cap C^\perp \neq \emptyset$.

Example 6.2.10. Suppose $C=\{(0,0),(1,1)\}\subseteq F_2^2$. Then $C^\perp=\{(0,0),(1,1)\}\subseteq F_2^2$.

Theorem 6.2.11. *Suppose $C \subseteq F_2^m$ is a subspace. Then*

$$\sum_{u\in C} F(u) = |C| \sum_{v\in C^\perp} (-1)^{f(v)}.$$

Proof. It is clear for the case $C = \{0\}$. Suppose $C \neq 0$ and fix $v \notin C^\perp$. Define an onto function $t_v : C \longrightarrow F_2$ by $t_v(u) = u \circ v$. Then t_v is linear and $dim(ker(t_v)) = dim(C) - 1$. (In fact, $C/ker(t_v) \cong F_2$.) Thus $|t_v^{-1}(0)| = |t_v^{-1}(1)| = 2^{|C|-1}$. So, $\sum_{u\in C} (-1)^{u\circ v} = 0$.

Now

$$\begin{aligned}
\sum_{u\in C} F(u) &= \sum_{u\in C}\sum_{v\in F_2^m} (-1)^{u\circ v+f(v)} \\
&= \sum_{v\in F_2^m}\sum_{u\in C}(-1)^{u\circ v+f(v)} \\
&= \sum_{v\in C^\perp}\sum_{u\in C}(-1)^{u\circ v+f(v)} + \sum_{v\notin C^\perp}\sum_{u\in C}(-1)^{u\circ v+f(v)} \\
&= \sum_{v\in C^\perp}(-1)^{f(v)}|C| + \sum_{v\notin C^\perp}(-1)^{f(v)}(\sum_{u\in C}(-1)^{u\circ v}) \\
&= |C|\sum_{v\in C^\perp}(-1)^{f(v)}.
\end{aligned}$$

□

The following Lemma is a similar version of Theorem 4.3.8.

Lemma 6.2.12. *Suppose* $f = \sum_{\rho\subseteq[m]} f_\rho x_\rho \in R_m$ *for some* $f_\rho \in F_2$. *Then*

$$f_\sigma = \sum_{w\in(1,1,\cdots,1)+S_{\overline{\sigma}}} f(w)$$

for any $\sigma \subseteq [m]$ *with* $|\sigma| \leq \deg(f)$.

Proof. If $\deg(f) = |\sigma|$, then we have shown in Theorem 4.3.8,

$$f_\sigma = \sum_{w\in(1,1,\cdots,1)+S_{\overline{\sigma}}} f(w).$$

Observe

$$\begin{aligned}
& w \in (1,1,\cdots,1) + S_{\overline{\sigma}}. \\
\Longleftrightarrow\ & w_i = 0 \text{ for } i \notin \sigma. \\
\Longrightarrow\ & x_\rho(w) = 0 \text{ for any } |\rho| > |\sigma|.
\end{aligned}$$

Hence the statement is true for any σ with $|\sigma| \leq \deg(f)$. □

Theorem 6.2.13. *If* $f \in R_m$ *is a bent function, then* $f \in RM(\frac{m}{2}, m)$, *where* $m > 2$ *is even.*

Proof. Suppose $f = \sum\limits_{\rho \subseteq [m]} f_\rho x_\rho$ for $f_\rho \in F_2$. Let $\sigma \subseteq \{1, 2, \cdots, m\}$ with $|\sigma| > \frac{m}{2}$. We want to show $f_\sigma = 0$ with referring to notation in Definition 4.3.1, set $C = (1, 1, \cdots, 1) + S_{\overline{\sigma}}$. Observe $C \subseteq F_2^m$ is a subspace, $|C| = 2^{|\sigma|}$ and $|C^\perp| = 2^{m-|\sigma|}$. Note $F(u) = C_u 2^{\frac{m}{2}}$ for some $C_u \in \{-1, 1\}$, since f is a bent function write $(-1)^{t(u)} = C_u$ or equivalently $C_u = 1 - 2t(u)$, where $t(u) \in F_2$. Then by Lemma 6.2.12 and Theorem 6.2.11,

$$
\begin{aligned}
f_\sigma &= \sum_{u \in C} f(u) \\
&= \sum_{u \in C} \frac{1 - (-1)^{f(u)}}{2} \\
&= \frac{|C|}{2} - \frac{1}{2} \sum_{u \in C} (-1)^{f(u)} \\
&= \frac{|C|}{2} - \frac{1}{2|C^\perp|} \sum_{u \in C^\perp} F(u) \\
&= \frac{|C|}{2} - \frac{1}{2|C^\perp|} \sum_{u \in C^\perp} C_u 2^{\frac{m}{2}} \\
&= 2^{|\sigma|-1} - 2^{\frac{m}{2}-1} + 2^{|\sigma|-\frac{m}{2}} \sum_{u \in C^\perp} t(u) \\
&= 0.
\end{aligned}
$$

$\square$

7

Hexacode and Extended Binary Golay Code

7.1 Hexacode

In this section, we fix a finite field $F_4 = \{0, 1, x, 1+x\}$ where the multiplication is modulo $x^2 + x + 1$.

Definition 7.1.1. The map $- : F_4 \longrightarrow F_4$ is defined by

$$\overline{0} = 0,\ \overline{1} = 1,\ \overline{x} = x+1,\ \overline{x+1} = x$$

and $-$ is called the *conjugate map* in F_4.

The conjugate has similar properties as in $\mathbb{C}$.

Note 7.1.2. $a \cdot \overline{a} \in F_2$, $\overline{ab} = \overline{a} \cdot \overline{b}$, $\overline{a+b} = \overline{a} + \overline{b}$ and $\overline{\overline{a}} = a$ for any $a, b \in F_4$.

Definition 7.1.3. For any $(u_1, u_2, \cdots, u_n) \in F_4^n,\ (v_1, v_2, \cdots, v_n) \in F_4^n$,

$$u \bullet v := u_1\overline{v_1} + u_2\overline{v_2} + \cdots + u_n\overline{v_n}$$

is called the *Hermition inner product* of u and v.

Definition 7.1.4.

$$HC = \text{span}\{(1,0,0,1,x,\overline{x}),(0,1,0,1,\overline{x},x),(0,0,1,1,1,1)\} \subseteq F_4^6$$

is called the *Hexacode* over F_4.

Note 7.1.5. The length of HC is 6 and the dimension of HC is 3 and $HC^{\perp} = HC$.

Lemma 7.1.6. *The minimum distance $d(HC)$ is 4.*

Proof. Since $HC^{\perp} = HC$, we obtain

$$HC = \{(a_1,a_2,a_3,a_4,a_5,a_6) \mid (a_1,a_2,a_3,a_4,a_5,a_6)\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \\ \overline{x} & x & 1 \\ x & \overline{x} & 1 \end{pmatrix}_{6\times 3} = 0\}.$$

Hence

$$\begin{aligned} d(HC) &= \text{the minimum } wt(w) \text{ where } 0 \neq w \in HC \\ &= \text{the least number of rows in } \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \\ \overline{x} & x & 1 \\ x & \overline{x} & 1 \end{pmatrix}_{6\times 3} \text{ that are linear dependent} \\ &= 4. \end{aligned}$$

□

Note 7.1.7. HC is $[6,3,4]-$linear code over F_4. Hence $d = n - k + 1$.

Definition 7.1.8. An $[n, k, d]-$linear code with $d = n - k + 1$ is called a *maximum distance separable code*. (MDS code.)

Note 7.1.9. Let PHC be the code obtained by puncturing a coordinate of HC. Then PHC is $[5, 3, 3]-$linear code.

Note 7.1.10. An $[n, k, d]-$ linear code over F_q is *perfect* if

$$q^k \sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \begin{pmatrix} n \\ i \end{pmatrix} (q-1)^i = q^n.$$

Note 7.1.11. By direct computation we have that PHC is perfect.

