April 2007

Two Problems in Extremal Set Theory

Joshua Brown Kramer
University of Nebraska - Lincoln, s-jbrown18@math.unl.edu

TWO PROBLEMS IN EXTREMAL SET THEORY

by

Joshua Brown Kramer

A DISSERTATION

Presented to the Faculty of

The Graduate College at the University of Nebraska

In Partial Fulfillment of Requirements

For the Degree of Doctor of Philosophy

Major: Mathematics

Under the Supervision of Professor Jamie Radcliffe

Lincoln, Nebraska

April, 2007

TWO PROBLEMS IN EXTREMAL SET THEORY

Joshua Brown Kramer, Ph. D.

University of Nebraska, 2007

Advisor: Jamie Radcliffe

The focus of this dissertation is on two problems in extremal set theory, which is a branch of extremal combinatorics. The general problem in extremal set theory is to start with all collections of subsets of an underlying ground set, apply restrictions, and then ask how large or small some property can be under those restrictions. We give a brief introduction to extremal combinatorics and consider two open questions.

One open question we consider is an extremal problem under "dimension constraints". We give a brief account of the history of this subject and we consider the open problem of determining the maximum number of Hamming weight w vectors in a k-dimensional subspace of $\mathbb{F}_2^n$. We determine this number for particular choices of n, k, and w, and provide a conjecture for the complete solution when w is odd. This problem is related to coding theory (the study of efficient transmission of data over noisy channels).

One tool used to study this problem is a linear map that decreases the weight of nonzero vectors by a constant. We characterize such maps. Using the tools we develop, we give a new elementary proof of the MacWilliams Extension Theorem (which characterizes weight-preserving linear maps).

The other open problem explored in this dissertation is related to a classical object known as a t-intersecting family, a set system where the size of the intersection of any two family members is at least t. The basic problem is to maximize the size of such a family. We give a history of the relevant theorems (with proofs, where appropriate).

A next question is how few pairs with intersection size less than t are possible in a (large) set system. Bollobás and Leader gave a new proof of a well-known partial solution to the $t = 1$ case by extending set systems to what they call fractional set systems. Although that paper claims the result for $t > 1$ in fact their generalization is false. In this dissertation we give give several counterexamples, as well as a fast algorithm to determine the minimizing fractional set systems when $t > 1$.

ACKNOWLEDGEMENTS

I would first like to thank Dr. Jamie Radcliffe for giving me a tremendous amount of advice and encouragment. I simply would not have been able to complete this task without his support.

I would also like to thank my committee members: Dr. Susan Hermiller, Dr. Stephen Scott, and Dr. Judy Walker. They were very helpful, especially in catching errors in this dissertation. Dr. Mark Brittenham was also kind enough to give me comments on a draft.

I would like to thank Mr. Hansen, my sixth grade teacher. He was one of the first people outside of my family to really encourage me. He asked that I dedicate my first book to him. This is the best I can do.

I would like to thank my family for always being supportive and proud of me. I would particularly like to thank my mom for feeding me, my dad for taping *24*, and my sister for being one of the funniest people I know.

Finally, I would like to thank my wife, Carolyn, for loving me and supporting me, and for understanding why some nights had to be long.

Contents

Chapter 1

Our Notation

1.1 General Notation

$$
\begin{aligned}
[n] &= \{1, 2, \dots, n\} \\
[m, n] &= \{m, m+1, m+2, \dots, n\} \\
|S| &= \text{the size of } S\text{; i.e. the number of elements in the set } S \\
A^S &= \text{the collection of functions from } S \text{ to } A\text{, where } A \text{ and } S \text{ are sets} \\
2^S &= \text{the power set of } S\text{; i.e. } 2^S = \{A : A \subseteq S\} \\
S^C &= \text{the complement of } S\text{. Usually } S \subseteq [n]\text{, and so } S^C = [n] \setminus S \\
\binom{[n]}{r} &= \{A \subseteq [n] : |A| = r\}\text{, the collection of subsets of } [n] \text{ having size } r \\
\binom{n}{r} &= \text{“}n \text{ choose } r\text{”} = \left|\binom{[n]}{r}\right| = \frac{n!}{(n-r)!r!} \\
\binom{[n]}{\geq r} &= \{A \subseteq [n] : |A| \geq r\} = \binom{[n]}{r} \cup \binom{[n]}{r+1} \cup \cdots \cup \binom{[n]}{n} \\
\binom{n}{\geq r} &= \sum_{i=r}^{n} \binom{n}{i} = \left|\binom{[n]}{\geq r}\right| \\
\lceil r \rceil &= \text{the ceiling of } r\text{; i.e. } \lceil r \rceil \text{ is the unique } n \in \mathbb{Z} \text{ such that } 0 \leq n - r < 1 \\
\mathcal{K}_{n,t}^{w} &= \text{the } t\text{-constant fractional set systems of weight } w\text{. Defined on page 27} \\
\mathcal{C}_{n,t}^{w} &= \text{the } t\text{-canonical fractional set systems of weight } w\text{. Defined on page 30}
\end{aligned}
$$

1.2 Vector Space Notation

$$\begin{aligned} \mathbb{F}_q &= \text{the field with } q \text{ elements, where } q \text{ is a prime power} \\ \mathbb{F}_q^\times &= \mathbb{F}_q \setminus \{0\} \end{aligned}$$

Let $S \subseteq \mathbb{F}_q^n$ and $s \in S$.

$$\begin{aligned} \operatorname{span}(S) &= \text{the span of } S\text{; i.e.} \operatorname{span}(S) = \{\sum_{t \in S} c_t t \;:\; c_t \in \mathbb{F}_q\} \\ S < \mathbb{F}_q^n &\Rightarrow S \text{ is a subspace of } \mathbb{F}_q^n\text{. We also say } S \text{ is a } \textit{linear code} \\ \pi_i(s) &= \text{the } i^{th} \text{ coordinate of } s \\ \pi_I(s) &= \text{the projection of } s \text{ onto the coordinates } I \\ \mathrm{wt}(s) &= \text{the } \textit{Hamming weight} \text{ of } s\text{; i.e. } \mathrm{wt}(s) = |\{i \in [n] \;:\; \pi_i(s) \neq 0\}| \\ A_w(S) &= |\{s \in S : \mathrm{wt}(s) = w\}| \\ \vec{0} &= \vec{0}_n = \text{ the vector in } \mathbb{F}_q^n \text{ consisting entirely of zeroes} \\ \vec{1} &= \vec{1}_n = \text{ the vector in } \mathbb{F}_q^n \text{ consisting entirely of ones} \\ \overline{s} &= \vec{1} + s \\ m(n,k,w) &= \max\{A_w(\mathcal{C}) \;:\; \mathcal{C} < \mathbb{F}_2^n, \dim \mathcal{C} = k\} \\ \mathcal{S}_k &= \text{the } k\text{-dimensional binary simplex code. Defined on page 50} \\ \mathcal{S}(k,t,n) &= \text{a sequence of simplex codes. Defined on page 51} \\ \operatorname{supp}(S) &= \text{the support of } S; \\ & \quad \text{i.e. } \operatorname{supp}(S) = \{i \in [n] \;:\; \exists\, t \in S \text{ with } \pi_i(t) \neq 0\} \end{aligned}$$

Chapter 2

Extremal Problems in Combinatorics

2.1 Introduction

The main focus of this thesis is on two problems in extremal combinatorics, specifically extremal set theory. An extremal problem has the following flavor: we put restrictions on a collection of combinatorial objects and then ask how large or small some property (often the size) of the objects can be under those restrictions. In *extremal set theory*, the underlying objects are collections of subsets of some finite ground set. A collection of subsets is variously called a *set system*, a *family of subsets*, or a *hypergraph*. The rest of this chapter provides some examples of extremal problems.

2.2 Examples

2.2.1 Ramsey Theory

We now give an old example of an extremal problem. Say we invite people to a party, and we wish to choose them in such a way that no three are mutual strangers and no three are mutual friends. What is the maximum number of people that can be at such a party? The following fairly easy argument tells us that the answer is 5 and no more.

We re-envision the problem as a graph edge coloring problem. Let K_n be the complete graph on n vertices. We will interpret these vertices as the people invited to the party. We color the edges of K_n either red or blue, red indicating friends, and blue indicating strangers. We now wish to know how large n can be if we would like to avoid a monochromatic triangle. With 5 vertices, we may avoid such a triangle by coloring as indicated in Figure 2.1.

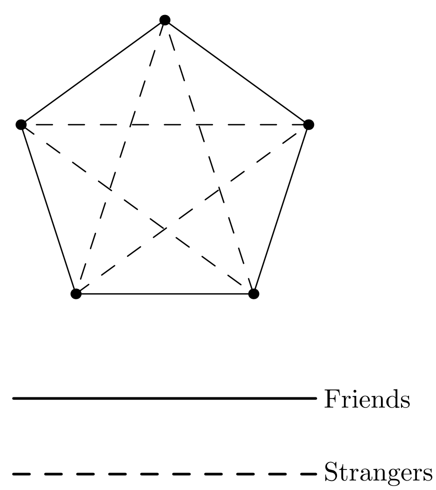

Figure 2.1: A configuration without 3 mutual strangers or 3 mutual friends

We now show that we cannot do this for 6 or more vertices. Color the edges of K_6 red and blue. Pick a vertex $v \in K_6$. There are 5 edges emanating from v. Thus there are either at least 3 red, or at least 3 blue edges from v. Let us assume without loss of generality that they are red. Let the set of endpoints of these red edges be called S. Either there is a red edge between some pair of members $u, w \in S$, or there is not. In the first case v, u, and w are the vertices of a red triangle. In the second case, S is the set of vertices for a blue triangle.

The fact above is a specific case of Ramsey's Theorem [27], one version of which can be stated as follows.

Theorem 2.2.1 (Ramsey's Theorem)**.** *Given positive integers r and b, there exists $R(r, b) > 0$ (called the* Ramsey number for r and b*) such that if $n \geq R(r, b)$, all red and blue edge-colorings of the complete graph on n vertices contain either a copy of K_r, all of whose edges are red, or a copy of K_b, all of whose edges are blue.*

We have shown that $R(3, 3) = 6$. There is a natural proof of Theorem 2.2.1 that is very similar to the specific case given above, so it is not provided here.

Finding $R(r, b)$ is an extremal problem. We start with the collection of complete graphs colored red and blue, and we place the restriction on them that they have no red K_r or blue K_b. We then ask how large the largest of these colored graphs is. The answer is $R(r, b) - 1$. Finding $R(r, b)$ is a very hard problem in general. It is only known exactly in a small number of cases. See [26] for a survey of the known Ramsey numbers.

2.2.2 Sperner Families

We will now discuss another classical problem from extremal combinatorics. Here, the underlying combinatorial objects are collections of subsets of a ground set. For this reason, the problem falls under the category of extremal set theory.

Let $\mathcal{A} \subseteq 2^{[n]}$ be a family of subsets. We say that $\mathcal{A}$ is a *Sperner family* or *antichain* if no two subsets in $\mathcal{A}$ are comparable. That is, for all $A, B \in \mathcal{A}$, if $A \subseteq B$ then $A = B$. The natural extremal problem is to find how large such a family can be. Sperner [28] found the answer in 1928.

Theorem 2.2.2 (Sperner's Theorem)**.** *If $\mathcal{A} \subseteq 2^{[n]}$ is an antichain then $|\mathcal{A}| \leq \binom{n}{\lfloor \frac{n}{2} \rfloor}$.*

One way to prove this result is to use the so-called *LYM inequality* proved independently by Lubell[22], Yamamoto[31], Meshalkin[25], and Bollobás[6].

Theorem 2.2.3 (The LYM Inequality)**.** *Let $\mathcal{A} \subseteq 2^{[n]}$ be an antichain. Then*

$$\sum_{A \in \mathcal{A}} \binom{n}{|A|}^{-1} \leq 1.$$

The LYM inequality can be proved by a beautiful double counting argument, which requires a definition. A *maximal chain* in $2^{[n]}$ is a collection of sets $\{C_0, C_1, C_2, \ldots C_n\}$ with the property that $\emptyset = C_0 \subsetneq C_1 \subsetneq \cdots \subsetneq C_{n-1} \subsetneq C_n = [n]$. Notice that the i^{th} set in a maximal chain contains exactly one more element than the $(i-1)^{st}$. We can then associate the i^{th} set with this new element. A maximal chain can thereby be associated with an ordering of the elements of $[n]$. Thus the number of maximal chains is $n!$. We now proceed to the proof of the LYM inequality.

Proof of the LYM inequality. Let $\mathcal{A} \subseteq 2^{[n]}$ be a Sperner family and define the following collection of pairs.

$$P = \{(A, \mathcal{C}) \,:\, A \in \mathcal{A} \text{ and } \mathcal{C} \text{ is a maximal chain with } A \in \mathcal{C}\}.$$

We count P in two ways. First, given $A \in \mathcal{A}$, we count the number of maximal chains containing A. By the discussion above, this is the same as the number of ways to order $[n]$ so that the first $|A|$ elements of the ordering are a permutation of A and the last $n - |A|$ elements are a permutation of $[n] \setminus A$. The number of maximal chains containing A is therefore $|A|!(n-|A|)!$. Summing over all elements of $\mathcal{A}$, we have

$$|P| = \sum_{A \in \mathcal{A}} |A|!(n-|A|)!.$$

Now we fix a maximal chain $\mathcal{C}$ in $2^{[n]}$. Notice that any two sets from $\mathcal{C}$ are comparable. But by the definition of a Sperner family, if $A, B \in \mathcal{A}$ and $A \neq B$, then A and B are not comparable. Thus at most one element of $\mathcal{A}$ is in $\mathcal{C}$. Since there are $n!$ maximal chains in $2^{[n]}$, we have that $|P| \leq n!$. Hence

$$\begin{aligned}
\sum_{A \in \mathcal{A}} |A|!(n-|A|)! &\leq n! \\
\sum_{A \in \mathcal{A}} \frac{|A|!(n-|A|)!}{n!} &\leq 1 \\
\sum_{A \in \mathcal{A}} \left[\frac{n!}{|A|!(n-|A|)!}\right]^{-1} &\leq 1 \\
\sum_{A \in \mathcal{A}} \binom{n}{|A|}^{-1} &\leq 1.
\end{aligned}$$

□

We now use the LYM inequality to prove Sperner's Theorem.

Proof of Sperner's Theorem. Let $\mathcal{A}$ be a Sperner family. It is easy to show that for all $r \in [n]$, $\binom{n}{r} \leq \binom{n}{\lfloor \frac{n}{2} \rfloor}$. Then by the LYM inequality,

$$
\begin{aligned}
|\mathcal{A}|\binom{n}{\lfloor \frac{n}{2} \rfloor}^{-1} &= \sum_{A\in\mathcal{A}} \binom{n}{\lfloor \frac{n}{2} \rfloor}^{-1} \\
&\leq \sum_{A\in\mathcal{A}} \binom{n}{|A|}^{-1} \\
&\leq 1.
\end{aligned}
$$

Hence $|\mathcal{A}|\binom{n}{\lfloor \frac{n}{2} \rfloor}^{-1} \leq 1$ and thus $|\mathcal{A}| \leq \binom{n}{\lfloor \frac{n}{2} \rfloor}$, as desired. $\square$

Sperner's Theorem and Ramsey's Theorem are two classical examples of problems from extremal combinatorics. They come from extremal set theory and extremal graph theory respectively. There are many more examples of extremal problems (see [7],[11], and [20] for examples). The remainder of this dissertation will consist of work on some open problems in extremal set theory.

Chapter 3

Intersecting Families

3.1 Introduction

We now introduce another classical object from combinatorics. A family of subsets $\mathcal{A} \subseteq 2^{[n]}$ is called *intersecting* if for all $A, B \in \mathcal{A}$, we have $A \cap B \neq \emptyset$. Given an integer $t \geq 1$ we may insist that for all $A, B \in \mathcal{A}$ we have $|A \cap B| \geq t$. In this case we say $\mathcal{A}$ is t*-intersecting*. In particular, an intersecting family is a 1-intersecting family. We might also insist that the families we consider be subsets of $\binom{[n]}{r}$, for some $r \in \mathbb{N}$. In all cases the first natural question is how large such a family can be. The answer to each of these problems is completely known. A survey of the results (with proofs where appropriate) appears in Section 3.2.

Define $M(n,t) \in \mathbb{N}$ to be the size of a largest t-intersecting set on $[n]$. If $\mathcal{A} \subseteq 2^{[n]}$ is a set system with $|\mathcal{A}| > M(n,t)$ then $\mathcal{A}$ has at least one pair $A, B \in \mathcal{A}$ such that $|A \cap B| < t$. We may ask for the set system which minimizes the number of non–t–intersecting pairs. Some results are known for this problem. We summarize them in Section 3.2.4.

In [10], Bollobás and Leader gave a new proof of a partial result of the $t = 1$

case. They use what they call fractional set systems, which they introduced in [9]. Although [10] claims the result for $t > 1$ in fact the generalization is false. In Section 3.3, we give several counterexamples as well as a fast algorithm to determine the minimizing fractional set systems when $t > 1$.

3.2 Survey of Known Results

3.2.1 The Easy Unrestricted Case

The following bound on the size of an intersecting family is well known (see [7] for example).

Theorem 3.2.1. *If $\mathcal{A} \subseteq 2^{[n]}$ is an intersecting family then $|\mathcal{A}| \leq 2^{n-1}$.*

Proof. Let $A \in \mathcal{A}$. We have that $A \cap A^C = \emptyset$. Thus $A^C \notin \mathcal{A}$. $\mathcal{A}$ is missing the complement of each of its members, so it contains at most half of the elements of $2^{[n]}$. Thus $|\mathcal{A}| \leq |2^{[n]}|/2 = 2^n/2 = 2^{n-1}$. □

Furthermore, this bound is tight. There are many examples of intersecting families on $[n]$ with 2^{n-1} elements. Indeed, every maximal intersecting family has size 2^{n-1}. That is, given an intersecting family $\mathcal{A} \subseteq 2^{[n]}$, there is an intersecting family $\mathcal{A}' \subseteq 2^{[n]}$ with $\mathcal{A} \subseteq \mathcal{A}'$, and $|\mathcal{A}'| = 2^{n-1}$. This is also well known (again see [7] for example).

Theorem 3.2.2. *Every maximal intersecting family on $[n]$ has size 2^{n-1}.*

Proof. Suppose to the contrary that there is a maximal intersecting family $\mathcal{A} \subseteq 2^{[n]}$ with $|\mathcal{A}| < 2^{n-1}$. There is $A \in 2^{[n]}$ such that $A \notin \mathcal{A}$ and $A^C \notin \mathcal{A}$. By maximality, there are $B, C \in \mathcal{A}$ such that $A \cap B = \emptyset$, and $A^C \cap C = \emptyset$. Thus $B \subseteq A^C$ and $C \subseteq A$. Hence $B \cap C = \emptyset$. This contradicts $\mathcal{A}$ being an intersecting family. □

The two most important examples of maximal intersecting families appear below. They are, respectively, the family of all sets containing a fixed element, and the family of all "large sets".

$$\mathcal{A} = \left\{A \in 2^{[n]} \,:\, 1 \in A\right\}$$

and

$$\mathcal{B} = \begin{cases} \binom{[n]}{\geq \frac{n+1}{2}}, & n \text{ odd;} \\ \binom{[n]}{\geq \frac{n}{2}+1} \cup \left\{B \in 2^{[n]} \,:\, |B| = \frac{n}{2}, \text{ and } 1 \in B\right\}, & n \text{ even.} \end{cases}$$

It is clear that $\mathcal{A}$ in intersecting. Let $A, B \in \mathcal{B}$. If n is odd, then

$$|A \cap B| = |A| + |B| - |A \cup B| \geq \frac{n+1}{2} + \frac{n+1}{2} - n = 1.$$

If n is even and $|A| = |B| = n/2$ then $1 \in A \cap B$. Otherwise

$$|A \cap B| = |A| + |B| - |A \cup B| \geq \frac{n}{2} + 1 + \frac{n}{2} - n = 1.$$

3.2.2 The Unrestricted t-Intersecting Case

The problem for general t is more difficult. It was solved by Katona [21]. If we let $M(n,t) = \max\left\{|\mathcal{A}| \,:\, \mathcal{A} \subseteq 2^{[n]} \text{ and } \mathcal{A} \text{ is } t\text{-intesecting}\right\}$ then we have the following theorem.

Theorem 3.2.3 (Katona's Intersection Theorem)**.** *For $t \geq 1$,*

$$M(n,t) = \begin{cases} \binom{n}{\geq \frac{n+t}{2}} & \textit{if } n+t \textit{ is even;} \\ 2\binom{n-1}{\geq \frac{n+t-1}{2}} & \textit{if } n+t \textit{ is odd.} \end{cases}$$

Four proofs of this fact appear in a recent paper by Ahlswede and Khachatrian [5]. We will present a very elegant proof from that paper, filling in some of the details omitted there.

Loosely, the idea of the proof is to take a maximum t–intersecting family $\mathcal{A}$ and repeatedly "shift it to the left" in a way that preserves the size of the family and leaves the family t-intersecting. Eventually we will arrive at a family that cannot be shifted further to the left. We call such a family left-compressed. The desired inequality is easy to establish for left-compressed families. We now make these ideas precise. [1]

Let $i, j \in [n]$, where $i < j$. Define $S_{i \leftarrow j} : 2^{[n]} \to 2^{[n]}$ by

$$S_{i \leftarrow j}(A) = \begin{cases} (A \setminus \{j\}) \cup \{i\} & \text{if } j \in A \text{ and } i \notin A; \\ A & \text{otherwise.} \end{cases}$$

We call $S_{i \leftarrow j}$ a *left shift*. Unfortunately, $S_{i \leftarrow j}$ is not injective. Given a family $\mathcal{A} \subseteq 2^{[n]}$, we may modify the left shift in such a way that it is injective when restricted to $\mathcal{A}$. To this end, we define $S_{\mathcal{A}, i \leftarrow j} : \mathcal{A} \to 2^{[n]}$ as follows.

$$S_{\mathcal{A}, i \leftarrow j}(A) = \begin{cases} S_{i \leftarrow j}(A) & \text{if } S_{i \leftarrow j}(A) \notin \mathcal{A}; \\ A & \text{if } S_{i \leftarrow j}(A) \in \mathcal{A}. \end{cases}$$

Lemma 3.2.4. *$S_{\mathcal{A}, i \leftarrow j}$ is injective.*

[1]It should be noted that shifting techniques have found wide applicability to extremal problems (See for example [8], [17], or [30]). In particular, the lemmas in this subsection are very well-known.

Proof. Let $A, B \in \mathcal{A}$ be distinct sets. Suppose for the sake of contradiction that $S_{\mathcal{A},i\leftarrow j}(A) = S_{\mathcal{A},i\leftarrow j}(B)$. This implies that $A \setminus \{i,j\} = B \setminus \{i,j\}$. First we show that exactly one of the equalities $S_{\mathcal{A},i\leftarrow j}(A) = A$ and $S_{\mathcal{A},i\leftarrow j}(B) = B$ holds. They do not both hold, since $A \neq B$. Notice that if $S_{\mathcal{A},i\leftarrow j}(A) \neq A$, then $j \in A$ and $i \notin A$. In those circumstances, $S_{\mathcal{A},i\leftarrow j}(A) = (A \setminus \{j\}) \cup \{i\}$, and so $A = (S_{\mathcal{A},i\leftarrow j}(A) \setminus \{i\}) \cup \{j\}$. Similarly, if $S_{\mathcal{A},i\leftarrow j}(B) \neq B$ then $B = (S_{\mathcal{A},i\leftarrow j}(A) \setminus \{i\}) \cup \{j\}$. Therefore, if $S_{\mathcal{A},i\leftarrow j}(A) \neq A$ and $S_{\mathcal{A},i\leftarrow j}(B) \neq B$ then $A = (S_{\mathcal{A},i\leftarrow j}(A) \setminus \{i\}) \cup \{j\} = (S_{\mathcal{A},i\leftarrow j}(B) \setminus \{i\}) \cup \{j\} = B$, a contradiction. We may now assume without loss of generality that $S_{\mathcal{A},i\leftarrow j}(A) \neq A$ and $S_{\mathcal{A},i\leftarrow j}(B) = B$. But this situation cannot happen, since otherwise $S_{i\leftarrow j}(A) = S_{\mathcal{A},i\leftarrow j}(A) = S_{\mathcal{A},i\leftarrow j}(B) = B \in \mathcal{A}$ and so by definition, $S_{\mathcal{A},i\leftarrow j}(A) = A$. $\square$

We now define

$$S_{i\leftarrow j}(\mathcal{A}) = \{S_{\mathcal{A},i\leftarrow j}(A) \,:\, A \in \mathcal{A}\}$$

Lemma 3.2.5. *If $\mathcal{A} \subseteq [n]$ is t-intersecting then $S_{i\leftarrow j}(\mathcal{A})$ is also t-intersecting.*

Proof. Let $A', B' \in S_{i\leftarrow j}(\mathcal{A})$. We want to show that $|A' \cap B'| \geq t$. We have that $A' = S_{\mathcal{A},i\leftarrow j}(A)$ for some $A \in \mathcal{A}$ and $B' = S_{\mathcal{A},i\leftarrow j}(B)$ for some $B \in \mathcal{A}$. Since $\mathcal{A}$ is t-intersecting, we have that $|A \cap B| \geq t$. If $A = A'$ and $B = B'$ then

$$|A' \cap B'| = |A \cap B| \geq t,$$

as desired. If $A' \neq A$ and $B' \neq B$, then

$$|A' \cap B'| = |A \cap B| - |\{j\}| + |\{i\}| = |A \cap B| \geq t.$$

We may now assume, without loss of generality, that $A' \neq A$ and $B' = B$. One of three possibilities has occurred. Either $j \notin B$ or $i \in B$ or $S_{i\leftarrow j}(B) \in \mathcal{A}$.

Case 1: $j \notin B$**.**

Notice that $i \notin A$. Thus $A \cap B = (A \cap B) \setminus \{i, j\}$. Thus

$$|A' \cap B'| = |A' \cap B| = |((A \setminus \{j\}) \cup \{i\}) \cap B| \geq |(A \cap B) \setminus \{i, j\}| = |A \cap B| \geq t.$$

Case 2: $i \in B$**.**

Notice that $i \notin A$. In particular, $A \setminus \{j\} = A \setminus \{i, j\}$ and $|(A \setminus \{i, j\}) \cap B| \geq |A \cap B| - 1$. Thus we have

$$\begin{aligned}
|A' \cap B'| &= |A' \cap B| \\
&= |((A \setminus \{j\}) \cup \{i\}) \cap B| \\
&= |((A \setminus \{j\}) \cap B) \cup (\{i\} \cap B)| \\
&= |((A \setminus \{i, j\}) \cap B) \cup (\{i\} \cap B)| \\
&= |((A \setminus \{i, j\}) \cap B)| + |\{i\} \cap B| \\
&\geq |A \cap B| - 1 + 1 \\
&= |A \cap B| \\
&\geq t.
\end{aligned}$$

Case 3: $S_{i \leftarrow j}(B) \in \mathcal{A}$**.**

If $S_{i \leftarrow j}(B) = B$ then one of the cases above holds. Otherwise, $S_{i \leftarrow j}(B) = (B \setminus \{j\}) \cup \{i\}$. Thus $j \notin S_{i \leftarrow j}(B)$ and $i \in S_{i \leftarrow j}(B)$. On the other hand, $j \in A$ and $i \notin A$. In particular, $A \cap S_{i \leftarrow j}(B) = (A \cap B) \setminus \{i, j\}$. But $S_{i \leftarrow j}(B) \in \mathcal{A}$, so $|A \cap S_{i \leftarrow j}(B)| \geq t$. Thus

$$|A' \cap B'| = |A' \cap B| \geq |(A \cap B) \setminus \{i, j\}| = |A \cap S_{i \leftarrow j}(B)| \geq t.$$

$\square$

We say that a family $\mathcal{A} \subseteq 2^{[n]}$ is *left-compressed* if for all $i, j \in [n]$, where $i < j$, we have $S_{i\leftarrow j}(\mathcal{A}) = \mathcal{A}$. We are now ready to prove Katona's intersection theorem.

Proof of Theorem 3.2.3. We treat the case where $n+t$ is even (the other case is similar). First let $\mathcal{A} = \binom{[n]}{\geq \frac{n+t}{2}}$. Given A and B in $\mathcal{A}$, we have

$$|A \cap B| = |A| + |B| - |A \cup B| \geq \frac{n+t}{2} + \frac{n+t}{2} - n = t.$$

Thus $\mathcal{A}$ is t-intersecting, and so $M(n,t) \geq |\mathcal{A}| = \binom{n}{\geq \frac{n+t}{2}}$.

We must show that $M(n,t) \leq \binom{n}{\geq \frac{n+t}{2}}$. We prove this statement by induction on n. For $n = 1$, we want to show that the largest t-intersecting family on $\{1\}$ is $\{\{1\}\}$ if $t = 1$ and $\emptyset$ if $t > 1$. These facts are clear.

For $n > 1$, let $\mathcal{A}' \subseteq 2^{[n]}$ be a maximum size t-intersecting family. Notice that $|\mathcal{A}'| = M(n,t)$. By starting with $\mathcal{A}'$ and repeatedly applying left–shifts, we eventually arrive at $\mathcal{A} \subseteq 2^{[n]}$, a left–compressed t-intersecting family of size $M(n,t)$. It only remains to show that $|\mathcal{A}| \leq \binom{n}{\geq \frac{n+t}{2}}$.

We define the following families on the ground set $\{2, \ldots, n\}$.

$$\mathcal{A}_- = \{A \,:\, A \in \mathcal{A} \text{ and } 1 \notin A\}.$$

$$\mathcal{A}_+ = \{A \setminus \{1\} \,:\, A \in \mathcal{A} \text{ and } 1 \in A\}.$$

Notice that $|\mathcal{A}_-| + |\mathcal{A}_+| = |\mathcal{A}|$. We have that $\mathcal{A}_+$ is $(t-1)$-intersecting. It turns out that $\mathcal{A}_-$ is $(t+1)$-intersecting. To see this, consider $A, B \in \mathcal{A}_-$. Notice that $|A \cap B| \geq t \geq 1$. Thus there is some $j \in A \cap B$. Since $\mathcal{A}$ is left–compressed, $S_{\mathcal{A},1\leftarrow j}(A) = A$ and hence $A' = (A \setminus \{j\}) \cup \{1\}$ is in $\mathcal{A}$. But then $|A' \cap B| \geq t$. We have $A \cap B = (A' \cap B) \cup \{j\}$. Thus $|A \cap B| \geq t + 1$.

By induction,

$$\begin{aligned}
M(n,t) &= |\mathcal{A}| \\
&= |\mathcal{A}_-| + |\mathcal{A}_+| \\
&\leq \sum_{i=\frac{(n-1)+(t+1)}{2}}^{n-1} \binom{n-1}{i} + \sum_{i=\frac{(n-1)+(t-1)}{2}}^{n-1} \binom{n-1}{i} \\
&= \sum_{i=\frac{n+t}{2}}^{n-1} \binom{n-1}{i} + \sum_{i=\frac{n+t}{2}-1}^{n-1} \binom{n-1}{i} \\
&= \sum_{i=\frac{n+t}{2}}^{n-1} \binom{n-1}{i} + \sum_{i=\frac{n+t}{2}}^{n} \binom{n-1}{i-1} \\
&= \binom{n-1}{n-1} + \sum_{i=\frac{n+t}{2}}^{n-1} \left[\binom{n-1}{i} + \binom{n-1}{i-1}\right] \\
&= \binom{n}{n} + \sum_{i=\frac{n+t}{2}}^{n-1} \binom{n}{i} \\
&= \sum_{i=\frac{n+t}{2}}^{n} \binom{n}{i} \\
&= \binom{n}{\geq \frac{n+t}{2}}.
\end{aligned}$$

□

3.2.3 The Restricted Case

Let $r \in \mathbb{N}$. We ask for the largest intersecting family $\mathcal{A} \subseteq \binom{[n]}{r}$. If $r > n/2$ this is easy: given two sets, $A, B \in \binom{[n]}{r}$, we have

$$|A \cap B| = |A| + |B| - |A \cup B| \geq r + r - n > n - n = 0.$$

Thus $\binom{[n]}{r}$ is itself intersecting.