Type (i)	Type (i)	Type (i)
$(0,1,0,1,\overline{x},x)$	$(0,x,0,x,1,\overline{x})$	$(0,\overline{x},0,\overline{x},x,1)$
$(0,1,\overline{x},x,0,1)$	$(0,x,1,\overline{x},0,x)$	$(0,\overline{x},x,1,0,\overline{x})$
$(\overline{x},x,0,1,0,1)$	$(1,\overline{x},0,x,0,x)$	$(x,1,0,\overline{x},0,\overline{x})$
$(0,1,1,0,x,\overline{x})$	$(0,x,x,0,\overline{x},1)$	$(0,\overline{x},\overline{x},0,1,x)$
$(0,1,x,\overline{x},1,0)$	$(0,x,\overline{x},1,x,0)$	$(0,\overline{x},1,x,\overline{x},0)$
$(\overline{x},x,1,0,1,0)$	$(1,\overline{x},x,0,x,0)$	$(x,1,\overline{x},0,\overline{x},0)$
$(1,0,0,1,x,\overline{x})$	$(x,0,0,x,\overline{x},1)$	$(\overline{x},0,0,\overline{x},1,x)$
$(1,0,\overline{x},x,1,0)$	$(x,0,1,\overline{x},x,0)$	$(\overline{x},0,x,1,\overline{x},0)$
$(x,\overline{x},0,1,1,0)$	$(\overline{x},1,0,x,x,0)$	$(1,x,0,\overline{x},\overline{x},0)$
$(1,0,1,0,\overline{x},x)$	$(x,0,x,0,1,\overline{x})$	$(\overline{x},0,\overline{x},0,x,1)$
$(1,0,x,\overline{x},0,1)$	$(x,0,\overline{x},1,0,x)$	$(\overline{x},0,1,x,0,\overline{x})$
$(x,\overline{x},1,0,0,1)$	$(\overline{x},1,x,0,0,x)$	$(1,x,\overline{x},0,0,\overline{x})$
Type (ii)	Type (ii)	Type (ii)
$(\overline{x},x,\overline{x},x,\overline{x},x)$	$(1,\overline{x},1,\overline{x},1,\overline{x})$	$(x,1,x,1,x,1)$
$(\overline{x},x,x,\overline{x},x,\overline{x})$	$(1,\overline{x},\overline{x},1,\overline{x},1)$	$(x,1,1,x,1,x)$
$(x,\overline{x},\overline{x},x,x,\overline{x})$	$(\overline{x},1,1,\overline{x},\overline{x},1)$	$(1,x,x,1,1,x)$
$(x,\overline{x},x,\overline{x},\overline{x},x)$	$(\overline{x},1,\overline{x},1,1,\overline{x})$	$(1,x,1,x,x,1)$
Type (iii)	Type (iii)	Type (iii)
$(0,0,1,1,1,1)$	$(0,0,x,x,x,x)$	$(0,0,\overline{x},\overline{x},\overline{x},\overline{x})$
$(1,1,0,0,1,1)$	$(x,x,0,0,x,x)$	$(\overline{x},\overline{x},0,0,\overline{x},\overline{x})$
$(1,1,1,1,0,0)$	$(x,x,x,x,0,0)$	$(\overline{x},\overline{x},\overline{x},\overline{x},0,0)$
Type (iv)	Type (iv)	Type (iv)
$(1,1,x,x,\overline{x},\overline{x})$	$(x,x,\overline{x},\overline{x},1,1)$	$(\overline{x},\overline{x},1,1,x,x)$
$(1,1,\overline{x},\overline{x},x,x)$	$(x,x,1,1,\overline{x},\overline{x})$	$(\overline{x},\overline{x},x,x,1,1)$

Table 7.1 List all nonzero elements of Hexacode.

F_2.

Type	Representative	Number of codewords
(i)	$(0,1,0,1,\overline{x},x)$	36
(ii)	$(\overline{x},x,\overline{x},x,\overline{x},x)$	12
(iii)	$(0,0,1,1,1,1)$	9
(iv)	$(1,1,x,x,\overline{x},\overline{x})$	6

We divide the coordinates of each codeword into three blocks I, II, III, where block I (resp. II) (resp. III) contains coordinates $1,2$ (resp. $3,4$) (resp. $5,6$), like

$$\Big(\ \underset{\text{I}}{\underline{a\ ,\ b}},\ \ \underset{\text{II}}{\underline{c\ ,\ d}},\ \ \underset{\text{III}}{\underline{e\ ,\ f}}\ \Big)\ .$$

The codewords in each type are preserved by (a) a nonzreo scalor multiplication; (b) the permutation of blocks I, II, III, (c) the switch of the two coordinates in each of two blocks. Hence the number of type (i) codewords is 36, the number of type (ii) codewords is 12, the number of type (iii) codewords is 9 and the number of type (iv) codewords is 6.

Example 7.1.12. If $(c_1,c_2,c_3,c_4,c_5,c_6) \in HC$, then

$$(xc_1,xc_2,xc_3,xc_4,xc_5,xc_6),\ (c_3,c_4,c_1,c_2,c_5,c_6),\ (c_1,c_2,c_4,c_3,c_6,c_5)$$

all have the same type as $(c_1,c_2,c_3,c_4,c_5,c_6)$ in HC.

7.2 Extended Binary Golay Code

We use Hexacode to define the extended binary Golay code in this section.

Definition 7.2.1. For a vector $u = (u_1,u_2,\cdots,u_n) \in F_2^n$, the *parity* of u is $\sum\limits_{i=1}^{n} u_i \in F_2$.

Definition 7.2.2. Let $F_2^{4\times 6}$ denoted the set of 4×6 matrices over F_2.

$$EBGC := \{A \in F_2^{4\times 6} \quad | \quad (0,1,x,\overline{x})A \in HC \text{ and each column of } A \text{ has the same parity as the first row}\}$$

is called the *Extended Binary Golay code.* Parity(A), the parity of the first row of A, is called the *parity* of A over F_2.

Example 7.2.3. Suppose the matrix

$$A = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}_{4\times 6}$$

over $F_2^{4\times 6}$. Then $(0,1,x,\overline{x})A = (0,1,0,1,\overline{x},x)$ is the type (i) of HC and parity(A)=1 over F_2. Hence $A \in EBGC$.

The following property will be used later.

Note 7.2.4. Suppose

$$(0,1,x,\overline{x}) \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = y$$

for some $y \in \{0,1,x,\overline{x}\}$. The number of solution of such $(a,b,c,d) \in F_2^4$ has 2 with odd parity and 2 with even parity over F_2.

Example 7.2.5. Suppose $y = 0$ in Note 7.2.4. Then

$$\begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

has even parity and

$$\begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

has odd parity over F_2.

Theorem 7.2.6. *The EBGC is* $[24, 12, 8]-$*linear code over* F_2.

Proof. Clearly the codewords of $EBGC$ has length $24 = 4 \times 6$. We prove

$$dim(EBGC) = 12$$

by showing $|EBGC| = 2^{12}$. Note $|HC| = 64 = 2^6$. First, we count those $A \in EBGC$ with even parity over F_2. For each $u \in HC$, to determine A with $(0, 1, x, \overline{x})A = u$ and Parity(A)=0, there are two choices for each of the first 5 columns of A by Note 7.2.4, however there is only one choice for the last column to have parity 0 in the first row. Hence there are 2^{11} such $A \in EBGC$ with parity$(A) = 0$. Similarly for the number of $A \in EBGC$ with Parity$(A) = 1$. Hence

$$|EBGC| = 2^{12}.$$

Claim: $d(EBGC) = 8$. Fix $A \in EBGC$ with $A \neq 0$.

Case 1: Parity$(A) = 0$ and $(0, 1, x, \overline{x})A \neq 0$: Since HC is $[6, 3, 4]-$linear code, by $d(HC) = wt((0, 1, x, \overline{x})A) \geq 4$. And since the column of A has even weight, $wt(A) \geq 4 \times 2 = 8$.

Case 2: Parity$(A) = 0$ and $(0, 1, x, \overline{x})A = 0$: Observe since the columns of A has even weight and $(0, 1, x, \overline{x})A = 0$, there is at least one column of A is $\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$.

But the first row of A has even parity. Then A has at least 2 such columns. Hence $wt(A) \geq 8$.

Case 3: Parity$(A) = 1$ and $(0, 1, x, \overline{x})A \neq 0$: Suppose $wt(A) < 8$. Since parity$(A) = 1$, there are at most two kinds of weights of the columns in A, one has weight 1 and the other has weight 3. In fact every column has weight 1, since we assume $wt(A) < 8$. Note that $wt((0, 1, x, \overline{x})A) \geq 4$ by Note 7.1.7. Hence the first row of A has weight 1. This implies $wt((0, 1, x, \overline{x})A) = 5$. But there is no Hexacodeword of weight 5 from Table 7.1. Then $wt(A) \geq 8$.