For the case $r \leq n/2$, let $x \in [n]$ and define

$$\binom{[n]}{r}_x = \left\{ A \in \binom{[n]}{r} \,:\, x \in A \right\}.$$

Clearly $\binom{[n]}{r}_x$ is intersecting. Its size is $\binom{n-1}{r-1}$. Moreover, the famous Erdős-Ko-Rado Theorem [15] tells us that this is the best possible.

Theorem 3.2.6 (Erdős-Ko-Rado)**.** *If $1 \leq r \leq n/2$ and $\mathcal{A} \subseteq \binom{[n]}{r}$ is an intersecting family then $|\mathcal{A}| \leq \binom{n-1}{r-1}$. Equality is achieved if and only if $\mathcal{A} = \binom{[n]}{r}_x$ for some $x \in [n]$.*

□

In [15], Erdős, Ko, and Rado also determined the limiting behavior for the t-intersecting case.

Theorem 3.2.7 (Erdős-Ko-Rado)**.** *Let $r \in \mathbb{N}$. There exists $N \in \mathbb{N}$ so that for all $n \geq N$, every t-intersecting family $\mathcal{A} \subseteq \binom{[n]}{r}$ has $|\mathcal{A}| \leq \binom{n-t}{r-t}$. Furthermore, N can be chosen large enough that if $n \geq N$ and $\mathcal{A}$ is t-intersecting with $|\mathcal{A}| = \binom{n-t}{r-t}$, then $\mathcal{A}$ consists of all sets in $\binom{[n]}{r}$ containing some particular set of size t.*

□

The complete solution to the restricted t-intersecting problem for all n and r was found by Ahlswede and Khachatrian [4]. To state it requires some definitions. Given $n, r, t \in \mathbb{N}$, we define $I(n, r, t)$ to be the set of all t-intersecting families consisting of subsets of $[n]$ having size r. That is

$$I(n, r, t) = \left\{ \mathcal{A} \subseteq \binom{[n]}{r} \,:\, |A \cap B| \geq t \text{ for all } A, B \in \mathcal{A} \right\}.$$

We are interested in finding

$$M(n,r,t) = \max_{\mathcal{A} \in I(n,r,t)} |\mathcal{A}| .$$

Given $n, r, t, i \in \mathbb{N}$, with $0 \leq i \leq \dfrac{n-t}{2}$, set

$$\mathcal{F}_i = \left\{ F \in \binom{[n]}{r} \; : \; |F \cap [t+2i]| \geq t+i \right\}.$$

We claim that $\mathcal{F}_i$ is t-intersecting for all $0 \leq i \leq \dfrac{n-t}{2}$. Given $A, B \in \mathcal{F}_i$, we have

$$\begin{aligned}
|A \cap B| &\geq |(A \cap [t+2i]) \cap (B \cap [t+2i])| \\
&= |(A \cap [t+2i])| + |(B \cap [t+2i])| - |(A \cap [t+2i]) \cup (B \cap [t+2i])| \\
&\geq (t+i) + (t+i) - (t+2i) \\
&= t.
\end{aligned}$$

The theorem of Ahlswede and Khachatrian will tell us that given $n, r, t \in \mathbb{N}$, there is some $0 \leq i \leq \dfrac{n-t}{2}$ for which $M(n,r,t) = |\mathcal{F}_i|$. More specifically, we have

Theorem 3.2.8 (Ahlswede and Khachatrian)**.** *For $1 \leq t \leq r \leq n$ we have the following cases*

(i) $(r-t+1)(2+(t-1)/(i+1)) < n < (r-t+1)(2+(t-1)/i)$ *for some* $i \in \mathbb{N}$. *In this case we have*

$$M(n,r,t) = |\mathcal{F}_i| ,$$

and up to permutation, $\mathcal{F}_i$ is the unique optimum.

(ii) $(r-t+1)(2+(t-1)/(i+1)) = n$ *for some* $i \in \mathbb{N}$. *In this case we have*

$$M(n,r,t) = |\mathcal{F}_i| = |\mathcal{F}_{i+1}|\,,$$

and up to permutation, $\mathcal{F}_i$ *and* $\mathcal{F}_{i+1}$ *are the only optimal families.*

□

3.2.4 Further Research

The maximum sizes of intersecting families under various restrictions are now well known. A natural next question is: given (large) $s \in \mathbb{N}$, how close to intersecting can a family of size s be? More precisely: given $\mathcal{A} \subseteq 2^{[n]}$, define $D_t(\mathcal{A})$ to be the number of pairs of sets from $\mathcal{A}$ that have intersection size less than t. That is

$$D_t(\mathcal{A}) = |\{(A,B) \in \mathcal{A} \times \mathcal{A} \,:\, |A \cap B| < t\}|\,.$$

Given $s \in \mathbb{N}$, we wish to minimize $D_t(\mathcal{A})$ over all systems with $|\mathcal{A}| = s$. Define $D_{n,t}(s)$ to be this minimum. That is, we wish to find

$$D_{n,t}(s) = \min\left\{D_t(\mathcal{A}) \,:\, \mathcal{A} \subseteq 2^{[n]},\ \mathcal{A} \text{ is } t\text{-intersecting, and } |\mathcal{A}| = s\right\}.$$

Theorem 3.2.3 (Katona's Intersection Theorem) established the values of s for which $D_{n,t}(s) = 0$.

Frankl [16] and Ahlswede [1] independently determined the answer for particular values of s when $t = 1$. Essentially, the optimal family has as many large sets as possible. More precisely, we have the following theorem.

Theorem 3.2.9 (Frankl and Ahlswede)**.** *Let* $n \in \mathbb{N}$. *Given* $\mathcal{B} \subseteq 2^{[n]}$, *let* r *be such* *that* $\binom{n}{\geq r+1} \leq |\mathcal{B}| \leq \binom{n}{\geq r}$. *Then there is* $\mathcal{A} \subseteq 2^{[n]}$ *with* $|\mathcal{A}| = |\mathcal{B}|$, $\binom{[n]}{\geq r+1} \subseteq \mathcal{A} \subseteq \binom{[n]}{\geq r}$ *and* $D_1(\mathcal{A}) \leq D_1(\mathcal{B})$.

An immediate corollary of this theorem is that if $s = \binom{n}{\geq r}$, then $D_1(s) = D_1\left(\binom{[n]}{\geq r}\right)$. Bollobás and Leader [10] provided another proof of this corollary (but not of the theorem) by generalizing to what they call "fractional set systems" (we will give the precise definitions of fractional set system and other relevant terms in Section 3.3.1). They extend the definition of D_1 for fractional set systems, and they extend cardinality to what they call weight. Given a fixed number, w, they then determine the fractional set system of weight w that minimizes D_1. When $w = \binom{n}{\geq r}$, the minimizing fractional set system is the classical set system $\binom{[n]}{\geq r}$.

Though [10] claims the same result for $t > 1$, in fact their generalization is false. In Section 3.3.3 we give several counterexamples. Thus the question of determining the D_t minimizing fractional set systems of a given weight is still open. We give examples that indicate that the situation is relatively complicated. In Section 3.3.4 we give a polynomial time algorithm (in n) for determining a minimizing fractional set system. More precisely, we give a polynomial time algorithm for "graphing" $D_{n,t}(s)$.

3.3 Fractional Set Systems

3.3.1 The Theorem of Bollobás and Leader

Given $n \in \mathbb{N}$, we define a *fractional set system on* $[n]$ to be a map

$$f : 2^{[n]} \to [0, 1].$$

The $\{0,1\}$-valued fractional systems correspond to classical set systems. In particular, if f is a $\{0,1\}$-valued fractional system on $[n]$ then f corresponds to the set

$$\left\{A \in 2^{[n]} \,:\, f(A) = 1\right\}.$$

We denote the set of all fractional set systems on $2^{[n]}$ by $\mathcal{F}_n$. If $f \in \mathcal{F}_n$, we define its *weight*, $W(f)$, to be

$$W(f) = \sum_{A \in 2^{[n]}} f(A).$$

Given $t \in \mathbb{N}$, we define

$$D_t(f) = \sum_{\substack{(A,B) \in 2^{[n]} \times 2^{[n]} \\ |A \cap B| < t}} f(A) \oplus f(B),$$

where for all $r, s \in \mathbb{R}$,

$$r \oplus s = \max\{0, r + s - 1\}.$$

(It is useful to think of $r \oplus s$ as the liquid that spills out of a test tube of volume 1 if liquids of volume r and s are added to it.) Notice that the D_t we've defined for fractional set systems corresponds to the D_t defined for actual set systems. Thus, given a fixed weight $w \geq 0$, we are looking for

$$D_{n,t}(w) = \inf\{D_t(f) \,:\, f \in \mathcal{F}_n, W(f) = w\}.$$

To apply induction, it is useful to count the number of disjoint pairs between two (often different) fractional set systems. Given $n, t \in \mathbb{N}$ and $f, g \in \mathcal{F}_n$, we define

$$D_t(f, g) = \sum_{\substack{(A,B) \in 2^{[n]} \times 2^{[n]} \\ |A \cap B| < t}} f(A) \oplus g(B).$$

Notice, in particular, that $D_t(f) = D_t(f,f)$. Given $v, w \in \mathbb{R}$, define

$$D_{n,t}(v,w) = \inf\left\{D_t(f,g) \,:\, f,g \in \mathcal{F}_n, W(f) = v, W(g) = w\right\}.$$

Given a fixed weight w with $0 \le w \le 2^n$, there is exactly one $f \in \mathcal{F}_n$ of weight w for which there exists $k \in [0,n]$ and $\alpha \in [0,1]$ such that

$$f(A) = \begin{cases} 1, & |A| > k; \\ \alpha, & |A| = k; \\ 0, & |A| < k. \end{cases}$$

We call this the *fractional Hamming ball of weight w on $2^{[n]}$*, and denote it by b_n^w or just b^w. Notice, in particular, that if $w = \binom{n}{\ge r}$ for some $n, r \in \mathbb{N}$ then b_n^w is $\{0,1\}$-valued and it corresponds to the set $\binom{[n]}{\ge r}$.

In [10], Bollobás and Leader proved the following theorem.

Theorem 3.3.1 (Bollobás and Leader)**.** *Given $n \in \mathbb{N}$ and $v, w \in \mathbb{R}$,*

$$D_{n,1}(v,w) = D_1(b_n^v, b_n^w).$$

□

The paper ([10]) claims that this theorem is true if 1 is replaced by t. We give a very small counterexample to establish that this claim is false.

Example 1. *Let $t > 1$ and consider $D_{1,t}(1,1)$. Let $f \in \mathcal{F}_1$ be given by $f(\{1\}) = .5$ and $f(\emptyset) = .5$. We have that $D_t(f,f) = 0$. On the other hand, $D_t(b_1^1, b_1^1) = 1$. Similarly, for any positive integers n, t with $2 \le t \le n$, we have $D_{n,t}(2^{n-1}, 2^{n-1}) = 0$, but $D_t(b_n^{2^{n-1}}, b_n^{2^{n-1}}) > 0$.*

It is not the case that there are only counterexamples for relatively low weights. To see this, we first establish some general facts about D_t minimizing fractional set systems in Section 3.3.2. In Section 3.3.3 we use these facts to give a large class of counterexamples. Finally, in section 3.3.4 we use these facts to produce an efficient algorithm to "graph" $D_{n,t}(w)$ for given n and t.

3.3.2 Facts About Optimal Fractional Set Systems

This section establishes some new facts about D_t minimizing fractional set systems. Let $f \in \mathcal{F}_n$. Notice that we can interpret f as a point in $[0,1]^{(2^n)}$, a compact space. Notice further that W is a continuous function on $[0,1]^{(2^n)}$. Thus, given $r \in \mathbb{R}$, we have that $W^{-1}(r)$ is compact. Finally, D_t is a continuous function on this compact space of fixed weight points. Thus it achieves its minimum. In other words, given $0 \leq w \leq 2^n$, there is $f \in \mathcal{F}_n$ with $W(f) = w$ and $D_{n,t}(w) = D_t(f)$. We now prove some facts about the structure of such an optimal fractional set system.

A fractional set system $f \in \mathcal{F}_n$ is called *constant on layers* if for all $A, B \in 2^{[n]}$ with $|A| = |B|$, we have $f(A) = f(B)$. We may turn any fractional set system into one which is constant on layers by averaging each layer. More precisely, given $f \in \mathcal{F}_n$, we define the *smear operation* $\sigma : F_n \to F_n$ by

$$\sigma(f)(A) = \binom{n}{|A|}^{-1} \sum_{B \in \binom{[n]}{|A|}} f(B).$$

According to the following lemma, smearing a set system never increases D_t.

Lemma 3.3.2. *Given fractional set systems $f, g \in \mathcal{F}_n$, we have*

$$D_t(\sigma(f), \sigma(g)) \leq D_t(f, g).$$

To prove Lemma 3.3.2, we establish a more general fact that relies on the convexity of D_t.

Lemma 3.3.3. *The function D_t is convex. That is, given $n, t \in \mathbb{N}$, $f_1, g_1, f_2, g_2 \in \mathcal{F}_n$, and $\lambda \in [0,1]$, we have*

$$D_t(\lambda(f_1, g_1) + (1-\lambda)(f_2, g_2)) \leq \lambda D_t(f_1, g_1) + (1-\lambda) D_t(f_2, g_2).$$

Proof. Notice that the function $h(x) = \max\{0, x\}$ is convex. This is the source of the only inequality below.

$$\begin{aligned}
&D_t(\lambda(f_1, g_1) + (1-\lambda)(f_2, g_2)) \\
&\quad = \sum_{\substack{(A,B)\in 2^{[n]}\times 2^{[n]} \\ |A\cap B|<t}} (\lambda f_1(A) + (1-\lambda) f_2(A)) \oplus (\lambda g_1(B) + (1-\lambda) g_2(B)) \\
&\quad = \sum_{\substack{(A,B)\in 2^{[n]}\times 2^{[n]} \\ |A\cap B|<t}} h\left(\lambda(f_1(A) + g_1(B) - 1) + (1-\lambda)(f_2(A) + g_2(B) - 1)\right) \\
&\quad \leq \sum_{\substack{(A,B)\in 2^{[n]}\times 2^{[n]} \\ |A\cap B|<t}} \lambda h\left(f_1(A) + g_1(B) - 1\right) \\
&\qquad + \sum_{\substack{(A,B)\in 2^{[n]}\times 2^{[n]} \\ |A\cap B|<t}} (1-\lambda) h\left(f_2(A) + g_2(B) - 1\right) \\
&\quad = \lambda D_t(f_1, g_1) + (1-\lambda) D_t(f_2, g_2).
\end{aligned}$$

□

Define the graph $G_{n,t}$ to be the bipartite graph each of whose partite sets is a copy of $2^{[n]}$, and where AB is an edge if $|A \cap B| < t$. Let $\mathcal{P} = \{P_1, P_2, \ldots, P_p\}$ be a partition of the vertices of $G_{n,t}$. Given $v \in G_{n,t}$, let P_v be the part that contains v. A pair $(f, g) \in \mathcal{F}_n \times \mathcal{F}_n$ is naturally a vertex weighting $(f, g) : V(G_{n,t}) \to \mathbb{R}$. Define

$\sigma_{\mathcal{P}}(f,g)$ to be the pair $(f',g') \in \mathcal{F}_n \times \mathcal{F}_n$ given by

$$(f',g')(v) = \frac{1}{|P_v|} \sum_{v' \in P_v} (f,g)(v').$$

In particular, if $\mathcal{A}$ is a group of automorphisms of $G_{n,t}$ and if the orbits of $\mathcal{A}$ are the sets of $\mathcal{O} = \{O_1, O_2, \ldots, O_p\}$, we define $\sigma_{\mathcal{A}} = \sigma_{\mathcal{O}}$.

Lemma 3.3.4. *Given $n, t \in \mathbb{N}$, if $\mathcal{A}$ is a group of automorphisms of $G_{n,t}$ then given $f, g \in \mathcal{F}_n$, we have*

$$D_t(\sigma_{\mathcal{A}}(f,g)) \le D_t(f,g).$$

In order to prove Lemma 3.3.4, we will make use of Jensen's Inequality [19], which says that convex functions are sublinear for convex combinations. More precisely, we have

Lemma 3.3.5 (Jensen's Inequality)**.** *Let $\phi : \mathbb{R} \to \mathbb{R}$ be convex. If $x_1, x_2, \ldots, x_n$ are reals and $\lambda_1, \lambda_2, \ldots, \lambda_n$ are positive weights that sum to 1 then*

$$\phi\left(\sum_{i=1}^{n} \lambda_i x_i\right) \le \sum_{i=1}^{n} \lambda_i \phi(x_i).$$

□

Proof of Lemma 3.3.4. Since $\mathcal{A}$ acts on $V(G_{n,t})$, there is a natural action of $\mathcal{A}$ on $\mathcal{F}_n \times \mathcal{F}_n$: Given $\phi \in \mathcal{A}$ and $(f,g) \in \mathcal{F}_n \times \mathcal{F}_n$, we define $\phi(f,g)$ to be the function in $\mathcal{F}_n \times \mathcal{F}_n$ given by

$$\phi(f,g)(v) = (f,g)(\phi^{-1}(v)).$$

Because ϕ is a graph automorphism, we have

$$D_t(\phi(f,g)) = D_t(f,g).$$

Furthermore,

$$\sigma_{\mathcal{A}}(f,g) = \frac{1}{|\mathcal{A}|}\sum_{\phi\in\mathcal{A}} \phi(f,g).$$

By Lemma 3.3.3, D_t is convex. By 3.3.5 (Jensen's Inequality), we have

$$D_t(\sigma_{\mathcal{A}}(f,g)) = D_t\left(\frac{1}{|\mathcal{A}|}\sum_{\phi\in\mathcal{A}} \phi(f,g)\right) \leq \frac{1}{|\mathcal{A}|}\sum_{\phi\in\mathcal{A}} D_t(\phi(f,g)) = D_t(f,g).$$

□

We may use this fact to establish Lemma 3.3.2.

Proof of Lemma 3.3.2. Let $\phi \in S_n$ be a permutation of $[n]$. Notice that ϕ induces a graph automorphism on $G_{n,t}$: a vertex $A \subseteq [n]$ in a partite set of $G_{n,t}$ is sent to the copy of $\phi(A)$ in the same partite set. Two vertices $v, w \in G_{n,t}$ are in the same orbit of S_n if and only if $|v| = |w|$ and v and w are in the same partite set. Thus $\sigma = \sigma_{\mathcal{A}}$, and so the claim follows by Lemma 3.3.4. □

Notice that in $G_{n,t}$, every set $A \in \binom{[n]}{<t}$ is connected to every other set (in the opposite partition). Thus the set of maps that permute these vertices (without changing partitions) and fix all other vertices is a group of automorphisms of $G_{n,t}$. By applying Lemma 3.3.4 and Lemma 3.3.2, we then have the following fact.

Lemma 3.3.6. *Let $n \in \mathbb{N}$, $t \in [0,n]$, and $u, w \in \mathbb{R}$ with $0 \leq u, w \leq 2^{[n]}$. There are $f, g \in \mathcal{F}_n$ with*

$$D_{n,t}(u,w) = D_t(f,g),$$

where f and g are constant on layers, $W(f) = u$, $W(g) = w$, and for all $A, B \in \binom{[n]}{<t}$ we have $f(A) = f(B)$ and $g(A) = g(B)$.

□

We say a fractional set system, f, is *constant below* t if $f(A) = f(B)$ for all $A, B \in \binom{[n]}{<t}$. By Lemma 3.3.6, we may assume without loss of generality that a D_t-minimizing fractional set system is constant on layers and constant below t. We call such a fractional set system *t-constant*. We denote the set of t-constant fractional set systems of weight w on $[n]$ by $\mathcal{K}_{n,t}^{w}$. Given $f \in \mathcal{K}_{n,t}^{w}$ and $i \in [0, n]$, we may define

$$f_i = f(A),$$

where A is any set in $\binom{[n]}{i}$. For all $j, k < t$, we have $f_j = f_k$. We will denote this common weight by $f_{<t}$.

Given $n, t \in \mathbb{N}$ and $w \in \mathbb{R}$ with $0 \leq w \leq 2^n$, we would like there to exist an $f \in \mathcal{K}_{n,t}^{w}$ such that $D_{n,t}(w, w) = D_t(f, f)$. This would imply $D_{n,t}(w, w) = D_{n,t}(w)$. The following lemma establishes this.

Lemma 3.3.7. *Given $n, t \in \mathbb{N}$ and $f, g \in \mathcal{F}_n$,*

$$D_t\left(\frac{f+g}{2}, \frac{f+g}{2}\right) \leq D_t(f, g).$$

Proof. Notice that the function $\phi : G_{n,t} \to G_{n,t}$ sending a vertex $A \in G_{n,t}$ to the copy of itself in the opposite partite set is a graph automorphism. Further, $\mathcal{A} = \{1, \phi\}$ is a group. Applying Lemma 3.3.4 gives the desired result. □

We now introduce another important property of a D_t-minimizing fractional set system. We say a function $f \in \mathcal{F}_n$ is *nondecreasing* if for all $A, B \in 2^{[n]}$ with $|A| \leq |B|$, we have $f(A) \leq f(B)$. (Notice that if f is nondecreasing then it is constant on layers.) We have the following lemma.

Lemma 3.3.8. *Given $n \in \mathbb{N}$ and $v, w \in \mathbb{R}$, there are nondecreasing fractional set systems $f, g \in \mathcal{F}_n$ with $W(f) = v$ and $W(g) = w$ such that $D_{n,t}(v, w) = D_t(f, g)$.*

To aid in the proof, we introduce the following notation: Given $n, t \in \mathbb{N}$, $A \subseteq [n]$, and $j \in [0, n]$, the number of j-sets of $[n]$ that are *t-disjoint* from A is

$$\Lambda(A, j) = \Lambda_{n,t}(A, j) = \left| \left\{ B \in \binom{[n]}{j} \, : \, |A \cap B| < t \right\} \right|.$$

Notice that as a function of A, $\Lambda_{n,t}(A, j)$ only depends on $|A|$. In particular, if $|A| = i$, we define

$$\Lambda(i, j) = \Lambda(A, j) = \sum_{d=0}^{t-1} \binom{i}{d} \binom{n-i}{j-d}.$$

Proof of Lemma 3.3.8. Let $n, t \in \mathbb{N}$ and $v, w \in \mathbb{R}$. Suppose

$$D_{n,t}(v, w) = D_t(f, g),$$

Where $f, g \in \mathcal{F}_n$ be constant on layers with $W(f) = v$ and $W(g) = w$. Define

$$s(f, g) = \sum_{i=0}^{n} i(f_i + g_i).$$

We may assume (by another compactness argument) that $s(f, g)$ is maximized over all pairs $(f, g) \in \mathcal{F}_n \times \mathcal{F}_n$ that are constant on layers, have the proper weight, and satisfy $D_t(f, g) = D_{n,t}(v, w)$. We want to show that f and g are nondecreasing. Suppose by way of contradiction that there are integers $0 \leq i < j \leq n$ such that $f_i > f_j$ (the case $g_i > g_j$ is the same). We will shift some weight from i to j to obtain f' with $s(f', g) > s(f, g)$. By shifting wisely, we will have $D_t(f', g) \leq D_t(f, g)$, a contradiction. To that end, choose $\Delta W > 0$ small enough that for all $k \in [0, n]$ for which $f_j + g_k < 1$, we have $f_j + g_k + \binom{n}{j}^{-1} \Delta W < 1$. The quantity ΔW should also be small enough that $f_i - \binom{n}{i}^{-1} \Delta W \geq f_j + \binom{n}{j}^{-1} \Delta W$. Finally, it should be the case that $f_j + \binom{n}{j}^{-1}\Delta W \le 1$. Define $f' \in \mathcal{F}_n$ by

$$f'(A) = \begin{cases} f(A), & \text{if } |A| \notin \{i,j\}\,; \\ f_j + \binom{n}{j}^{-1}\Delta W & \text{if } |A| = j; \\ f_i - \binom{n}{i}^{-1}\Delta W & \text{if } |A| = i. \end{cases}$$

Notice that $W(f') = W(f)$, and that $s(f',g) = s(f,g) + (j-i)\Delta W$. Further notice that

$$\begin{aligned} D_t(f,g) - D_t(f',g) &= \sum_{\substack{A\in\binom{[n]}{j}, B\in 2^{[n]} \\ |A\cap B|<t}} [f(A)\oplus g(B) - f'(A)\oplus g(B)] \\ &\quad + \sum_{\substack{A\in\binom{[n]}{i}, B\in 2^{[n]} \\ |A\cap B|<t}} [f(A)\oplus g(B) - f'(A)\oplus g(B)] \\ &= \sum_{k=0}^{n}\Bigg(\sum_{\substack{A\in\binom{[n]}{j}, B\in\binom{[n]}{k} \\ |A\cap B|<t}} [f(A)\oplus g(B) - f'(A)\oplus g(B)] \\ &\quad + \sum_{\substack{A\in\binom{[n]}{i}, B\in\binom{[n]}{k} \\ |A\cap B|<t}} [f(A)\oplus g(B) - f'(A)\oplus g(B)]\Bigg) \end{aligned} \tag{3.3.1}$$

Fix $k \in [0,n]$. We show that the corresponding term in (3.3.1) is nonnegative. We have two cases: either $f_j + g_k < 1$ or $f_j + g_k \ge 1$. If $f_j + g_k < 1$ then, by our choice of ΔW, we have $f'_j + g_k < 1$. Thus, for all $A \in \binom{[n]}{j}$ and $B \in \binom{[n]}{k}$, we have $f(A)\oplus g(B) = 0$ and $f'(A)\oplus g(B) = 0$. For $A \in \binom{[n]}{i}$ and $B \in \binom{[n]}{k}$, $f(A)\oplus g(B) - f'(A)\oplus g(B)$ is always nonnegative, so the case $f_j + f_k < 1$ is settled.

If $f_j + g_k \ge 1$ then $f_i + g_k \ge 1$ and $f'_j + g_k \ge 1$. By our choice of ΔW, we have

$f_i' + f_k \geq 1$. Thus

$$\begin{aligned}
&\sum_{\substack{A\in\binom{[n]}{j}, B\in\binom{[n]}{k} \\ |A\cap B|<t}} [f(A)\oplus g(B) - f'(A)\oplus g(B)] \\
&\qquad = \sum_{\substack{A\in\binom{[n]}{j}, B\in\binom{[n]}{k} \\ |A\cap B|<t}} \left[(f_j + g_k - 1) - \left(f_j + \binom{n}{j}^{-1}\Delta W + g_k - 1\right)\right] \\
&\qquad = -\binom{n}{j}\Lambda(j,k)\binom{n}{j}^{-1}\Delta W \\
&\qquad = -\Lambda(j,k)\Delta W.
\end{aligned}$$

Similarly,

$$\sum_{\substack{A\in\binom{[n]}{i}, B\in\binom{[n]}{k} \\ |A\cap B|<t}} [f(A)\oplus g(B) - f'(A)\oplus g(B)] = \Lambda(i,k)\Delta W.$$

Notice that because $j > i$, there are more k sets that have small intersection with a given i set than there are k sets that have small intersection with a given j set. In other words, $\Lambda(j,k) \leq \Lambda(i,k)$. Hence the term corresponding to k in (3.3.1) is nonnegative. □

We say a set system $f \in \mathcal{K}_{n,t}^{w}$ is *t-canonical* if f is nondecreasing. We denote the set of t-canonical fractional set systems of weight w on $[n]$ by $\mathcal{C}_{n,t}^{w}$.

3.3.3 Counterexamples

In this section we give some more counterexamples to the $t > 1$ case of Theorem 3.3.1 of Bollobás and Leader. We also find the $D_{n,t}$ minimizing fractional set systems when $t > \lceil \frac{n}{2} \rceil$.

Example 2. *Let $n, t \in \mathbb{N}$, where $t \leq n$. For $w \in \mathbb{R}$ with*

$$\binom{n}{\geq t} + \frac{1}{2}\binom{n}{t-1} < w < 2^n - \frac{1}{2},$$

we have $D_t(b_n^w) > D_{n,t}(w)$.

Proof. Let $A = \{1, 2, \ldots, t-1\}$. By our choice of w, we have $b_n^w(A) > 1/2$, and $b_n^w(\emptyset) < 1/2$. Thus we may choose $\Delta w > 0$ to be a real number with

$$\Delta w < \min \left\{ b_n^w(A) - 1/2, 1/2 - b_n^w(\emptyset) \right\}.$$

Define $f \in \mathcal{F}_n$ by

$$f(B) = \begin{cases} b_n^w(B) & \text{if } B \notin \{A, \emptyset\}; \\ b_n^w(A) - \Delta w & \text{if } B = A; \\ \Delta w & \text{if } B = \emptyset. \end{cases}$$

Since A and $\emptyset$ each have size less than t, the intersection with either of them and any other set in $2^{[n]}$ has size less than t. Thus

$$
\begin{aligned}
&D_t(b_n^w) - D_t(f) \\
&\quad = 2 \sum_{B \in 2^{[n]} \setminus \{\emptyset, A\}} [b_n^w(A) \oplus b_n^w(B) + b_n^w(\emptyset) \oplus b_n^w(B) - f(A) \oplus f(B) - f(\emptyset) \oplus f(B)] \\
&\qquad + b_n^w(A) \oplus b_n^w(A) + b_n^w(\emptyset) \oplus b_n^w(\emptyset) \\
&\qquad - f(A) \oplus f(A) - f(\emptyset) \oplus f(\emptyset) \\
&\quad = 2 \sum_{B \in 2^{[n]} \setminus \{\emptyset, A\}} [(b_n^w(A) \oplus b_n^w(B) - f(A) \oplus f(B)) + (b_n^w(\emptyset) \oplus b_n^w(B) - f(\emptyset) \oplus f(B))] \\
&\qquad + (b_n^w(A) + b_n^w(A) - 1) - (f(A) + f(A) - 1) \\
&\quad = 2 \sum_{B \in 2^{[n]} \setminus \{\emptyset, A\}} [(b_n^w(A) \oplus b_n^w(B) - f(A) \oplus f(B)) + (b_n^w(\emptyset) \oplus b_n^w(B) - f(\emptyset) \oplus f(B))] \\
&\qquad + 2\Delta w.
\end{aligned}
$$

Let $B \notin \{A, \emptyset\}$. We would like to show that

$$(b_n^w(A) \oplus b_n^w(B) - f(A) \oplus f(B)) + (b_n^w(\emptyset) \oplus b_n^w(B) - f(\emptyset) \oplus f(B)) \geq 0.$$

Since $f(A) < b_n^w(A)$, we have that $b_n^w(A) \oplus b_n^w(B) - f(A) \oplus f(B) \geq 0$. If $b_n^w(\emptyset) \oplus b_n^w(B) - f(\emptyset) \oplus f(B) \geq 0$, we're done. Otherwise, $f(\emptyset) \oplus f(B) > 0$, so $f(\emptyset) \oplus f(B) =$

$f(\emptyset) + f(B) - 1$. Thus

$$\begin{aligned}
(b_n^w(A) \oplus b_n^w(B) - f(A) \oplus f(B)) + (b_n^w(\emptyset) \oplus b_n^w(B) - f(\emptyset) \oplus f(B)) \\
&= (f(A) + \Delta w + f(B) - 1) - (f(A) + f(B) - 1) \\
&\quad + (f(\emptyset) - \Delta w) \oplus f(B) - (f(\emptyset) + f(B) - 1) \\
&= \Delta w \\
&\quad + (f(\emptyset) - \Delta w) \oplus f(B) - (f(\emptyset) + f(B) - 1) \\
&\geq \Delta w \\
&\quad + (f(\emptyset) - \Delta w + f(B) - 1) - (f(\emptyset) + f(B) - 1) \\
&= 0.
\end{aligned}$$

Thus $D_t(b_n^w) - D_t(f) \geq 2\Delta w > 0$ as desired. $\square$

Next we find minimizers in the case where $t > \lceil n/2 \rceil$. Furthermore, we will see that b_n^w is (usually) not a minimizer in this case. Given $n, t \in \mathbb{N}$ and a fixed weight w with $2^{n-1} \leq w \leq 2^n$, there is exactly one $f \in \mathcal{C}_{n,t}^w$ of the form

$$f(A) = \begin{cases} 1 & \text{if } |A| > k; \\ \alpha & \text{if } |A| = k; \\ 1/2 & \text{if } |A| < k. \end{cases}$$

Here $\alpha \in \mathbb{R}$ has $1/2 \leq \alpha < 1$, and $k \in [t-1, n]$. (Recall that for $i < t-1$, we have $f_i = f_{t-1}$.) We call f the *t-half-ball of weight w on $2^{[n]}$*. For $w < 2^{n-1}$, the system with constant weight $f(A) = w2^{-n}$ will also be called a t-half-ball. We denote the t-half-ball of weight w on $2^{[n]}$ by $h_{n,t}^w$.