Case 4:Parity$(A) = 1$ and $(0, 1, x, \overline{x})A = 0$: Each column has weight at least 1 and the parity of the first row of A is 1 such that there is at least a column of weight 3. Hence A has weight at least 8.

$\square$

7.3 Decoding in Extended Binary Golay Code

Note 7.3.1. Suppose $(0, 1, x, \overline{x})\begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \end{pmatrix} = (0, 1, x, \overline{x})\begin{pmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \end{pmatrix}$ and $\sum_{i=1}^{4} a_i = \sum_{i=1}^{4} b_i$ in F_2. Then $a_i = b_i$ for all i or $a_i = \overline{b_i}$ for all i in F_2.

Note 7.3.2. With restriction to any 3 positions in the basis of HC, the 3 vectors are still linear independent.

Note 7.3.3. We know each Hexacodeword from its three positions.

Suppose we receive a codeword A and assume at most 3 errors in A where $A \in EBGC$.

Decoding Algorithm

(1) Compute the parity on each column of A.

Case 1: At least 4 columns with the same parity. Then these columns have correct parity and they might still have errors in these columns.

Case 1.1: There are 4 columns with the same parity. Go to (2).

Case 2: 3 columns with odd parity and 3 columns with even parity. Guess any one of the parity. Go to (2).

(2) Project the columns you think are correct in A into a partition of a Hexacodeword. Since a Hexacodeword is unique determined by its three positions, this partition will determine the complete Hexacodeword, possible with some correction. If there is no such Hexacodeword in Table 7.1, then we have wrong guess in Case 2, so we guess again the parity and do the process (2) again.
(3) Use the Hexacodeword obtained in (2) to determine the correct A by using the correct parity information.

Example 7.3.4. Receive $A = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \end{pmatrix}_{4\times 6}$, and assume at most 3 errors in A. We do the following.
(1) Guess those columns with odd parity are with correct parity.
(2) Observe $(0, 1, x, \overline{x}) \begin{pmatrix} * & 0 & * & 0 & 0 & * \\ * & 0 & * & 0 & 0 & * \\ * & 0 & * & 1 & 0 & * \\ * & 1 & * & 0 & 1 & * \end{pmatrix}_{4\times 6} = (*, \overline{x}, *, x, \overline{x}, *)$ is contained in type(i) of HC in Table 7.1. Suppose the Hexacodeword is $(0, \overline{x}, 1, x, \overline{x}, 0)$.
(3) Hence $A = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \end{pmatrix}_{4\times 6}$, but the first row has parity 0. Hence guess Wrongly, so we reguess again.

(1) Guess those columns with even parity are with correct parity.

(2) Observe $(0,1,x,\overline{x})\begin{pmatrix}1 & * & 1 & * & * & 1\\ 0 & * & 1 & * & * & 0\\ 1 & * & 0 & * & * & 0\\ 0 & * & 0 & * & * & 1\end{pmatrix}_{4\times 6} = (\overline{x},*,1,*,*,\overline{x})$ is contained in type(i) of HC in Table 7.1. Then the Hexacodeword is $(\overline{x},0,1,x,0,\overline{x})$.

(3) Hence $A = \begin{pmatrix}1 & 0 & 1 & 1 & 0 & 1\\ 0 & 0 & 1 & 0 & 0 & 0\\ 1 & 0 & 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 1\end{pmatrix}_{4\times 6}$ is correct by checking the parity.

Note 7.3.5. Under at most 3 errors in the codeword A assumption, the decoding algorithm will find the exact codeword A. The reason is the minimum distance of $EBGC$ is 8.

7.4 Remarks

The definition of extended binary Golay code is not standard. We refer the reader to standard text books [14],[1] of coding theory for the definition.

8

Convolutional Codes

A convolutional code is a code over rational functions. This will be clear after we see some definitions and notations.

8.1 Definition

Definition 8.1.1.

$$F_q[x] := \{a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \mid a_i \in F_q, n \in \mathbb{N} \cup \{0\}\}$$

is the set of *polynomials* over F_q.

Definition 8.1.2.

$$F_q(x) := \{f(x)/g(x) \mid f(x), g(x) \in F_q[x] \text{ and } g(x) \neq 0\}$$

is the set of *rational functions* over F_q. Note that $F_q(x)$ is a field.

Definition 8.1.3.

$$F_q((x)) := \{\sum_{i=M}^{\infty} a_ix^i \mid a_i \in F_q \text{ and } M \in \mathbb{Z}\}$$

is the set of *formal power series*.

Note 8.1.4. $F_q(x) \subsetneq F_q((x))$. $F_q(x) \neq F_q((x))$ since they have different cardinality.

Example 8.1.5.

$$\begin{aligned} \frac{1}{x^5(1-x^2)} &= x^{-5}(1+x^2+x^4+\cdots) \\ &= x^{-5}+x^{-3}+x^{-1}+x+x^3+\cdots. \end{aligned}$$

8.2 Convolutional Code

We give the definition of convolutional code now.

Definition 8.2.1. A subspace $CV \subseteq F_q(x)^n$ with dimension k over $F_q(x)$ is called an $[n, k] -$ *convolutional code*.

Although a codeword is an element in $F_q(x)^n$, we prefer the basis of CV is chosen from $F_q[x]^n$.

Definition 8.2.2. $G(x) \in F_q[x]^{k\times n}$ is a *polynomial generating matrix* (PGM) of CV if the rows of $G(x)$ span CV.

Lemma 8.2.3. *Let $CV \subseteq F_q(x)^n$ be a $k-$subspace. Then there exists a basis*

$$G_1(x), G_2(x), \cdots, G_k(x) \in F_q[x]^n$$

of CV.

Proof. Let

$$(g_{11}(x)/h_{11}(x), g_{12}(x)/h_{12}(x), \cdots, g_{1n}(x)/h_{1n}(x)),$$

$$(g_{21}(x)/h_{21}(x), g_{22}(x)/h_{22}(x), \cdots, g_{2n}(x)/h_{2n}(x)),$$

$$\vdots$$

$$(g_{k1}(x)/h_{k1}(x)g_{k2}(x)/h_{k2}(x), \cdots, g_{kn}(x)/h_{kn}(x))$$

$\in F_q(x)^n$ be a basis of CV, where $g_{ij}(x)$,$h_{ij}(x) \in F_q[x]$. Let $h(x)$ be the least common multiple of $h_{ij}(x)$. Set $G_{ij} = h(x) \cdot \dfrac{g_{ij}(x)}{h_{ij}(x)}$. Then

$$G_i(x) := (G_{i1}(x), G_{i2}(x), \cdots, G_{in}(x)) \in F_q[x]^n,$$

and $G_1(x), G_2(x), \cdots, G_k(x) \in F_q[x]^n$ is a basis of CV. $\square$

Observe $CV = \{S(x)G(x) \mid S(x) \in F_q(x)^k\}$. So we want $G(x)$ as "simple" as possible. The following identification is used when we want to apply CV to real world application.

Note 8.2.4. $F_q[x]^k \cong F_q^k[x]$.

Example 8.2.5. Suppose $k = 3$. Then

$$(1+x, 1+x^2, x+x^3) = (1,1,0) + (1,0,1)x + (0,1,0)x^2 + (0,0,1)x^3.$$

8.3 Elementary rows and columns operations on $G(x)$

Three *elementary rows and columns operations* ($ERCO$'s) are as following:

(a) Interchange two columns(rows).

$\Longrightarrow det(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}) = -1.$

(b) Add a polynomial $f(x) \in F_q[x]$ multiple a column(row) to another column(row).

$\Longrightarrow det(\begin{pmatrix} 1 & 0 \\ f(x) & 1 \end{pmatrix}) = 1.$

(c) Multiple a column(row) by a nonzero element $\alpha \in F_q$

$\Longrightarrow det(\begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix}) = \alpha.$

The matrices corresponding to *ERCO*'s are called *elementary matrices*. In the 2×2 cases, there are matrices of the forms $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ f(x) & 1 \end{pmatrix}$, $\begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix}$, where $f(x) \in F_q[x]$ and $\alpha \in F_q$. The determinant of a elementary matrix is an element in F_q.

Definition 8.3.1. An $t \times t$ matrix $U(x)$ over $F_q[x]$ is *unimodular* if $0 \neq det(U(x)) \in F_q$.

We will show that each unimodular matrix is the product of elementary matrices.