Theorem 3.3.9. *Let $n, t \in \mathbb{N}$ with $t > \left\lceil \dfrac{n}{2} \right\rceil$, and let $w \in \mathbb{R}$ with $0 \leq w \leq 2^n$. Then*

$$D_{n,t}(w) = D_t(h^w_{n,t}).$$

Proof. If $w \leq 2^{n-1}$, then $h^w_{n,t}$ is the constant fractional set system with total weight w. This constant value is no more than $1/2$, so $D_t(h^w_n) = 0 = D_{n,t}(w)$ as desired. Thus we assume that $w > 2^{n-1}$.

Let $f \in \mathcal{C}^w_{n,t}$ with $D_{n,t}(w) = D_t(f)$. We may assume (by a compactness argument) that $f_{<t}$ is as large as possible. We claim that $f_{<t} \geq 1/2$.

Suppose, on the contrary, that $f_{<t} < 1/2$. Notice that $\{j \in [0, n] : f_j > 1/2\}$ is nonempty since $w > 2^{n-1}$. Let

$$l = \min \{j \in [0, n] \, : \, f_j > 1/2\} .$$

Notice that $l > t - 1$. Choose $\Delta w > 0$ small enough so that $f_{l-1} + \binom{n}{\leq l-1}^{-1} \Delta w \leq f_l - \binom{n}{\geq l}^{-1} \Delta w$ and $f_{l-1} + \binom{n}{\leq l-1}^{-1} \Delta w \leq 1/2$. Define $g \in \mathcal{C}^w_{n,t}$ by

$$g_i = \begin{cases} f_i - \binom{n}{\geq l}^{-1} \Delta w & \text{if } i \geq l; \\ f_i + \binom{n}{\leq l-1}^{-1} \Delta w & \text{if } i < l. \end{cases}$$

We show that for any $(i, j) \in [0, n] \times [0, n]$, we have $g_i \oplus g_j \leq f_i \oplus f_j$. For $(i, j) \in [l, n] \times [l, n]$, we have $g_i < f_i$ and $g_j < f_j$. Thus $g_i \oplus g_j \leq f_i \oplus f_j$. For $(i, j) \in [l, n] \times [0, l-1]$, we have $g_i + g_j = f_i - \binom{n}{\geq l}^{-1} \Delta w + f_j + \binom{n}{\leq l-1}^{-1} \Delta w$. But $l \geq t > \lceil n/2 \rceil$, so $\binom{n}{\geq l} \leq \binom{n}{\leq l-1}$ and hence $g_i + g_j \leq f_i + f_j$, so $g_i \oplus g_j \leq f_i \oplus f_j$. Similarly, for $(i, j) \in [0, l-1] \times [l, n]$, we have $g_i \oplus g_j \leq f_i \oplus f_j$. If $(i, j) \in [0, l-1] \times [0, l-1]$ then, by our choice of Δw, we have that g_i and g_j are both no more than $1/2$, and so $g_i + g_j \leq 1$, and $g_i \oplus g_j = 0 \leq f_i \oplus f_j$.

Recall that $\Lambda(i,j)$ is defined on page 28. We have

$$\begin{aligned} D_t(g) &= \sum_{(i,j)\in[0,n]\times[0,n]} \binom{n}{i}\Lambda(i,j)\,(g_i \oplus g_j) \\ &\leq \sum_{(i,j)\in[0,n]\times[0,n]} \binom{n}{i}\Lambda(i,j)\,(f_i \oplus f_j) \\ &= D_t(f). \end{aligned}$$

But by our choice of Δw, we have $g \in \mathcal{C}_{n,t}^w$ and furthermore $g_{<t} > f_{<t}$. This is a contradiction. Hence $f_{<t} \geq 1/2$.

Since f is nondecreasing, it follows that

$$D_t(f) = \sum_{\substack{(A,B)\in 2^{[n]}\times 2^{[n]} \\ |A\cap B|<t}} f(A) + f(B) - 1.$$

This is an affine function. Thus we want to keep weight in the sets that occur least often in the sum. That is, we want as much weight as possible in large sets while maintaining the property that the weight on every set is at least $1/2$. Of course, $h_{n,t}^w$ does exactly that, and so $D_{n,t}(w) = D_t(f) \geq D_t(h_{n,t}^w)$, and the theorem is proved. □

The following Lemma shows that under the conditions of Theorem 3.3.9, b_n^w is only a minimizer when w is so small that $D_t(b_n^w) = 0$ or when w is so large that anything sensible is a minimizer.

Corollary 3.3.10. *Let $n, t \in \mathbb{N}$ with $t > \left\lceil \frac{n}{2} \right\rceil$. Then given $w \in \mathbb{R}$ with $D_t(b_n^w) > 0$ and $w < 2^n - 1/2$, we have*

$$D_t(b_n^w) > D_{n,t}(w).$$

Proof. If $w > \binom{n}{\geq t} + \frac{1}{2}\binom{n}{t-1}$ then by Example 2, we are done. Thus we assume that $w \leq \binom{n}{\geq t} + \frac{1}{2}\binom{n}{\leq t-1}$. Smearing b_n^w below t yields f, a t-canonical fractional set system with the property that $f_{<t} < 1/2$ and $D_t(f) \leq D_t(b_n^w)$. If $D_t(f) = 0 < D_t(b_n^w)$, then we are done. Otherwise, since f is t-canonical and $f_{<t} < 1/2$, we may apply the shift described in the proof of Theorem 3.3.9. Since $D_t(f) > 0$, the shift strictly decreases D_t. □

3.3.4 An Algorithmic Solution

Given $n, t \in \mathbb{N}$ and w with $0 \leq w \leq 2^n$, we say a fractional set system $f \in \mathcal{F}_n$ is a *t-pseudo-ball* if it is t-canonical, and $f_i \in \{0, 1/2, 1\}$ for all $i \in [n]$. Notice that the number of t-pseudo-balls in $\mathcal{C}_{n,t}^w$ is finite. In fact, there are $\binom{n-t+4}{2}$ t-pseudo-balls in $\mathcal{C}_{n,t}^w$. We have the following theorem, which we will prove after we have established some supporting facts.

Theorem 3.3.11. *$D_{n,t}(w)$ is the maximum convex function with the property that*

$$D_{n,t}(W(f)) \leq D_{n,t}(f) \textit{ where } f \textit{ is any } t\textit{-pseudo-ball.}$$

In particular, $D_{n,t}(w)$ is piecewise linear and the points where the slope changes correspond to pseudo-balls. Thus we may "graph" $D_{n,t}(w)$ as follows: compute D_t for each of the pseudo-balls and then use a convex hull-like algorithm to determine $D_{n,t}(w)$. There are $\binom{n-t+4}{2} = O(n^2)$ pseudo-balls in $\mathcal{C}_{n,t}^w$, and it takes $O(n^3)$ time to compute D_t of a given pseudo-ball. This yields an $O(n^5)$ run time to compute D_t for every pseudo-ball. We apply the convex hull-like algorithm to the $O(n^2)$ pseudo-balls. This takes $O(n^4)$ time. Overall this process completes in $O(n^5)$ time. We have implemented this algorithm in Mathematica. We used this technique to produce Figure 3.3.4, a graph of $D_{56,14}(w)$ and $D_{14}(b_{56}^w)$. Notice that $D_{56,14}(w) \leq D_{14}(b_{56}^w)$, with strict inequality for many values of w.

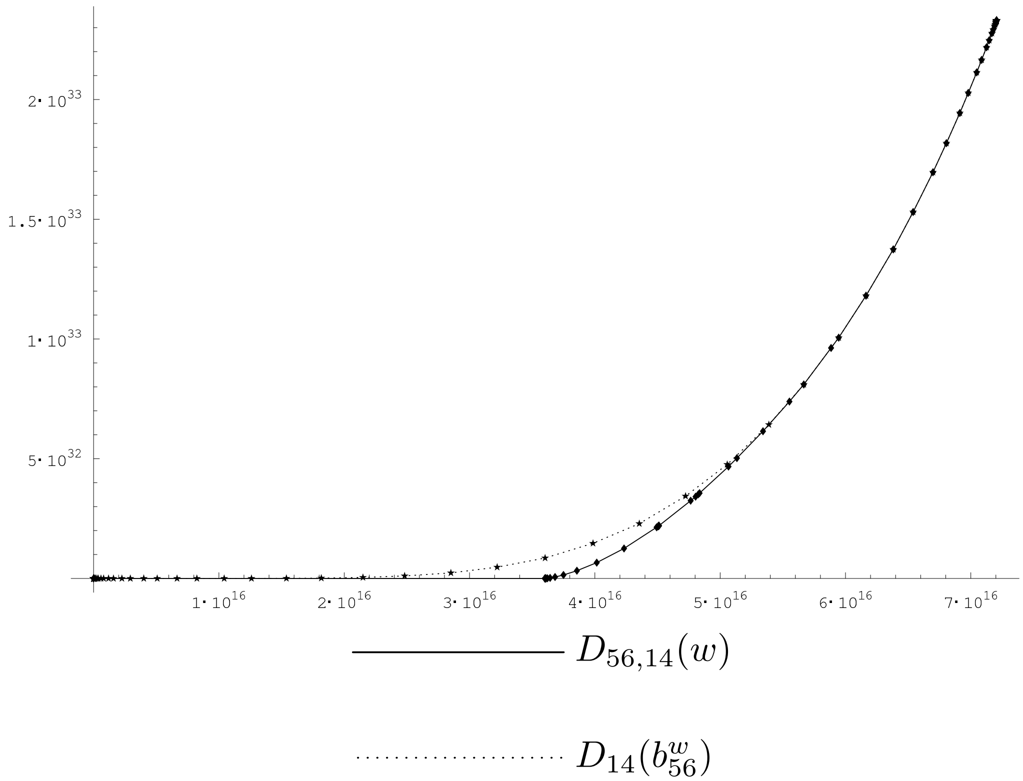

Figure 3.1: $D_{56,14}(w)$ and $D_{14}(b_{56}^w)$

To prove Theorem 3.3.11, we make use of the following fact.

Theorem 3.3.12. *Given $n, t \in \mathbb{N}$ and $0 \leq w \leq 2^n$, there is $f \in \mathcal{C}_{n,t}^w$ with $D_{n,t}(w) = D_t(f)$ and with $(f_i)_{i=0}^n$ having the form*

$$(f_i)_{i=0}^n = (\underbrace{0, \ldots 0}_{l_0}, \underbrace{1-\delta, \ldots, 1-\delta}_{l_{1-\delta}}, \underbrace{1/2, \ldots, 1/2}_{l_{1/2}}, \underbrace{\delta, \ldots, \delta}_{l_\delta}, \underbrace{1, \ldots, 1}_{l_1}),$$

where $1/2 < \delta < 1$, and $l_0, l_{1-\delta}, l_{1/2}, l_\delta, l_1 \in [0, n+1]$ are integers that sum to $n+1$.

Proof of Theorem 3.3.12. We will see that the space $\mathcal{C}_{n,t}^w$ can be divided into finitely many parts, $P_1, \ldots, P_p$ defined by linear inequalities, in such a way that D_t is an affine function on each part. Thus, on each part, minimizing D_t is a linear programming problem (for more on linear programming, see [14], for example). Recall that if a (minimizing) solution to a linear programming problem exists, then there is a solution at a vertex of the feasible region of the problem. We will see that for all i, every vertex in P_i is of the form claimed in the lemma. Since the D_t minimizing f must appear in one of the parts, the lemma will be established.

First, we may think of a fractional set system $f \in \mathcal{C}^w_{n,t}$ as a function in $\mathbb{R}^{\{t-1,\ldots,n\}}$. This function is subject to the following linear constraints. (Recall that we use $f_{<t}$ to denote the common weight on the sets of size less than t. This is identical to f_{t-1}.)

$$W(f) = w \tag{3.3.2}$$

$$0 \leq f_{<t} \tag{3.3.3}$$

$$f_i \leq f_{i+1} \text{ for all } i \in [t-1, n-1] \tag{3.3.4}$$

$$f_n \leq 1 \tag{3.3.5}$$

Let $R \subseteq [t-1,n] \times [t-1,n]$. Then we define P_R to be the set of functions $f \in \mathcal{C}^w_{n,t}$ subject to additional constraints

$$f_i + f_j \geq 1 \text{ if } (i,j) \in R \tag{3.3.6}$$

$$f_i + f_j \leq 1 \text{ if } (i,j) \notin R \tag{3.3.7}$$

Notice that, given $f \in \mathcal{C}^w_{n,t}$, every pair $(i,j) \in [t-1,n] \times [t-1,n]$ either has $f_i + f_j \leq 1$ or $f_i + f_j \geq 1$, and so f is in some P_R. More importantly, if we set

$$c_{i,j} = \begin{cases} \binom{n}{i} \Lambda(i,j) & \text{if } i \geq t; \\ \binom{n}{<t} \sum_{k=0}^{t-1} \Lambda(i,k) & \text{if } i = t-1 \end{cases}$$

(where $\Lambda(i,j)$ is as defined on page 28) then for all $f \in P_R$,

$$D_t(f) = \sum_{(i,j)\in R} c_{i,j}(f_i + f_j - 1).$$

Thus D_t is affine on each P_R.

Fix R. We are now ready to find the vertices of P_R. We may think of the coefficients on a constraint as a vector in $\mathbb{R}^{n-t+2}$. For example, the constraint $f_i \leq f_{i+1}$ is equivalent to $f_i - f_{i+1} \leq 0$ and so it corresponds to a vector of the form

$$(0,\ldots,0,1,-1,0,\ldots,0).$$

Similarly, the constraint $f_i + f_j \geq 1$ becomes a vector with ones in positions i and j, and 0's elsewhere. Since we are thinking of $\mathcal{C}^w_{n,t}$ as an $n-t+2$ dimensional space, a fractional set system is a vertex if it achieves equality for $n-t+2$ linearly independent constraints. Notice that equality always holds for the weight constraint (3.3.2), and so we want equality to hold for $n-t+1$ linearly independent constraints of types (3.3.3)-(3.3.7).