Theorem 8.3.2. *(Smith normal form theorem(SNF)) Let $G(x)$ be an $k \times n$ matrix over $F_q[x]$. Then $G(x)$ can be reduced to*

$$\begin{pmatrix} d_1(x) & & & & & & \\ & d_2(x) & & & 0 & & \\ & & \ddots & & & & \\ & & & d_s(x) & & & \\ & & & & 0 & & \\ & 0 & & & & \ddots & \\ & & & & & & 0 \end{pmatrix}_{k \times n}$$

by ERCO's where $d_1(x)|d_2(x)|\cdots|d_s(x)$ are monic polynomial over F_q. The sequence $d_1(x), d_2(x), \cdots, d_s(x)$ is called the sequence of invariant factors of $G(x)$.

Proof. Suppose $G(x) = \begin{pmatrix} G_{11}(x) & G_{12}(x) & \cdots & G_{1n}(x) \\ G_{21}(x) & G_{22}(x) & \cdots & G_{2n}(x) \\ & \vdots & & \\ G_{k1}(x) & G_{k2}(x) & \cdots & G_{kn}(x) \end{pmatrix}_{k \times n}$. We do the following.

(a) Using rows interchanging and column interchanging, we assume $G_{11}(x)$ has minimal degree.

(b) Reduce the degree of $G_{1i}(x)$ for $i \geq 2$ by adding a polynomial multiple of the first column to the ith column. Go to (a) until $G_{1i}(x) = 0$ for $i \geq 2$.

(c) Similar to (a)∼(b), we do until $G_{j1}(x) = 0$ for $j \geq 2$.

(d) After (c), it could be $G_{1i}(x) \neq 0$. So do (a),(b),(c) again and again, until $G_{1i}(x) = 0$ and $G_{j1}(x) = 0$ for all $i, j \geq 2$.

(e) If $G_{11}(x) \nmid G_{ij}(x)$ for some i, j, then we add the first column to jth column and then add a polynomial multiple of the first row to decrease the degree of $G_{ij}(x)$ below the degree of $G_{11}(x)$. Repeat doing (a)∼(e) until $G_{11}(x)|G_{ij}(x)$ and $G_{11}(x)$ is monic.

(f) Do (a)∼(e) in the submatrix $G'(x)$ where

$$G(x) = \begin{pmatrix} G_{11}(x) & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & G'(x) & \\ 0 & & & \end{pmatrix}_{k \times n}$$

□

Example 8.3.3. Suppose $G(x) = \begin{pmatrix} x & x^2 \\ x^3 & x^4 \end{pmatrix}_{2\times 2}$. Then $d_1(x) = x$ and $d_2(x) = 0$.

Corollary 8.3.4. *An unimodular matrix is a product of elementary matrices.*

Proof. Let $U(x)$ be an $t \times t$ unimodular matrix. Then

$$U(x) = E(x) \begin{pmatrix} d_1(x) & & & 0 \\ & d_2(x) & & \\ & & \ddots & \\ 0 & & & d_t(x) \end{pmatrix}_{t \times t} F(x),$$

where $E(x), F(x)$ are product of elementary matrices. Hence

$$det(U(x)) = det(E(x))det(F(x))d_1(x)d_2(x)\cdots d_t(x) \in F_q - \{0\}.$$

Thus

$$d_i = d_i(x) \in F_q - \{0\} \text{ for } i = 1, 2, \cdots, t$$

and

$$U(x) = E(x) \begin{pmatrix} d_1 & & & & 0 \\ & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ 0 & & & & 1 \end{pmatrix}_{t\times t} \begin{pmatrix} 1 & & & & 0 \\ & d_2 & & & \\ & & 1 & & \\ & & & \ddots & \\ 0 & & & & 1 \end{pmatrix}_{t\times t} \cdots \begin{pmatrix} 1 & & & & 0 \\ & 1 & & & \\ & & \ddots & & \\ & & & 1 & \\ 0 & & & & d_t \end{pmatrix}_{t\times t} F(x).$$

□

We need more notations of matrices.

Definition 8.3.5. Let A be an $n \times m$ matrix, $\alpha \subseteq [n]$ and $\beta \subseteq [m]$. We define $A[\alpha \mid \beta]$ to be the submatrix of A with size $|\alpha| \times |\beta|$, the rows in α and columns in β of A being chosen.

Example 8.3.6. Suppose $A = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 6 & 1 & 7 & 8 \\ 3 & 1 & 0 & 1 & 2 \end{pmatrix}_{3\times 5}$. Then

$$A[\{1,3\} \mid \{2,4,5\}] = \begin{pmatrix} 2 & 4 & 5 \\ 1 & 1 & 2 \end{pmatrix}_{2\times 3}.$$

Definition 8.3.7. Similarly to the Definition 8.3.5, we define $(a)-(e)$ as the following.

(a) $A[- \mid \beta] := A[\ [n] \mid \beta]$.

(b) $A[\alpha \mid -] := A[\alpha \mid [m]\ ]$.

(c) $A(\alpha \mid \beta) := A[\overline{\alpha} \mid \overline{\beta}]$.

(d) $A(\alpha \mid \beta] := A[\overline{\alpha} \mid \beta]$.

(e) $A[\alpha \mid \beta) := A[\alpha \mid \overline{\beta}]$.

We quote a theorem without proof.

Theorem 8.3.8. *(Cauchy Binet Theorem) Let A,B be the matrices of size $n \times m$ and $m \times t$, respectively. Then*

$$det(AB[\alpha \mid \beta]) = \sum_{w \subseteq [m], |w| = |\alpha|} (detA[\alpha \mid w])(detB[w \mid \beta])$$

when $\alpha \subseteq [n], \beta \subseteq [t]$ with $|\alpha| = |\beta|$. □

Note 8.3.9. We give two special cases of Cauchy Binet Theorem.

(a) Suppose $\alpha = \{i\}$ and $\beta = \{j\}$. Then $(AB)_{ij} = \sum_{k=1}^{m} A_{ik}B_{kj}$.

(b) Suppose $\alpha = [n], \beta = [t]$ and $n = t = m$. Then $det(AB) = det(A)det(B)$.

Definition 8.3.10. $detA[\alpha \mid \beta]$ is called an $|\alpha|$-*minor* when $|\alpha| = |\beta|$.

Example 8.3.11. Suppose $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}_{2\times 2}$. Then $1, 2, 3, 4$ are 1-minors and -2 is 2-minor.

Corollary 8.3.12. *Let $G(x)$ be an $k \times n$ matrix over $F_q[x]$. Then the invariant factors $d_1(x), d_2(x), \cdots, d_s(x)$ of $G(x)$ are unique. In fact,*

$$d_i(x) = \frac{k_i(x)}{k_{i-1}(x)}$$

for $i = 1, 2, \cdots, s$ where $k_0(x) := 1$ and $k_i(x) :=$ the greatest common divisor of i-minors of $G(x)$.

Proof. Suppose $G(x) = E(x)D(x)F(x)$ where

$$D(x) = \begin{pmatrix} d_1(x) & & & & & & \\ & d_2(x) & & & 0 & & \\ & & \ddots & & & & \\ & & & d_s(x) & & & \\ & & & & 0 & & \\ & 0 & & & & \ddots & \\ & & & & & & 0 \end{pmatrix}_{k\times n}$$

in smith normal form and $E(x), F(x)$ are unimodular. By Theorem 8.3.8, $k_i^D(x) \mid k_i(x)$ where $k_i^D(x)$ is the greatest common divisor of i-minors of $D(x)$. Note $D(x) = E(x)^{-1}G(x)F(x)^{-1}$ and $E(x)^{-1}, F(x)^{-1}$ are polynomial matrices. Hence again,

$$k_i(x) \mid k_i^D(x).$$

Thus for $1 \leq i \leq s$,

$$k_i(x) = k_i^D(x) = d_1(x)d_2(x)\cdots d_i(x).$$

Then for $1 \leq i \leq s$,

$$d_i(x) = \frac{k_i(x)}{k_{i-1}(x)}.$$

□

We see an example as following.

Example 8.3.13.

$$\text{Suppose } A(x) = \begin{pmatrix} x & x^2 & x^3 \\ x & 1 & x^2 \\ x^2 & x & x^3 \end{pmatrix}_{3\times 3}.$$

$$\begin{aligned}
k_1(x) &= gcd\ \{x, x^2, x^3, x, 1, x^2, x^2, x, x^3\} = 1, \\
k_2(x) &= gcd\ \{x - x^3, x^3 - x^4, x^4 - x^3, x^2 - x^4, x^4 - x^5, x^5 - x^4, 0\} = x - 1, \\
k_3(x) &= x^4 - x^6 - x^5 - x^5 - x^6 - x^4 = 0.
\end{aligned}$$

Then $d_1(x) = \dfrac{1}{1} = 1, d_2(x) = \dfrac{x-1}{1} = x - 1, d_3(x) = \dfrac{0}{x-1} = 0$. Hence, $1, x - 1$ are invariant factors.

In the following, we introduce some PGM of a CV code which has good properties.

Definition 8.3.14. Let $G(x)$ be a $k \times n$ PGM of some CV. Then the maximum degree of k-minors of $G(x)$ is called *internal degree* of $G(x)$.

Example 8.3.15. Suppose $G(x) = (1 + x^2, 1 + x + x^2)$. Then

$$\text{int deg}(G(x)) = \max\{\deg(1 + x^2), \deg(1 + x + x^2)\} = 2.$$

Example 8.3.16. Suppose $G(x) = \begin{pmatrix} 1 & 0 & 1+x \\ 0 & 1 & x \end{pmatrix}_{2\times 3}$. Then

$$\text{int}\ \deg(G(x)) = \max\{\deg(1), \deg(x), \deg(-x-1)\} = 1.$$

Definition 8.3.17. A PGM $G(x)$ is *basic* in CV if $G(x)$ has the smallest internal degree among all PGM of CV.

Before giving the characterization of basic PGM, we need some background from linear algebra.

Definition 8.3.18. Let A be an $n \times n$ matrix. Then $adj(A)$ is an $n \times n$ matrix defined by $(adj(A))_{ij} := (-1)^{i+j} A(\{j\} \mid \{i\})$.

Example 8.3.19. Suppose $A = \begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix}_{2\times 2}$. Then $adj(A) = \begin{pmatrix} 4 & -3 \\ -2 & 1 \end{pmatrix}_{2\times 2}$.

Note 8.3.20. *(Cramer's Rule)* $A \cdot adj(A) = adj(A) \cdot A = \det(A) \cdot I$.

Example 8.3.21.

$$\begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix} \begin{pmatrix} 4 & -3 \\ -2 & 1 \end{pmatrix} = \begin{pmatrix} 4 & -3 \\ -2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix}$$
$$= \begin{pmatrix} -2 & 0 \\ 0 & -2 \end{pmatrix} = \det(\begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix}) \cdot I_2.$$

Theorem 8.3.22. *Suppose $G(x)$ is an $k \times n$ PGM of $CV \subseteq F_q(x)^n$. Then the following are equivalent.*

(a) *$G(x)$ is basis.*

(b) *Invariant factor of $G(x)$ are all 1's.*

(c) *gcd of k-minors of $G(x)$ is 1.*

(d) *$rank(G(\alpha)) = k$ for any α in the algebraic closure $\overline{F_q}$.*

(e) *$G(x)$ has right inverse over $F_q[x]$.*

(f) *(predicable rule)$y(x) = z(x)G(x)$, where $y(x) \in F_q[x]^{k\times n}$ and $z(x) \in F_q(x)^{k\times k}$*

$\Longrightarrow z(x) \in F_q[x]^{k\times k}$.

(g) *$G(x)$ can be extended to an $n \times n$ unimodular matrix by adding more rows.*

Proof. $(a) \Longrightarrow (b)$ In SNF Theorem,

$$
\begin{aligned}
& G(x) \\
= \;& E(x)D(x)F(x) \\
= \;& E(x)\begin{pmatrix} d_1(x) & & & & 0 & \\ & d_2(x) & & & & \\ & & d_3(x) & & & 0 \\ & & & \ddots & & \\ 0 & & & & d_k(x) & \end{pmatrix}_{k\times n} \begin{pmatrix} F_1(x) \\ F_2(x) \end{pmatrix} \\
= \;& E(x)\begin{pmatrix} d_1(x) & & 0 \\ & d_2(x) & \\ & & \ddots & \\ 0 & & & d_k(x) \end{pmatrix}_{k\times k} F_1(x),
\end{aligned}
$$

where $F(x) = \begin{pmatrix} F_1(x) \\ F_2(x) \end{pmatrix}$ and $F_1(x)$, $F_2(x)$ are matrices over $F_q[x]$ of size $k \times n$, $(n-k)\times n$ respectively. Then

$$
F_1(x) = \begin{pmatrix} d_1(x)^{-1} & & & 0 \\ & d_1(x)^{-1} & & \\ & & \ddots & \\ 0 & & & d_k(x)^{-1} \end{pmatrix}_{k\times k} E(x)^{-1}G(x)
$$

is a PGM of CV with internal degree

$$\text{int deg}(G(x)) - \deg\,(d_1(x)d_2(x)\cdots d_k(x)).$$

Since $G(x)$ is basic, $d_1(x) = d_2(x) = \cdots = d_k(x) = 1$.

$(b) \Longrightarrow (c)$ Let $k_i(x)$ be the gcd of i-minors of $G(x)$ and recall from Corollary 8.3.12, $d_i(x) = \dfrac{k_i(x)}{k_{i-1}(x)}$. Since $d_i(x) = 1$ for all i, $k_i(x) = 1$ for all i. In particular $k_k(x) = 1$.

$(c) \Longrightarrow (e)$ Let $m_1(x), m_2(x), \cdots, m_t(x)$ be the k-minors of $G(x)$, where $t = \begin{pmatrix} n \\ k \end{pmatrix}$. By (c) we can pick $a_i(x) \in F_q[x]$ such that

$$\sum_{i=1}^{t} a_i(x) m_i(x) = 1.$$

By using Cramer's Rule to a $k \times k$ invertible submatrix of $G(x)$, for each i, there exists $H_i(x) \in F_q[x]^{n \times k}$ (filled with 0 for those rows outside the k rows in considering) such that

$$G(x)H_i(x) = m_i(x)I_k.$$

Set $H(x) = \sum_{i=1}^{t} a_i(x)H_i(x)$. Then

$$G(x)H(x) = \sum_{i=1}^{t} a_i(x)G(x)H_i(x) = (\sum_{i=1}^{t} a_i(x)m_i(x))I_k = I_k.$$

$(e) \Longrightarrow (f)$ Suppose $G(x)H(x) = I_k$ and $y(x) = z(x)G(x)$. Then

$$z(x) = z(x) \cdot I_k = z(x)G(x)H(x) = y(x)H(x) \in F_q[x]^{k \times k}.$$

$(f) \Longrightarrow (a)$ Suppose $G'(x)$ is another PGM of CV. Then $G'(x) = z(x)G(x)$ for some $z(x) \in F_q(x)^{k \times k}$. Then $z(x) \in F_q[x]^{k \times k}$ by (f). Hence by Cauchy Binet Theorem, int $\deg(G'(x)) \geq$ int $\deg(G(x))$.

$(c) \Longrightarrow (d)$ Pick $\alpha \in \overline{F_q}$. Let $P(x) \in F_q[x]$ be the minimal polynomial of α. Then by assumption (c),

$$P(x) \nmid \det(G(x)[- \mid \beta])$$

for some $\beta \subseteq [n]$ with $|\beta| = k$. Hence

$$\det(G(\alpha)[- \mid \beta]) \neq 0.$$

Then $\operatorname{rank}(G(\alpha)) \geq k$. Thus $\operatorname{rank}(G(\alpha)) = k$.

$(d) \Longrightarrow (c)$ Suppose gcd of k-minors is $P(x) \neq 1$. Then

$$G(x) \xrightarrow{ERCO's} \begin{pmatrix} d_1(x) & & 0 & \\ & d_2(x) & & \\ & & \ddots & 0 \\ 0 & & d_k(x) & \end{pmatrix}$$

where $d_k(x) \neq 1$. Pick $\alpha \in \overline{F_q}$ such that $d_k(\alpha) = 0$. Then

$\operatorname{rank}(G(\alpha))=\operatorname{rank}\begin{pmatrix} d_1(\alpha) & & 0 & \\ & d_2(\alpha) & & \\ & & \ddots & 0 \\ 0 & & d_k(\alpha) & \end{pmatrix} \leq k-1$. We get a contradiction.