Let $f \in P_R$ be a vertex of P_R. Given $\delta \in [1/2, 1]$, define

$$S_\delta = \{i \in [t-1, n] \,:\, f_i = \delta \text{ or } f_i = 1-\delta\}.$$

Define C_δ to be the set of coefficient vectors for the constraints of types (3.3.3)-(3.3.7) that f exactly meets, and where for some $i \in S_\delta$, the coefficient on f_i is nonzero. Let C be the set of vectors corresponding to all constraints for which f achieves equality. Define

$$r = \operatorname{rank} C.$$

By our choice of f, we have $r = n - t + 2$. On the other hand, if $\vec{w}$ is the vector corresponding to the weight constraint, then

$$C = \{\vec{w}\} \cup \bigcup_{\delta \in [1/2,1]} C_\delta,$$

and so

$$r \leq 1 + \sum_{\delta \in [1/2,1]} \operatorname{rank} C_\delta.$$

Notice that this sum is actually finite, since f only takes on finitely many values. Notice further that the only nonzero coefficients in a constraint in C_δ are on f_i with $f_i = \delta$ or $f_i = 1 - \delta$. Thus rank $C_\delta \leq |S_\delta|$. Consider δ not equal to 1/2 or 1. Given $v \in [0,1]$, denote $f^{-1}(v) = \{i \in [t-1, n] \,:\, f_i = v\}$. Let $p \in \mathbb{R}^{\{t-1,t,\ldots,n\}}$ be the vector that is 1 on $f^{-1}(\delta)$, -1 on $f^{-1}(1-\delta)$, and 0 everywhere else. Notice that no vector in C_δ corresponds to constraints (3.3.3) or (3.3.5), and so in particular for all $v \in C_\delta$, we have $v \cdot p = 0$. Thus when we restrict our vectors to S_δ (the support of C_δ), the dimension of the space perpendicular to C_δ is at least 1. This implies that

$$\operatorname{rank} C_\delta \leq |S_\delta| - 1.$$

Thus if d is the number of distinct nonempty S_δ other than S_1 and $S_{1/2}$, we have

$$\begin{aligned} n - t + 2 &= r \\ &\leq 1 + \sum_{\delta \in [1/2,1]} \operatorname{rank} C_\delta \\ &\leq 1 - d + \sum_{\delta \in [1/2,1]} |S_\delta| \\ &= 1 - d + n - t + 2. \end{aligned}$$

By canceling terms and rearranging, $d \leq 1$, and the claim is proved. $\square$

Proof of Theorem 3.3.11. First we show that $D_{n,t}$ is convex. Let w_1 and w_2 have $0 \leq w_1 \leq w_2 \leq 2^n$. For $i = 1$ or 2, there exists $f_i \in C_{n,t}^{w_i}$ such that $D_{n,t}(w_i) = D_t(f_i)$. Let $\lambda \in [0,1]$. We have

$$\begin{aligned} &D_{n,t}\left(\lambda w_1 + (1-\lambda) w_2\right) \\ &\quad \leq D_t\left(\lambda f_1 + (1-\lambda) f_2\right) && (\text{since } W(\lambda f_1 + (1-\lambda) f_2) = \lambda w_1 + (1-\lambda) w_2) \\ &\quad \leq \lambda D_t(f_1) + (1-\lambda) D_t(f_2) && (\text{since } D_t \text{ is convex by Lemma 3.3.3}) \\ &\quad = \lambda D_{n,t}(w_1) + (1-\lambda) D_{n,t}(w_2). \end{aligned}$$

Next we see that $D_{n,t}$ is piecewise linear. Let l_0, $l_{1-\delta}$, $l_{1/2}$, l_δ, and l_1 be nonnegative integers that sum to $n+1$. Also, let $\delta \in [1/2, 1]$. Define

$$f_\delta = (\underbrace{0, \ldots 0}_{l_0}, \underbrace{1-\delta, \ldots, 1-\delta}_{l_{1-\delta}}, \underbrace{1/2, \ldots, 1/2}_{l_{1/2}}, \underbrace{\delta, \ldots, \delta}_{l_\delta}, \underbrace{1, \ldots, 1}_{l_1}).$$

Notice that the weight of f_δ is affine in δ, as is $D_{n,t}(f_\delta)$. Thus

$$\{(W(f_\delta), D_t(f_\delta)) \,:\, \delta \in [1/2, 1]\}$$

is a line segment. By Theorem 3.3.12, $D_{n,t}(w)$ is the minimum value among all the line segments of this type that are defined at w. Thus $D_{n,t}$ is piecewise linear.

Changes of slope either occur at the ends of the line segments described above or at the intersection of two of them. As it turns out, slope does not change at an intersection of two of these line segments if the intersection is not also an endpoint of one of the line segments. Otherwise, near the point of intersection, $D_{n,t}$ would be the minimum of two line segments, which is not a convex function. Thus the slope of $D_{n,t}$ changes at endpoints of the line segments described above. But the endpoints occur where $W(f_\delta)$ is maximized or minimized. These extrema occur when $\delta = 1/2$ and $\delta = 1$. In either case, f_δ is a pseudo-ball. $\square$

Chapter 4

Extremal Problems Under Dimension Constraints

4.1 Introduction

4.1.1 The History of the Problem

A new type of restriction on set systems was recently introduced by Ahlswede, Aydinian, and Khachatrian [2]. The general problem is to take an existing class of set systems (intersecting families, for example) in $2^{[n]}$, think of them as collections of $\{0,1\}$-valued vectors in $\mathbb{R}^n$, and impose the further restriction that their rank be at most (or at least) k. We then ask for the largest (or smallest) such set. A first problem in this program is to determine $M(n,k,w)$, the largest number of $\{0,1\}$-valued vectors with (Hamming) weight w in a k-dimensional subspace of $\mathbb{R}^n$. This was solved in a separate paper of Ahlswede, Aydinian, and Khachatrian [3].

Theorem 4.1.1 (Ahlswede, Aydinian, and Khachatrian)**.**

$$M(n,k,w) = M(n,k,n-w),$$

and for $w \leq n/2$,

$$M(n,k,w) = \begin{cases} \binom{k}{w} & \text{if } 2w \leq k; \\ \binom{2(k-w)}{k-w} 2^{2w-k} & \text{if } k < 2w < 2(k-1); \\ 2^{k-1} & \text{if } k-1 \leq w. \end{cases}$$

□

The same problem can be posed in other vector spaces. This chapter of the dissertation will focus on partial results in the $\mathbb{F}_2^n$ case. To that end, define $m(n,k,w)$ to be the maximum number of weight w vectors contained in a k-dimensional subspace of $\mathbb{F}_2^n$. Determining $m(n,k,w)$ requires different techniques from those used to determine $M(n,k,w)$. For example, in the $\mathbb{R}^n$ case the solution given by Ahlswede, Aydinian, and Khachatrian makes explicit use of the fact that the sum of a nonempty collection of positive numbers in $\mathbb{R}$ is nonzero. We do not have this fact in $\mathbb{F}_2$. The methods used and results found in this dissertation are similar to methods and results from coding theory. A complete description of $m(n,k,w)$ might be important to coding theory, since it would shed light on the weight distributions of binary linear codes. What follows is an overview of the results in this section.

Ahlswede, Aydinian, and Khachatrian note that the value of $m(n,k,w)$ depends crucially on the parity of w. For example, assuming $w \neq 0$ we have $m(n,k,w) \leq 2^k - 1$. Furthermore, there are many examples where w is even and $m(n,k,w) = 2^k - 1$. On the other hand, at least half of the vectors in a subspace $\mathcal{C} < \mathbb{F}_2^n$ have even weight. Thus if w is odd, $m(n,k,w) \leq 2^{k-1}$. Given w even, we prove a (well-known) characterization of the parameters for which $m(n,k,w) = 2^k - 1$. Given w odd, we prove a (well-known) characterization of the parameters for which $m(n,k,w) = 2^{k-1}$. More generally, define $f_2(w)$ to be such that $2^{f_2(w)}$ is the largest power of 2 that divides w. We show that $m(n,k,w) \leq 2^k - 2^{k-1-f_2(w)}$, and we characterize the parameters for which $m(n,k,w)$ meets this bound.

During the research process, it became important to study linear maps that decrease the weight of non-zero vectors by a constant, c. We call these maps *c-killers*. The result of our study of c-killers is a structure theorem for such maps, which is interesting in its own right. This structure theorem is a slight generalization of a result from coding theory known as the MacWilliams Extension Theorem [23], which characterizes weight-preserving linear maps (0-killers). We apply our structure theorem to determine when $m(n,k,w) = 2^{k-1} - 1$ in the case where w is odd. The number of such cases turns out to be very small.

Additionally, we prove miscellaneous results which give insight into the problem, and lead to conjectures. For instance, these results together with numerical evidence suggest that for w odd, we have $m(n,k,w) = M(n,k,w)$.

We now proceed to the work. We refer the reader to Chapter 1 for our notation.

4.1.2 Basics of Finite Vector Spaces

Let $q \in \mathbb{N}$ be a prime power. Define $\mathbb{F}_q$ to be the unique field of order q. In particular, if $q = 2$ then $\mathbb{F}_2 = \{0, 1\}$, where addition and multiplication are defined mod 2. The set

$$\mathbb{F}_q^n = \{(b_1, b_2, \ldots, b_n) \,:\, b_i \in \mathbb{F}_q\}$$

is the set of strings of length n over the alphabet $\mathbb{F}_q$. We endow $\mathbb{F}_q^n$ with an addition and a scalar multiplication, both defined componentwise. More precisely, let a,$b \in \mathbb{F}_q^n$

and let $\lambda \in \mathbb{F}_q$. Then $a = (a_1, a_2, \ldots, a_n)$ and $b = (b_1, b_2, \ldots, b_n)$, and we have the following definitions.

$$a + b = ((a_1 + b_1), (a_2 + b_2), \ldots, (a_n + b_n))$$

and

$$\lambda a = (\lambda a_1, \lambda a_2, \ldots, \lambda a_n)\,.$$

In the binary case (ie when $q = 2$) we have

$$ca = \begin{cases} a & \text{if } c = 1; \\ \vec{0} & \text{if } c = 0, \end{cases}$$

where $\vec{0}$ is the all zeroes vector.

Since $\mathbb{F}_q$ is a field, $\mathbb{F}_q^n$ is an $\mathbb{F}_q$ vector space under this addition and multiplication. Let $\mathcal{C} < \mathbb{F}_q^n$ be a subspace of $\mathbb{F}_q^n$. That is, $\mathcal{C}$ is nonempty and closed under addition and scalar multiplication. Notice that for any $\mathbb{F}_2$-vector space, closure under scalar multiplication follows from being nonempty and closed under addition. Suppose $\mathcal{C}$ is k-dimensional. By standard linear algebra arguments, $\mathcal{C}$ is isomorphic to $\mathbb{F}_q^k$. In particular, $|\mathcal{C}| = q^k$.

Let $\vec{1}_n = (1, 1, 1, \ldots, 1) \in \mathbb{F}_q^n$. We call $\vec{1}_n$ the *all ones vector of length n*. Notice that if $a \in \mathbb{F}_2^n$ then $a + \vec{1}_n$ is the opposite of a in every component. We call this vector the *complement* of a, and we denote it by $\overline{a}$.

Given a subspace $\mathcal{C} < \mathbb{F}_q^n$, it is often convenient to permute its entries. More specifically, let $\sigma : [n] \to [n]$ be a permutation. Given $c = (c_1, c_2, \ldots, c_n) \in \mathcal{C}$, define

$$\sigma(c) = \left(c_{\sigma^{-1}(1)}, c_{\sigma^{-1}(2)}, \ldots, c_{\sigma^{-1}(n)}\right).$$

Extending this to the entire code, $\sigma(\mathcal{C}) = \{\sigma(c) : c \in \mathcal{C}\}$. Notice that $\mathrm{wt}(\sigma(c)) = \mathrm{wt}(c)$. We call any map with this property *weight preserving*. Furthermore, the action of $\sigma : \mathcal{C} \to \sigma(\mathcal{C})$ can be "undone" by applying the inverse permutation, so σ is one-to-one. Thus for all $w \in [n]$, we have that $A_w(\sigma(\mathcal{C}))$ (the number of weight w vectors in $\sigma(\mathcal{C})$) is the same as $A_w(\mathcal{C})$. Therefore, we may employ the following strategy when establishing bounds on $m(n, k, w)$.

1. Start with a k-dimensional subspace $\mathcal{C} < \mathbb{F}_2^n$ that has $A_w(\mathcal{C}) = m(n, k, w)$.

2. If it is more convenient than proving the bound directly, establish the bound on $A_w(\sigma(\mathcal{C}))$ instead.

It is important to notice that $\sigma : \mathcal{C} \to \sigma(\mathcal{C})$ is a linear bijection. As described above, σ is one-to-one. By definition it is onto. Notice that as part of establishing linearity, we should show that for any $\lambda \in \mathbb{F}_q$ and $b \in \mathcal{C}$, we have $\sigma(\lambda b) = \lambda\sigma(b)$. In the case of establishing $\mathbb{F}_2$-linearity, this just reduces to showing that $\sigma(\vec{0}) = \vec{0}$. Clearly, by permuting the entries of the all zeroes vector you get the all zeroes vector back. For a general prime power, $q \in \mathbb{N}$, we have that

$$\begin{aligned}
\sigma(\lambda b) &= \sigma(\lambda(b_1, b_2, \ldots, b_n)) \\
&= \sigma((\lambda b_1, \lambda b_2, \ldots, \lambda b_n)) \\
&= (\lambda b_{\sigma^{-1}(1)}, \lambda b_{\sigma^{-1}(2)}, \ldots, \lambda b_{\sigma^{-1}(n)}) \\
&= \lambda(b_{\sigma^{-1}(1)}, b_{\sigma^{-1}(2)}, \ldots, b_{\sigma^{-1}(n)}) \\
&= \lambda\sigma(b).
\end{aligned}$$

Given b and $c \in \mathcal{C}$, we wish to show that $\sigma(b) + \sigma(c) = \sigma(b + c)$. This is easy to establish.

$$\begin{aligned}
\sigma(b) + \sigma(c) &= \sigma\left((b_1, b_2, \ldots, b_n)\right) + \sigma\left((c_1, c_2, \ldots, c_n)\right) \\
&= \left(b_{\sigma^{-1}(1)}, b_{\sigma^{-1}(2)}, \ldots, b_{\sigma^{-1}(n)}\right) + \left(c_{\sigma^{-1}(1)}, c_{\sigma^{-1}(2)}, \ldots, c_{\sigma^{-1}(n)}\right) \\
&= \left(b_{\sigma^{-1}(1)} + c_{\sigma^{-1}(1)}, b_{\sigma^{-1}(2)} + c_{\sigma^{-1}(2)}, \ldots, b_{\sigma^{-1}(n)} + c_{\sigma^{-1}(n)}\right) \\
&= \sigma\left((b_1 + c_1, b_2 + c_2, \ldots, b_n + c_n)\right) \\
&= \sigma(b + c)
\end{aligned}$$

We have proved that σ is a weight-preserving linear bijection. A theorem of MacWilliams [23] (see also [18] or [24]) tells us that in fact every weight-preserving linear bijection between binary codes (a binary code is an $\mathbb{F}_2$ vector space) is a permutation. Before we state the theorem in general, we need a definition. Let $\mathbb{F}_q$ be a finite field and let $n \in \mathbb{N}$. Let $V, W < \mathbb{F}_q^n$ be subspaces, and let $\phi : V \to W$ be an $\mathbb{F}_q$-linear map. We say that ϕ is a *monomial equivalence* if it is a permutation followed by a nonzero scaling of each entry. Formally, ϕ is a monomial equivalence if there are $\lambda_1, \lambda_2, \ldots, \lambda_n \in \mathbb{F}_q^\times = \mathbb{F}_q \setminus \{\vec{0}\}$ and a permutation $\sigma : [n] \to [n]$ such that for all $v = (v_1, v_2, \ldots, v_n) \in V$, we have $\phi(v) = \left(\lambda_1 v_{\sigma^{-1}(1)}, \lambda_2 v_{\sigma^{-1}(2)}, \ldots, \lambda_n v_{\sigma^{-1}(n)}\right)$. Notice that in the case $q = 2$, a monomial equivalence is a permutation. We are now ready for the theorem.

Theorem 4.1.2 (The MacWilliams Extension Theorem)**.** *Let $\mathbb{F}_q$ be a finite field. Let $V, W < \mathbb{F}_q^n$ be subspaces. If $\phi : V \to W$ is a weight preserving linear map then ϕ is a monomial equivalence.*

This is called an extension theorem because it tells us that any weight preserving homomorphism $\phi : V \to W$ can be extended to a weight preserving automorphism of $\mathbb{F}_q^n$. We give a new proof of the MacWilliams Extension Theorem in Section 4.5.3.

We may now start to look at our main problem.

4.2 Constant Weight Codes

Let $\mathcal{C} < \mathbb{F}_2^n$ have dimension k. $\mathcal{C}$ has 2^k vectors, one of which is $\vec{0}$. Thus, if w is not zero then $A_w(\mathcal{C}) \leq 2^k - 1$. Hence, for $w \neq 0$, we have

$$m(n,k,w) \leq 2^k - 1.$$

To discuss our main problem, it is important to find the parameters for which $m(n,k,w) = 2^k - 1$. We want to find those parameters n, k, and w for which there exists a k-dimensional subspace $\mathcal{C} < \mathbb{F}_2^n$ with $A_w(\mathcal{C}) = 2^k - 1$. We call such a subspace a *constant weight code of weight* w. In [3], Ahlswede, Aydinian, and Khachatrian mention the following characterization of the parameters for which a constant weight code exists.