$(b) \Longrightarrow (g)$

$$\begin{aligned} G(x) &= E(x)D(x)F(x) \\ &= E(x)(I_k\ 0)\begin{pmatrix} F_1(x) \\ F_2(x) \end{pmatrix} \\ &= E(x)F_1(x), \end{aligned}$$

where

$$F(x) = \begin{pmatrix} F_1(x) \\ F_2(x) \end{pmatrix}$$

and $F_1(x)$,$F_2(x)$ are matrices over $F_q[x]$ of size $k \times n$,$(n-k) \times n$ respectively.

Set $G'(x) = \begin{pmatrix} G(x) \\ F_2(x) \end{pmatrix}$. Observe

$$\begin{aligned} G'(x) &= \begin{pmatrix} E(x)F_1(x) \\ F_2(x) \end{pmatrix} \\ &= \begin{pmatrix} E(x) & 0 \\ 0 & I_{n-k} \end{pmatrix} F(x) \end{aligned}$$

is unimodular.

$(g) \Longrightarrow (b)$ Suppose $G'(x) = \begin{pmatrix} G(x) \\ * \end{pmatrix}$ is unimodular. Then $G(x) = I_k(I_k\ 0)G'(x)$. Hence invariant factors of $G(x)$ are all $1'$s.

$\square$

We will introduce another PGM of a CV code with good property.

Definition 8.3.23.

(a) The *degree* of a row is the maximal degree among all entries.

(b) The *external degree* $deg(G(x))$ of $G(x) \in F_q[x]^{k\times n}$ is the sum of degrees of the rows of $G(x)$.

(c) $G(x)$ is *reduced* if $\deg(E(x)G(x)) \geq \deg(G(x))$ for any unimodular $k \times k$ matrix $E(x)$.

Note 8.3.24. $G(x)$ is reduced if the external degree of $G(x)$ can not be reduced by elementary rows operations (ERO's).

Example 8.3.25. Suppose $G(x) = (1 + x^2\ \ 1 + x + x^2)_{1\times 2}$. Observe the internal degree and external degree are equal to 2.

Example 8.3.26. Suppose $G(x) = \begin{pmatrix} 1 & 0 & x+1 \\ 0 & 1 & x \end{pmatrix}_{2\times 3}$. Observe the internal degree is equal to 1 and the external degree is equal to 2. Note $G(x)$ is not reduced, since

$$G(x) = \begin{pmatrix} 1 & 0 & x+1 \\ 0 & 1 & x \end{pmatrix}_{2\times 3} \quad \xrightarrow{ERO's} \quad \begin{pmatrix} 1 & -1 & 1 \\ 0 & 1 & x \end{pmatrix}_{2\times 3},$$

and $deg(\begin{pmatrix} 1 & -1 & 1 \\ 0 & 1 & x \end{pmatrix}_{2\times 3}) = 1 < 2$.

Definition 8.3.27. Let $G(x) \in F_q[x]^{k\times n}$ be a PGM of CV. Let $e_1, e_2, \cdots, e_k$ be the degrees of rows $1, 2, \cdots, k$ respectively in $G(x)$. By interchanging rows of $G(x)$, we assume $e_1 \le e_2 \le \cdots \le e_k$. The *leading coefficients matrix* $\overline{G} \in F_q^{k\times n}$ is a matrix with ij-entry

$$\overline{G}_{ij} := \text{coefficients of } x^{e_i} \text{ in } G_{ij}(x),$$

where $G_{ij}(x)$ is the $ij-$entry of $G(x)$.

Example 8.3.28.

$$G(x) = \begin{pmatrix} 1+x & 2 & 1+x^2 \\ x & 2+x^3 & x^2+x^3 \end{pmatrix}_{2\times 3}$$

$$\Longrightarrow \quad e_1 = 2 \text{ and } e_2 = 3,\ \overline{G} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}_{2\times 3}.$$

Note 8.3.29.

(a) The coefficient of $x^{e_1+e_2+\cdots+e_k}$ of $\det(G(x)[- \mid \beta])$ is $\det(\overline{G}[- \mid \beta])$.

(b) Internal degree of $G(x) \le$ External degree of $G(x)$.

Theorem 8.3.30. *Let $G(x)$ be a $k \times n$ PGM of $CV \subseteq F_q(x)^n$. Then the following are equivalent.*

(a) *$G(x)$ is reduced.*

(b) *rank*($\overline{G}$) $= k$.

(c) *ext deg*($G(x)$) =*int deg*($G(x)$).

(d) *For every nonzero* $z(x) \in F_q[x]^k$, *deg*($z(x)G(x)$) =*max* e_j+*deg*($z_j(x)$) *where the maximum is taking for all* $1 \leq j \leq k$ *such that* $z_j(x) \neq 0$, *the* j*-th entry of* $z(x)$.

Proof. $(a) \Longrightarrow (b)$ Suppose rank($\overline{G}$) $< k$. Then there exists a nonzero vector $(\alpha_1, \alpha_2, \cdots, \alpha_k) \in F_q^k$ such that $(\alpha_1, \alpha_2, \cdots, \alpha_k)\overline{G} = 0$. Suppose t is the largest integer such that $\alpha_t \neq 0$, and suppose $G(x) = \begin{pmatrix} G_1(x) \\ G_2(x) \\ \vdots \\ G_k(x) \end{pmatrix}_{k \times n}$, where $\deg(G_i(x)) = e_i$ and $e_1 \leq e_2 \leq \cdots \leq e_k$. Set

$$G'_t(x) := \alpha_1 G_1(x) x^{e_t - e_1} + \alpha_2 G_2(x) x^{e_t - e_2} + \cdots + \alpha_t G_t(x) \in F_q[x]^n.$$

Note that $\deg(G'_t(x)) < \deg(G_t(x))$. Hence

$$\text{ext deg} \begin{pmatrix} G_1(x) \\ \vdots \\ G_{t-1}(x) \\ G'_t(x) \\ G_{t+1}(x) \\ \vdots \\ G_k(x) \end{pmatrix} < \text{ext deg}(G(x)),$$

a contradiction to $G(x)$ being reduced.

$(b) \Longrightarrow (c)$ Choose $\alpha \subseteq [n]$ with $|\alpha| = k$ such that

$$\det(\overline{G}[- \mid \alpha]) \neq 0,$$

the coefficient of $x^{e_1+e_2+\cdots+e_k}$ in $\det(G(x)[- \mid \alpha])$. Hence

$$\text{int deg}(G(x)) \geq \text{ext deg}(G(x)).$$

Thus, int deg$(G(x))$ =ext deg$(G(x))$.

$(c) \Longrightarrow (a)$ Let $E(x)$ be a $k \times k$ unimodular matrix.

$$\begin{aligned} \text{ext deg}(E(x)G(x)) &\geq \text{int deg}(E(x)G(x)) \\ &= \text{int deg}(G(x)) \\ &= \text{ext deg}(G(x)). \end{aligned}$$

$(b) \Longleftrightarrow (d)$

$$\begin{aligned} \deg(z(x)G(x)) &= \deg(z_1(x)G_1(x) + z_2(x)G_2(x) + \cdots + z_k(x)G_k(x)) \\ &\leq \max \deg(z_j(x)G_j(x)) \qquad (8.3.1) \\ &= \deg(z_t(x)G_t(x)) \text{ for some } t \in [k]. \end{aligned}$$

Set d :=$deg(z_t(x)G_t(x))$ and α_i is the coefficient of x^{d-e_i} in $z_i(x)$. Note that $\alpha_t \neq 0$ is the leading coefficient of $z_t(x)$, and $(\alpha_1,\alpha_2,\cdots,\alpha_k)\overline{G}$ is the coefficient row of x^d in $z(x)G(x)$. Hence

$$\begin{aligned} & (b) \text{ holds} \\ \Longleftrightarrow\ & (\alpha_1, \alpha_2, \cdots, \alpha_k)\overline{G} \neq 0 \text{ for any } (\alpha_1, \alpha_2, \cdots, \alpha_k) \neq 0 \\ \Longleftrightarrow\ & \deg(z(x)G(x)) = d \\ \Longleftrightarrow\ & \text{Equality holds in (8.3.1).} \end{aligned}$$

□

Definition 8.3.31. A PGM $G(x)$ of CV is minimal if it has minimal external degree among all PGM of CV.

We now introduce the third good PGM.

Theorem 8.3.32. *A PGM $G(x)$ is minimal in CV if and only if $G(x)$ is reduced and basic.*

Proof. ($\Longleftarrow$) Let $G_0(x)$ be a PGM of CV. Then

$$\begin{aligned}
\text{ext deg}(G_0(x)) &\geq \text{int deg}(G_0(x)) \\
&\geq \text{int deg}(G(x)) \quad (\text{since } G(x) \text{ is basic}) \\
&= \text{ext deg}(G(x)). \quad (\text{by Theorem 8.3.30}(c))
\end{aligned}$$

($\Longrightarrow$) $G(x)$ is clearly reduced. Suppose a basic PGM in CV has internal degree m_0. Choose a basic PGM $G_0(x)$ with the least external degree among all PGM with internal degree m_0.

Claim: $G_0(x)$ is reduced in CV.

Let $E(x)$ be a $k \times k$ unimodular matrix. Since

$$\text{int deg}(E(x)G_0(x)) = \text{int deg}(G_0(x)) = m_0,$$

we have

$$\text{ext deg}(E(x)G_0(x)) \geq \text{ext deg}(G_0(x)).$$

This shows $G_0(x)$ is reduced.

$$\begin{aligned}
m_0 &= \text{int deg}(G_0(x)) \\
&\leq \text{int deg}(G(x)) \\
&\leq \text{ext deg}(G(x)) \\
&\leq \text{ext deg}(G_0(x)) \quad (\text{since } G(x) \text{ is minimal}) \\
&= \text{int deg}(G_0(x)) \quad (\text{since } G_0(x) \text{ is reduced}) \\
&= m_0.
\end{aligned}$$

Then $\text{int deg}(G(x)) = m_0$. So $G(x)$ is basic. $\square$

Example 8.3.33. Suppose $G(x)=\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1+x & x & 1 \end{pmatrix}_{2\times 4}$. Then with CV= row space of $G(x)$ over $F_2(x)$, we have $e_1 = 0$ and $e_2 = 1$, ext deg$(G(x))$=e_1+e_2=1,and det$(G(x)[-|\alpha])$=$1+x$, x, 1, -1, $-x$, $1-x$ for any α with $|\alpha| = 2$. Hence int deg$((G(x)) = 1$ is the *gcd* of 2-minors of $G(x)$. Hence $G(x)$ is basic by Theorem 8.3.22, and is reduced by Theorem 8.3.30. Then $G(x)$ is minimal by Theorem 8.3.32.

Definition 8.3.34. A *degree* of a CV is the smallest possible internal degree of its PGM's.

Corollary 8.3.35. *A degree of CV is the smallest external degree of its PGM.* □

8.4 Forney Sequence and Free Distance

Theorem 8.4.1. *The sequence of row degrees in increasing order are the same for all minimal PGM's of CV.*

Proof. Let $G(x)$,$G'(x)$ be minimal PGM's with degree sequence $\{e_i\}$,$\{f_i\}$ respectively for i =1,2,$\cdots$,k in increasing order.

Claim: $e_i \leq f_i$ for all $i = 1, 2, \cdots, k$.

To the contrary, let t be the smallest integer such that f_t<e_t. Note that

$$G'(x) = z(x)G(x)$$

for some $z(x)$∈$F_q(x)^{k\times k}$. In fact, $z(x)$∈$F_q[x]^{k\times k}$ by Theorem 8.3.22 (f) since $G(x)$ is basic and $G'(x) \in F_q[x]^{k\times n}$. Suppose $z(x)$=$(z_{ij}(x))_{k\times k}$. Since $G(x)$ is reduced,

$$f_j = \max\ e_i + \deg(z_{ji}(x))$$

for $1 \leq j \leq k$ where the maximum is taking over all i with $z_{ji}(x) \neq 0$ by Theorem 8.3.30 (d). Then

$$z_{ij}(x) = 0$$

if $i \geq t$ and $j \leq t$ (if $z_{ji}(x) \neq 0$, then $f_j \geq e_i \geq e_t > f_t$ is a contradiction). Then the first t rows of $G'(x)$ are spanned by the first $t-1$ rows. This is a contradiction to $G'(x)$ being a PGM. Similarly, $f_i \leq e_i$ for all i. Then $f_i = e_i$ for all i. □

Definition 8.4.2. The sequence of row degrees of a minimal PGM's of CV in increasing order is called the *Forney sequence* of CV and e_k is called the *memory* of CV.

Definition 8.4.3. Fix $L \in \mathbb{N} \cup \{0\}$.

$$(CV)_L := \{f(x) \in CV \cap F_q[x]^n \mid \deg(f(x)) \leq L\}.$$

Note that $(CV)_L$ is a linear code over F_q with codewords of length $(L+1)n$.

Definition 8.4.4. Let δ_L be the dimension of $(CV)_L$.

Theorem 8.4.5. *Let CV be a convolutional code with Forney sequence $e_1 \leq e_2 \leq \cdots \leq e_k$. Then*

$(a)\delta_L = \sum_{i=1}^{k} \max\{L+1-e_i, 0\}$.

$(b)\sum_{L=0}^{\infty} \delta_L x^L = \dfrac{x^{e_1}+x^{e_2}+\cdots+x^{e^k}}{(1-x)^2}$.

Proof.

(a) Observe by Theorem 8.3.30 (d),

$$\begin{aligned}(CV)_L &= (CV)_L \cap F_q[x]^n \\ &= \{z(x)G(x) \in F_q[x]^n \mid z(x) \in F_q[x]^k \text{ with } \deg(z(x)G(x)) \leq L\} \\ &= \{z(x)G(x) \in F_q[x]^n \mid z(x) \in F_q[x]^k \text{ with } \max_{1\leq i\leq k} e_i + \deg(z_i(x)) \leq L\}\end{aligned}$$

where $G(x)$ is a minimal PGM with Forney sequence $e_1, e_2, \cdots, e_k$. Hence

$$\dim((CV)_L) = \sum_{i=1}^{k} \max\{L+1-e_i, 0\}.$$

$$(b) \quad \frac{x^{e_1}+x^{e_2}+\cdots+x^{e^k}}{(1-x)^2}$$
$$= (x^{e_1}+x^{e_2}+\cdots+x^{e_k})(1+x+x^2+\cdots)(1+x+x^2+\cdots)$$
$$= \sum_{L=0}^{\infty}(\sum_{i=1}^{k}\max\{L+1-e_i,0\})x^L$$
$$= \sum_{L=0}^{\infty}\delta_L x^L.$$

□

Definition 8.4.6. For $f(x) \in CV \cap F_q[x]^n$, $wt(f(x))$ is the sum of the number of nonzero coefficients in each position.

Example 8.4.7. $wt(2+x, x^4+x^5+x^6) = 2+3 = 5$.

We now give the free distance of a CV code.

Definition 8.4.8. $d_{\text{free}}(CV) := \min wt(f)$ for all $f(x) \in CV \cap F_q[x]^n$.

Lemma 8.4.9.

$$d_{\text{free}}(CV) \leq \min_{L\geq 0} \max_{C} \{d(C) \mid C \text{ is a } [(L+1)n, \delta_L] - \text{linear code over } F_q.\}$$

Proof. Observe $d_{\text{free}}(CV) = \min d((CV)_L)$, taking for all $L \geq 0$, and $(CV)_L$ is a $[(L+1)n, \delta_L]-$linear code. Hence, we have proved the lemma. □

Example 8.4.10. Suppose $G(x) = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1+x & x & 1 \end{pmatrix}_{2\times 4}$ and CV is the row space of $G(x)$ over $F_2(x)$. Note that $G(x)$ is minimal. Hence $e_1 = 0, e_2 = 1$ and

$$\begin{aligned} \sum_{L=0}^{\infty}\delta_L x^L &= (1+x)(1+x+x^2+\cdots)(1+x+x^2+\cdots) \\ &= \sum_{L=0}^{\infty}((L+1)+L)x^L \\ &= \sum_{L=0}^{\infty}(2L+1)x^L. \end{aligned}$$

Thus $\delta_L = 2L+1$. Since $\delta_0 = 1$, $(CV)_0 = \{(0,0,0,0),(1,1,1,1)\}$ is a $[4,1]-$code over F_2 with $d((CV)_0) = 4$. Thus, $d_{\text{free}}(CV) \leq 4$ by Lemma 8.4.9

8.5 Wyner-Ash Convolutional Code

We consider a special CV in this section.