Proposition 4.2.1. *There exists a k-dimensional constant weight code $\mathcal{C} < \mathbb{F}_2^n$ with nonzero weight w if and only if there is some $t \in \mathbb{N}$ for which $w = t2^{k-1}$ and $n \geq t(2^k - 1) = 2w - t$.*

Restated, there exists a k-dimensional constant weight code $\mathcal{C} < \mathbb{F}_2^n$ of weight w in $\mathbb{F}_2^n$ if and only if 2^{k-1} divides w and $n \geq 2w - w/2^{k-1}$. Before we prove this result, we first introduce some special constant weight codes, which we then use to find *all* constant weight codes. Let M_k be a $k \times (2^k - 1)$ matrix whose columns are the vectors of $\mathbb{F}_2^k \setminus \{\vec{0}\}$. For the sake of definiteness we order the columns in decreasing order from left to right according to their values as binary numbers. We give M_3 as an example.

$$M_3 = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

Define $\mathcal{S}_k$ to be the row space of M_k. This space is known as the *k-dimensional binary simplex code* (see [18] for example). We now prove the well-known fact (see [18]) that every non-zero vector of $\mathcal{S}_k$ has the same weight.

Proposition 4.2.2. *For all $s \in \mathcal{S}_k \setminus \{\vec{0}\}$, we have*

$$\mathrm{wt}(s) = 2^{k-1}.$$

Proof of Proposition 4.2.2. We proceed by induction on k. In the case $k = 1$ we have that $M_1 = [1]$, and so $\mathcal{S}_k = \{0, 1\}$, every nonzero vector of which has weight $1 = 2^{1-1}$. Notice that for $k > 1$, we have

$$M_k = \left[\begin{array}{c|c|c} 1\,1\,1\,1 \cdots 1\,1\,1\,1 & 1 & 0\,0\,0\,0 \cdots 0\,0\,0\,0 \\ \hline & 0 & \\ & 0 & \\ M_{k-1} & \vdots & M_{k-1} \\ & 0 & \\ & 0 & \end{array}\right].$$

Let the rows of this matrix be labeled $R_1, R_2, \ldots, R_k$, from top to bottom. We first consider $s \in \operatorname{span}\{R_2, R_3, \ldots, R_k\} \setminus \{\vec{0}\}$. We have $s = s'0s'$ for some $s' \in \mathcal{S}_{k-1} \setminus \{\vec{0}\}$. That is, s is the concatenation of s', 0, and s'. By induction,

$$\mathrm{wt}(s) = 2\,\mathrm{wt}(s') = 2 \times 2^{k-2} = 2^{k-1}.$$

Now let $s \in \operatorname{span}\{R_1, R_2, \ldots, R_k\} \setminus \operatorname{span}\{R_2, R_3, \ldots, R_k\}$. Then $s = R_1 + s'0s'$

for some $s' \in \mathcal{S}_{k-1}$. Thus $s = \overline{s'0}s'$, and we have

$$
\begin{aligned}
\mathrm{wt}(s) &= \mathrm{wt}(\overline{s'0}s') \\
&= \mathrm{wt}(\overline{s'0}) + \mathrm{wt}(s') \\
&= \mathrm{wt}(R_1) - \mathrm{wt}(s'0) + \mathrm{wt}(s') \\
&= \mathrm{wt}(R_1) - \mathrm{wt}(s') + \mathrm{wt}(s') \\
&= \mathrm{wt}(R_1) \\
&= 2^{k-1}.
\end{aligned}
$$

□

We are almost ready to prove Proposition 4.2.1, which characterizes the parameters n, k and w for which $m(n,k,w) = 2^k - 1$. First, we need a definition. Given $n, k, t \in \mathbb{N}$ with $n \geq t(2^k - 1)$, we construct the matrix

$$
\begin{array}{c}
\longleftarrow \quad t \text{ times} \quad \longrightarrow \;\; \longleftarrow n - t(2^k-1) \text{ times} \longrightarrow \\
\left[\begin{array}{c|c|c|c|c} M_k & M_k & \cdots & M_k & \vec{0}_k^T\vec{0}_k^T\vec{0}_k^T\vec{0}_k^T \cdots \vec{0}_k^T\vec{0}_k^T\vec{0}_k^T\vec{0}_k^T \end{array}\right].
\end{array}
$$

Define $\mathcal{S}(k,t,n)$ to be the row span of this matrix.

Proof of Proposition 4.2.1. We prove the reverse direction first. Suppose that there is $t \in \mathbb{N}$ such that $w = t2^{k-1}$ and $n \geq t(2^k - 1)$. We need to show that there is a k-dimensional constant weight code $\mathcal{C} < \mathbb{F}_2^n$ with nonzero weight w. Our candidate is $\mathcal{S}(k,t,n)$. Clearly $\mathcal{S}(k,t,n)$ has dimension k. By Proposition 4.2.2, every vector in $\mathcal{S}(k,t,n) \setminus \{\vec{0}\}$ has weight $t2^{k-1} = w$. Finally, $\mathcal{S}(k,t,n)$ has length $t(2^k - 1) + (n - t(2^k - 1)) = n$.

For the other direction, we are given that there exists a k-dimensional constant weight code $\mathcal{C} < \mathbb{F}_2^n$ with $A_w(\mathcal{C}) = 2^k - 1$, and we need to show that 2^{k-1} divides w and $n \geq 2w - w/2^{k-1}$. We will proceed by induction on k. For $k = 0$, we are to show that there is an integer t for which $\frac{1}{2}t = w$ and that $n \geq 0$. These are clearly true. For $k = 1$, we have that $\mathcal{C}$ contains a weight w vector, and we want to show that 2^{1-1} divides w, and $n \geq 2w - w/2^{1-1}$. That is, we want to show that 1 divides w, and $n \geq w$. Clearly 1 divides w, and n must be at least w, since $\mathcal{C} < \mathbb{F}_2^n$ contains a weight w vector.

Now we consider $k > 1$. Without loss of generality, we may permute entries as discussed in Section 4.1.2. Thus we may assume that there exists $v_1 \in V \setminus \{\vec{0}\}$ of the form

$$v_1 = \underbrace{1 \ldots 1}_{R_1}\underbrace{0 \ldots 0}_{R_0}.$$

Here $R_b = \{i \in [n] : \pi_i(v_1) = b\}$, where $b \in \mathbb{F}_2$. Thus $|R_1| = w$. Let $v_2 \in V \setminus \{\vec{0}, v_1\}$. Since $v_1 \neq v_2$, we have $v_1 + v_2 \neq \vec{0}$. Thus $\mathrm{wt}(v_1 + v_2) = w$. Recall that given $I \subseteq [n]$, we define $\pi_I(v)$ to be the projection of v onto the coordinates I. We have

$$\begin{aligned} w &= \mathrm{wt}(v_1 + v_2) \\ &= |R_1| - \mathrm{wt}(\pi_{R_1}(v_2)) + \mathrm{wt}(\pi_{R_0}(v_2)) \\ &= w - \mathrm{wt}(\pi_{R_1}(v_2)) + \mathrm{wt}(\pi_{R_0}(v_2)). \end{aligned}$$

Thus $\mathrm{wt}(\pi_{R_1}(v_2)) = \mathrm{wt}(\pi_{R_0}(v_2))$. We also have $\mathrm{wt}(\pi_{R_1}(v_2)) + \mathrm{wt}(\pi_{R_0}(v_2)) = \mathrm{wt}(v_2) = w$. Thus $\mathrm{wt}(\pi_{R_1}(v_2)) = \mathrm{wt}(\pi_{R_0}(v_2)) = w/2$. Set

$$W = \pi_{R_0}(V).$$

Given $v \in V$, we have

$$\mathrm{wt}(\pi_{R_0}(v)) = \begin{cases} 0 & \text{if } v \in \{\vec{0}, v_1\}; \\ w/2 & \text{if } v \in V \setminus \{\vec{0}, v_1\}. \end{cases}$$

Thus $\ker \pi_{R_0} = \{0, v_1\}$, which has dimension 1. Since $k = \dim \ker \pi_{R_0} + \dim W$, we have that $\dim W = k - 1$. Furthermore, W is a constant weight code of weight $w/2$. By induction, $w/2 = t2^{k-2}$ for some $t \in \mathbb{N}$. Hence $w = t2^{k-1}$. Also by induction, the length of W (which equals $|R_0|$) is at least $2(w/2)-t$. Thus $n \geq w+2(w/2)-t = 2w-t$, as desired.

□

Suppose that $m(n, k, w) = 2^k - 1$. We will see that the extremal subspace is unique up to permutation of entries. That is, up to permutation of entries, there is a unique k-dimensional subspace $V < \mathbb{F}_2^n$ with $A_w(V) = 2^k - 1$. This is a corollary of the MacWilliams Extension Theorem (Theorem 4.1.2). It is a special case of a theorem of Bonisoli [12].

Corollary 4.2.3 (Corollary of the MacWilliams Extension Theorem)**.** *Suppose*

$$m(n, k, w) = 2^k - 1$$

and $V < \mathbb{F}_2^n$ *is a* k*-dimensional subspace with* $A_w(V) = 2^{k-1}$*. If we set* $t = w/2^{k-1}$ *then up to monomial equivalence, we have*

$$V = \mathcal{S}(k, t, n).$$

Proof. Since any two codes of dimension k over $\mathbb{F}_2$ have a linear bijection between them, there is such a map $\phi : V \to \mathcal{S}(k, t, n)$. The weight of any nonzero vector of

V is w, as is the weight of any nonzero vector of $\mathcal{S}(k,t,n)$. Thus ϕ preserves weight. By the MacWilliams Extension Theorem, ϕ is a monomial equivalence. $\square$

4.3 The Case Where w is Odd and $m(n,k,w) = 2^{k-1}$

Let $\mathcal{C} < \mathbb{F}_2^n$. The map $p : \mathcal{C} \to \mathbb{F}_2$ defined by

$$p(c) = \sum_{i=1}^{n} \pi_i(c)$$

is the function which takes a vector c to the parity of its weight. Notice that p is a group homomorphism. Thus $p^{-1}(1)$ is either empty or a coset of $p^{-1}(0)$. In particular, $|p^{-1}(0)|$ is either $|\mathcal{C}|$ or $|\mathcal{C}|/2$. Thus if w is odd, we have $A_w(\mathcal{C}) \leq |p^{-1}(1)| \leq |\mathcal{C}|/2$. Therefore, if w is odd the natural first thing to determine is the parameters for which $m(n,k,w) = 2^{k-1}$. The following proposition from [3] gives those parameters.

Proposition 4.3.1. *Let w be odd and let $k \geq 1$. There is a k-dimensional subspace $V < \mathbb{F}_2^n$ with $A_w(V) = 2^{k-1}$ if and only if $k \leq w+1$ and $n \geq w+k-1$.*

Proof. For the forward direction, suppose that w is odd, $k \geq 1$, and that there exists a k-dimensional subspace $V < \mathbb{F}_2^n$ with $A_w(V) = 2^{k-1}$. If $k = 1$, then certainly $k \leq w+1$, and $n \geq w = w+1-1 = w+k-1$.

Suppose $k > 1$. Since $2^{k-1} > 0$, there is at least one vector of weight w. Permuting entries, we may assume without loss of generality that there is a vector $v \in V$ of the form

$$v = \underbrace{1\ldots1}_{R_1}\underbrace{0\ldots0}_{R_0},$$

where $|R_1| = w$. Now consider $\mathcal{E} < V$, the subspace of even weight vectors. Notice that because there is an odd weight vector, we have $\dim \mathcal{E} = k-1$. Let $e \in \mathcal{E}$. Consider $\mathrm{wt}(\pi_{R_1}(e))$, the number of 1's in the first w coordinates of e. Note that $e+v$

has weight w because $e+v$ has odd weight and all odd weight vectors have weight w. Thus by an argument similar to the one from Proposition 4.2.1, the function $\pi_{R_1} : \mathcal{E} \to \mathbb{F}_2^w$ has the property that

$$\mathrm{wt}(\pi_{R_1}(e)) = \begin{cases} 0 & \text{if } e = \vec{0}; \\ w/2 & \text{if } e \neq \vec{0}. \end{cases}$$

Thus $\ker \pi_{R_1} = \{\vec{0}\}$. Hence, π_{R_1} is injective as a function of $\mathcal{E}$. In particular, $\dim \pi_{R_1}(\mathcal{E}) = \dim \mathcal{E} = k-1$. Since $|R_1| = w$, this gives us that $k-1 \leq w$ and hence,

$$k \leq w+1,$$

as desired.

By a similar argument, $\pi_{R_0}(\mathcal{E})$ has dimension $k-1$. Thus

$$\begin{aligned} n &\geq |\mathrm{supp}(\pi_{R_1}(V))| + |\mathrm{supp}(\pi_{R_0}(V))| \\ &\geq w + |\mathrm{supp}(\pi_{R_0}(\mathcal{E}))| \\ &\geq w + k - 1. \end{aligned}$$

For the reverse direction, suppose w is odd, $1 \leq k \leq w+1$, and $n \geq w+k-1$. We want to show that there is $V < \mathbb{F}_2^n$ of dimension k with $A_w(V) = 2^{k-1}$. We essentially follow the model established above. First, set

$$v = \underbrace{1\ldots1}_{w}\underbrace{0\ldots0}_{n-w},$$

then set

$$\mathcal{E} = \{u\underbrace{00\ldots00}_{w+1-k}u\underbrace{00\ldots00}_{n-w-k+1} : u \in \mathbb{F}_2^{k-1}\},$$

and finally let

$$V = \mathcal{E} + v.$$

Every odd weight vector in V has the form

$$x = \underbrace{\overline{u00\ldots00}}_{w}u00\ldots00,$$

but

$$w(x) = w - \mathrm{wt}(u) + \mathrm{wt}(u) = w.$$

□

4.4 A Bound on $m(n, k, w)$

Let $f_2(w)$ denote the largest integer e such that 2^e divides w. In this section we establish that

$$m(n, k, w) \leq 2^k - 2^{k-f_2(w)-1}. \tag{4.4.1}$$

We also characterize the parameters n, k, and w for which the bound is met. This will show that among all upper bounds on $m(n, k, w)$ that are functions of only k and $f_2(w)$, (4.4.1) is the best possible. Propositions 4.2.1 and 4.3.1 are special cases of this characterization. The bound will be established by proving that if you throw out sufficiently few nonzero vectors from a subspace $V < \mathbb{F}_2^n$, then you can find a large subspace inside of what remains. In particular, if there are few non-weight-w vectors in V, then V contains a large constant weight code. By Proposition 4.2.1, this implies that w is divisible by a large power of two. We now make this argument precise.

Lemma 4.4.1. *Let V be an $\mathbb{F}_2$-vector space of dimension $k \geq 1$. Let $S \subseteq V \setminus \{\vec{0}\}$. If $b > 1$ and $|S| < |V|/2^{b-1} - 1$ then $V \setminus S$ contains a subspace, W, of dimension b.*

Proof. We establish the claim by induction on b. If $b = 1$ the claim says that if $\vec{0} \notin S$, and $|S| \leq |V| - 2$, then $V \setminus S$ contains a subspace of dimension 1. This is true, since $V \setminus S$ contains at least two vectors, one of which is $\vec{0}$.

Now suppose $b > 1$. Let $S \subseteq V \setminus \{\vec{0}\}$ with $|S| < |V|/2^{b-1} - 1$. Then $|S| < |V|/2^{(b-1)-1} - 1$. By induction, $V \setminus S$ contains a subspace, W', of dimension $b - 1$. Consider all extensions of W' to a b-dimensional subspace of V. If one of these extensions does not contain an element of S, we are done. Suppose for the sake of contradiction that every extension contains an element of S. There are a total of $\left(|V| - 2^{b-1}\right)/2^{b-1} = |V|/2^{b-1} - 1$ extensions. Notice that if E_1 and E_2 are two distinct b-dimensional extensions of W', then $E_1 \cap E_2 = W'$. That is, $(E_1 \setminus V')$ is disjoint from $(E_2 \setminus V')$. Thus $|S|$ is at least as large as the number of extensions. That is $|S| \geq |V|/2^{b-1} - 1$. This is a contradiction. $\square$

Proposition 4.4.2. $m(n, k, w) \leq 2^k - 2^{(k-1)-f_2(w)}$.