Definition 8.5.1.

$$\begin{aligned} G(x) &= \begin{pmatrix} 1 & & & 0 & 1+x \\ & 1 & & & 1+x^2 \\ & & 1 & & 1+x+x^2 \\ & & & \ddots & \vdots \\ 0 & & & 1 & 1+x+x^2+\cdots+x^m \end{pmatrix}_{(2^m-1)\times 2^m} \qquad (8.5.1) \\ &\in (F_2[x])^{(2^m-1)\times 2^m} \end{aligned}$$

where the last column contains the polynomials of degrees at most m and at least 1 with the constant term 1. Let $WACV_m$ denote the row space of $G(x)$ over $F_2(x)$. Then $WACV_m$ is called the mth *Wyner-Ash convolutional code.*

Lemma 8.5.2. *$G(x)$ in (8.5.1) is basic.*

Proof. This is clear from Theorem 8.3.22 since the determinant of the first $2^m - 1$ columns is a $(2^m - 1)$-minors with value 1. □

Lemma 8.5.3. $\deg(WACV_m) = m$.

Proof. This is because of int deg($G(x)$)=m and $G(x)$ is basic. □

It is clear that $G(x)$ is not minimal. The following example gives a minimal PGM of $WACV_2$

Example 8.5.4. For $m = 2$. Suppose

$$G(x) = \begin{pmatrix} 1 & 0 & 0 & 1+x \\ 0 & 1 & 0 & 1+x^2 \\ 0 & 0 & 1 & 1+x+x^2 \end{pmatrix}_{3\times 4}$$

$$\xrightarrow{ERO's} \begin{pmatrix} 1 & 0 & 0 & 1+x \\ -x & 1 & 0 & 1+x \\ -x & 0 & 1 & 1 \end{pmatrix}_{3\times 4}$$

$$\xrightarrow{ERO's} \begin{pmatrix} 1 & 0 & 0 & 1+x \\ 0 & 1 & 1 & x \\ -x & 0 & 1 & 1 \end{pmatrix}_{3\times 4}$$

$$\xrightarrow{ERO's} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & x \\ x & 0 & 1 & 1 \end{pmatrix}_{3\times 4}.$$

Since

$$\text{ext deg}(\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & x \\ x & 0 & 1 & 1 \end{pmatrix}) = 0+1+1 = 2 = \text{int deg}(G(x)) = \text{int deg}(\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & x \\ x & 0 & 1 & 1 \end{pmatrix}),$$

$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & x \\ x & 0 & 1 & 1 \end{pmatrix}$ is reduced by Theorem 8.3.30. $\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & x \\ x & 0 & 1 & 1 \end{pmatrix}$ is basic by Lemma 8.5.2. Then $\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & x \\ x & 0 & 1 & 1 \end{pmatrix}$ is minimal by Theorem 8.3.32.

We determine the free distance of $WACV_m$.

Lemma 8.5.5. $d_{\text{free}}(WACV_m) = 3$.

Proof. $d_{\text{free}}(WACV_m) \leq 3$ is clear from the first row of $G(x)$ in (8.5.1). Suppose $d_{\text{free}}(WACV_m) \leq 2$. Say that $z(x)G(x)$ has weight ≤ 2, where $z(x) \in (F_2(x))^{2^m-1}$. Then $z(x) \in (F_2[x])^{2^m-1}$ by Theorem 8.3.22 (f) and since $G(x)$ is basic.

Case 1: If $z(x)$ has only one nonzero entry. Then $z(x)G(x)$ is a polynomial multiple of a row of $G(x)$. Hence $wt(z(x)G(x)) \geq 3$, a contradiction.

Case 2: If $z(x)$ has at least 3 nonzero entries. This is similar to Case 1.

Case 3: If $z(x)$ has exactly 2 nonzero entries $z_i(x), z_j(x)$ where $i < j$. Then

$$z(x)G(x) = \begin{pmatrix} 0 \\ z_i(x) \\ 0 \\ z_j(x) \\ 0 \\ z_i(x)g_{i2^m}(x) + z_j(x)g_{j2^m}(x) \end{pmatrix},$$

Note that $z_i(x)g_{i2^m}(x) + z_j(x)g_{j2^m}(x) = 0$. Since $z(x)G(x)$ has weight at most 2. Note that $z_i(x) = x^a$ and $z_j(x) = x^b$ for some nonnegative integers a, b. Hence

$$g_{i2^m}(x)x^a + g_{j2^m}(x)x^b = 0.$$

Evaluating the lowest degree term, we find $x^a + x^b = 0$. Hence $a = b$ and $x^a(g_{i2^m}(x) + g_{j2^m}(x)) = 0$. Thus $g_{i2^m}(x) = g_{j2^m}(x)$, a contradiction.

□

Lemma 8.5.6. *Every $[2^m, 2^m - m]-$linear code over F_2 has minimal distance ≤ 2.*

Proof. Let C be a $[2^m, 2^m - m]-$linear code over F_2. Let H be a $m \times 2^m$ matrix over F_2 with the rows chosen from a basis of $C^{\perp}$. Then

$$C = \{(a_1, a_2, \cdots, a_{2^m}) \mid H \cdot (a_1, a_2, \cdots, a_{2^m})^t = 0\}.$$

Observe

$$\begin{aligned} d(C) &= \text{ the minimal number of linear dependent columns in } H. \\ &\leq 2, \end{aligned}$$

since either there are 2 same columns or the zero vector is a column of H. □

Theorem 8.5.7. *The Forney sequence of $WACV_m$ is $0, 0, \cdots, 0, 1, 1, \cdots, 1,$ where the number of $0's$ is $2^m - 1 - m$ and the number of $1's$ is m.*

Proof. Note that $e_1 + e_2 + \cdots + e_{2^m-1} =deg(WACV_m) = m$. We have done if we know all e_i at most 1. Suppose some $e_i \geq 2$. Then at least $2^m - m$ e_i are 0. Recall that $\delta_L = \sum_{i=1}^{2^m-1} \max\{L + 1 - e_i, 0\}$. Hence

$$\delta_0 = \sum_{i=1}^{2^m-1} \max\{1 - e_i, 0\} \geq 2^m - m.$$

By Lemma 8.5.6 every $[2^m, \delta_0]-$ linear code over F_2 has minimum distance ≤ 2. Now by Lemma 8.4.9,

$$\begin{aligned} 3 = d_{\text{free}}(WACV_m) &\leq d(WACV_m)_0 \\ &\leq 2, \end{aligned}$$

where C runs from all $[2^m, \delta_0]-$ linear code, a contradiction. □

Bibliography

[1] Richard E. Blahut, *Algebraic Codes for Data Transmission*, Cambridge University Press, Cambridge, 2003.

[2] R. A. Brualdi, *Introductory Combinatorics*, 4^{th} Ed., Pearson Prentics Hall, New Jersey, 2004.

[3] D. Du and F. K. Hwang, *Combinatorial Group Testing and Its Applications*, 2^{nd} Ed., World Scientific, Singapore, 2000.

[4] A. G. D'yachkov, F. K. Hwang, A. J. Macula, P. A. Vilenkin, C. Weng, A Construction of Pooling Designs with Some Happy Surprises, *Journal of Computational Biology, 12(8), 1127-1134, 2005.*

[5] P. Erdös, P. Frankl and D. Füredi, Families of finite sets in which no set is covered by the union of r others. *Israel J. Math.* 51:79–89, 1985.

[6] T. Huang and C. Weng, A note on decoding of superimposed codes, *Journal of Combinatorial Optimization*, 7, 381-384, 2003.

[7] T. Huang and C. Weng, Pooling spaces and non-adaptive designs. *Discrete Mathematics* 282:163–169, 2004.

[8] H. Huang, Y. Huang and C. Weng, More on Pooling Spaces, preprint.

[9] W. H. Kautz and R. C. Singleton. Nonadaptive binary superimposed codes. *IEEE Trans. Inform. Theory*, 10:363–377, 1964.

[10] J. H. van Lint and R. M. Wilson, *A Course in Combinatorics.* Cambridge, Victoria, 1992.

[11] A, J. Macula, A simple construction of d-disjunct matrices with certain constant weights. *Discrete Math.* 162:311–312, 1996.

[12] A. J. Macula, Error-correcting nonadaptive group testing with d^e-disjunct matrices. *Discrete Appl. Math.* 80:217-222, 1997.

[13] H. Ngo and D. Du, New Constructions of Non-Adaptive and Error-Tolerance Pooling Designs, *Discrete Math.*, 243:161–170, 2002.

[14] Vera Pless, *Introduction to the Theory of Error-Correcting Codes* John Wiley & Sons, Inc, New York, 1998.