Proof. Suppose not. Then there are three positive integers n,k, and w for which there is $V < \mathbb{F}_2^n$ of dimension k so that V has more than $2^k - 2^{(k-1)-f_2(w)}$ weight-w vectors. Let S be the set of non-zero, non-weight-w vectors in V. Let $b = f_2(w) + 2$. We have

$$\begin{aligned}
|S| &< (2^k - 1) - (2^k - 2^{(k-1)-f_2(w)}) \\
&= 2^{(k-1)-f_2(w)} - 1 \\
&= \frac{2^k}{2^{f_2(w)+1}} - 1 \\
&= \frac{|V|}{2^{b-1}} - 1.
\end{aligned}$$

By Lemma 4.4.1, there is a subspace $\mathcal{C} < V \setminus S$ with dimension b, all of whose nonzero vectors have weight w. Proposition 4.2.1 (the characterization of constant weight codes) implies that 2^{b-1} divides w. That is, $2^{f_2(w)+1}$ divides w. By the definition of $f_2(w)$, this is a contradiction. $\square$

One way to meet the bound in Proposition 4.4.2 would be to construct a space where the non-weight-w vectors form a subspace of dimension $k-1-f_2(w)$. We use the following lemma to characterize the parameters for which there is such a space.

Lemma 4.4.3. *There is a k-dimensional code $V < \mathbb{F}_2^n$ in which the non-weight-w vectors are contained in a subspace of dimension $l < k$ if and only if there is an integer $t \geq l$ such that $w = t2^{k-l-1}$ and $n \geq 2w - t + l$.*

Proof. Let $V < \mathbb{F}_2^n$ be a space for which the non-weight-w vectors are contained in a subspace of dimension $l < k$. We wish to show that there exists $t \geq l$ such that $w = t2^{k-l-1}$ and $n \geq 2w - t + l$. Let B be an l-dimensional subspace of V containing the non-weight-w vectors of V (the *bad* vectors of V). Let $\{b_1, b_2, \ldots, b_l\}$ be a basis for B. Given $s \in \mathbb{F}_2^l$, denote

$$R_s = \{i \in [n] \,:\, \pi_i(b_j) = \pi_j(s) \text{ for all } j \in [l]\}.$$

For example, if we take $l = 3$, with $b_1 = 1111110$, $b_2 = 1111000$, and $b_3 = 1111110$, then we have the following.

$$\begin{array}{rccccccc}
 & \multicolumn{4}{c}{\overbrace{\hphantom{1\quad 1\quad 1\quad 1}}^{R_{111}}} & \multicolumn{2}{c}{\overbrace{\hphantom{1\quad 1}}^{R_{101}}} & \overbrace{\hphantom{0}}^{R_{000}} \\
b_1 = & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\
b_2 = & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\
b_3 = & 1 & 1 & 1 & 1 & 1 & 1 & 0
\end{array}$$

Here $R_{111} = \{1,2,3,4\}$, $R_{101} = \{5,6\}$, and $R_{000} = \{7\}$. Also, $R_{001} = R_{010} = R_{011} = R_{100} = R_{110} = \emptyset$. Notice that for any $v \in \text{span}(B)$ and any $s \in \mathbb{F}_2^l$, $\pi_{R_s}(v)$ is either all 1's or all 0's.

Let $v \in \mathbb{F}_2^n$, and $c_1, c_2, \ldots, c_n \in \mathbb{N}$. Define $v(c_1, c_2, \ldots, c_n)$ to be the vector formed by repeating the i^{th} bit of v a total of c_i times, for $i = 1, 2, \ldots, n$. That is

$$v(c_1, c_2, \ldots, c_n) = \underbrace{\pi_1(v) \cdots \pi_1(v)}_{c_1 \text{ times}} \underbrace{\pi_2(v) \cdots \pi_2(v)}_{c_2 \text{ times}} \cdots \underbrace{\pi_n(v) \cdots \pi_n(v)}_{c_n \text{ times}}$$

For example

$$1010(4, 2, 3, 0) = 111100111.$$

We extend this definition to vector spaces: given $V < \mathbb{F}_2^n$, define

$$V(c_1, c_2, \ldots, c_n) = \{v(c_1, c_2, \ldots, c_n) \, : \, v \in V\}.$$

Recall that $\mathcal{S}_k$ is the binary simplex of dimension k. Define $\mathcal{S}_k^0 = \{s0 : s \in \mathcal{S}_k\}$. Then the space spanned by the vectors b_1, b_2, b_3 in the example above is equal to $\mathcal{S}_3^0(|R_{111}|, |R_{110}|, |R_{101}|, |R_{100}|, |R_{011}|, |R_{010}|, |R_{001}|, |R_{110}|)$. Let *any* B be given and define R_s as above. Up to permutation we have

$$B = \mathcal{S}_l^0(|R_{11\ldots11}|, |R_{11\ldots10}|, \ldots, |R_{00\ldots01}|, |R_{00\ldots00}|). \tag{4.4.2}$$

Let $r \in \mathbb{F}_2^l$. We claim that there is a weight $w_r \in \mathbb{N}$ such that for all $v \in V \setminus B$, we have $\mathrm{wt}(\pi_{R_r}(v)) = w_r$. Fix $v \in V \setminus B$. For all $r \in \mathbb{F}_2^l$, define $w'_r = \mathrm{wt}(\pi_{R_r}(v))$. We wish to show that w'_r is independent of our choice of v. If $b \in B$ then $v + b \notin B$. Thus $\mathrm{wt}(v + b) = w$. Therefore

$$w = \sum_{\substack{r \in \mathbb{F}_2^l \\ \pi_{R_r}(b) = \vec{0}}} w'_r + \sum_{\substack{r \in \mathbb{F}_2^l \\ \pi_{R_r}(b) = \vec{1}}} (|R_r| - w'_t). \tag{4.4.3}$$

If we consider each w'_t to be a variable then (4.4.3) is a real equation with 2^l variables.

This equation is true for any $b \in B$. Since $|B| = 2^l$, we have a system of 2^l equations, with 2^l unknowns. By (4.4.2), the coefficients in this system of equations are related to the elements of $\mathcal{S}_l^0$. In particular, define $\sigma : \mathbb{F}_2^l \to \mathbb{R}^l$ by

$$\pi_i\left(\sigma\left(r\right)\right) = \begin{cases} 1 & \text{if } \pi_i\left(r\right) = 0; \\ -1 & \text{if } \pi_i\left(r\right) = 1. \end{cases}$$

If we denote

$$\vec{w} = (w'_{11\ldots11}, w'_{11\ldots01}, \ldots, w'_{00\ldots01}, w'_{00\ldots00})$$

then we have the system of equations

$$\left\{ \sigma(s) \cdot \vec{w} = w - \sum_{\substack{r \in \mathbb{F}_2^l \\ \pi_{R_r}(s) = \vec{1}}} |R_r| \ : \ s \in \mathcal{S}_l^0 \right\}. \tag{4.4.4}$$

For example, if $l = 2$, we have the following system of equations.

$$\begin{bmatrix} -1 & -1 & 1 & 1 \\ -1 & 1 & -1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} w'_{11} \\ w'_{10} \\ w'_{01} \\ w'_{00} \end{bmatrix} = \begin{bmatrix} w - R_{11} - R_{10} \\ w - R_{11} - R_{01} \\ w - R_{10} - R_{01} \\ w \end{bmatrix}.$$

Let A be the coefficient matrix for system (4.4.4). We now prove that A is invertible. Given two vectors $u = (u_1, u_2, \ldots, u_n)$ and $v = (v_1, v_2, \ldots, v_n) \in \mathbb{R}^n$, define $u * v$ to be the componentwise product. That is,

$$u * v = (u_1 v_1, u_2 v_2, \ldots, u_n v_n).$$

Then σ is a homomorphism. That is, given $a, b \in \mathrm{cs}_l^0$, we have

$$\sigma(a+b) = \sigma(a) * \sigma(b).$$

Let u and v be distinct rows of A. We have $u = \sigma(a)$ and $v = \sigma(b)$ where a and b are distinct elements of S_l^0. But then

$$\begin{aligned} u \cdot v &= \sum_{i=1}^{2^l} \pi_i\left(u * v\right) \\ &= \sum_{i=1}^{2^l} \pi_i\left(\sigma(a+b)\right) \\ &= 0. \end{aligned}$$

The last equality is true because $a + b \in \mathcal{S}_l^0 \setminus \{\vec{0}\}$, every element of which has 2^{l-1} ones and 2^{l-1} zeroes. Furthermore, $u \cdot u = 2^l$ for all rows u of A. Thus $AA^T = 2^l I_n$, so A is invertible. In fact, A is a Hadamard matrix (see [13],[24], or [29] for more about Hadamard matrices). Thus w_s' is independent of our choice of v, as desired.

Let $s \in \mathbb{F}_2^l$ be such that $|R_s| \neq 0$. We aim to show that 2^{k-l-1} divides w_s. We'll first consider the case $s \neq \vec{0}$. Pick $b \in B$ with $\pi_{R_s}(b) = \vec{1}$, and let $v \in V \setminus B$. Then

$$\pi_{R_s}(v) \neq \vec{0}, \tag{4.4.5}$$

since otherwise $\pi_{R_s}(b+v) = \vec{1}$, contradicting $\mathrm{wt}(\pi_{R_s}(v)) = w_s = \mathrm{wt}(\pi_{R_s}(b+v))$. In particular, (4.4.5) tells us that $\dim\ker \pi_{R_s}|_V$ (the dimension of the kernel of π_{R_s} as a function of V) is equal to $\dim\ker \pi_{R_s}|_B$ (the dimension of the kernel of π_{R_s} as a function of B). But $\pi_{R_s}(B) = \{\vec{0}, \vec{1}\}$. Therefore $\ker \pi_{R_s}|_B$ contains $|B|/2$ vectors, and consists of the vectors of B that are zero on R_s. Thus $\dim\ker \pi_{R_s}|_B = l-1$, and therefore $\pi_{R_s}(V)$ has dimension $k - \ker \pi_{R_s}|_V = k - l + 1$. The set of vectors in $\pi_{R_s}(V)$

whose weight is not w_s is $\{\vec{0}, \vec{1}\}$. Therefore $\pi_{R_s}(V)$ contains a $(k-l)$-dimensional space that does not contain $\vec{1}$. This is a constant weight code of weight w_s. By Proposition 4.2.1 (the characterization of constant weight codes), 2^{k-l-1} divides w_s, as desired.

Now consider $s = \vec{0}$. Either w_s is 0 or it is not. If it is 0, then 2^{k-l-1} divides w_s, and we're done. If $w_s \neq 0$ then there is no v in $V \setminus B$ such thatS $\pi_{R_s}(v) = \vec{0}$. Thus, $\ker \pi_{R_s} = B$, which has dimension l. Therefore, $\pi_{R_s}(V)$ is a constant weight code of dimension $k-l$. By Proposition 4.2.1, 2^{k-l-1} divides w_s.

We have

$$w = \sum_{s \in \mathbb{F}_2^l} w_s, \tag{4.4.6}$$

so $w = t2^{k-l-1}$ for some $t \in \mathbb{N}$, as desired.

Now we argue that $t \geq l$. If $s \in \mathbb{F}_2^l \setminus \{\vec{0}\}$ and $|R_s| \neq 0$ then by equation (4.4.5) we have $w_s \neq 0$. By equation (4.4.6), we have

$$t \geq \left| \left\{ s \in \mathbb{F}_2^l \setminus \{\vec{0}\} \,:\, |R_s| \neq 0 \right\} \right|.$$

But for any $s \in {\mathbb{F}_2}^l$ and $b \in B$, we have that $\pi_{R_s}(b)$ is either $\vec{0}$ or $\vec{1}$. Since $\dim B = l$, at least l of the regions R_s must have $|R_s| \neq 0$.

Finally, we establish the bound on n. Let $s \in \mathbb{F}_2^l \setminus \{\vec{0}\}$ with $|R_s| \neq 0$. Let $v \in V \setminus B$

and $b \in B$ such that $\pi_{R_s}(b) = \vec{1}$. Since $v + b \in V \setminus B$, we have

$$\begin{aligned}
|R_s| &= |R_s| - w_s + w_s \\
&= |R_s| - \mathrm{wt}(\pi_{R_s}(v)) + w_s \\
&= \mathrm{wt}(\pi_{R_s}(v+b)) + w_s \\
&= w_s + w_s \\
&= 2w_s.
\end{aligned}$$

Now, $w_{\vec{0}} = t_{\vec{0}} 2^{k-l-1}$ for some $t_{\vec{0}} \in \mathbb{N}$. By the characterization of constant weight codes, $|R_{\vec{0}}| \geq 2w_{\vec{0}} - t_{\vec{0}}$. Thus

$$\begin{aligned}
n &= \sum_{s \in \mathbb{F}_2^l} |R_s| \\
&= \sum_{s \neq \vec{0}} 2w_s + |R_{\vec{0}}| \\
&\geq \sum_{s \neq \vec{0}} 2w_s + 2w_{\vec{0}} - t_{\vec{0}} \\
&= 2w - t_{\vec{0}} \\
&\geq 2w - (t - l).
\end{aligned}$$

The last inequality holds since, as we showed above, at least l of the t multiples of 2^{k-l-1} comprising w come from an R_s with $s \neq \vec{0}$.

Now we show the other direction. That is, suppose there is $t \geq l$ such that $w = t2^{k-l-1}$ and $n \geq 2w - t + l$. We want to show that there is a vector space $V < \mathbb{F}_2^n$ such that the span of the non-weight-w vectors has dimension $\leq l$. Consider the vector space V whose generator matrix is given below.

$$
\begin{array}{c}
\begin{bmatrix}
11\cdots1 & & & & & & & & & \\
 & 11\cdots1 & & & & & & & & \\
 & & \ddots & & & & & & & \\
 & & & 11\cdots1 & & & & & & \\
M_{k-l}\,0 & M_{k-l}\,0 & \cdots & M_{k-l}\,0 & M_{k-l} & M_{k-l} & \cdots & M_{k-l} & \vec{0}^T_{k-l}\vec{0}^T_{k-l}\cdots\vec{0}^T_{k-l}\vec{0}^T_{k-l}
\end{bmatrix} \\
\leftarrow \quad l \text{ blocks} \quad \rightarrow \quad \leftarrow \ t-l \text{ blocks } \rightarrow \quad \leftarrow n-(2w-t+l) \rightarrow
\end{array}
$$

The length of this matrix is

$$
\begin{aligned}
l2^{k-l} + (t-l)(2^{k-l}-1) + n - (2w-t+l) &= t2^{k-l} - (t-l) + n - (2w-t+l) \\
&= (2w-t+l) + n - (2w-t+l) \\
&= n.
\end{aligned}
$$

The dimension of V is $l + (k-l) = k$. Suppose $v \in V$ is the sum of a subset of the rows of the matrix above, at least one of which is is among the bottom $k-l$ rows. There is $s \in \mathcal{S}_k \setminus \{\vec{0}\}$ such that v is of the form

$$v = \overline{s0s0\ldots s0s0}s0s0\ldots s0s0ss\ldots ss00\ldots 00.$$

But $\mathrm{wt}(s) = 2^{k-l-1}$, and $\mathrm{wt}(\overline{s0}) = 2^{k-l-1}$, so the total weight of v is

$$\mathrm{wt}(v) = (l + (t-l))2^{k-l-1} = w.$$

Thus all non-weight-w vectors are in the span of the first l rows, and we have found the desired vector space. $\square$

Given $n, k, w \in \mathbb{N}$, and a k-dimensional code $V < \mathbb{F}_2^n$ with $A_w(V) = m(n,k,w)$, Lemma 4.4.2 implies that the rank of the non-weight-w vectors of V is at least $(k-1) - f_2(w)$. If the rank is $(k-1) - f_2(w)$ then by the previous lemma, $w = t2^{k-[(k-1)-f_2(w)]-1} = t2^{f_2(w)}$, where $t \geq (k-1) - f_2(w)$, and $n \geq 2w - t + (k-1) - f_2(w)$. These restrictions turn out to characterize the integers $n, k, w \in \mathbb{N}$ for which $m(n,k,w) = 2^k - 2^{(k-1)-f_2(w)}$.

Proposition 4.4.4. *$m(n,k,w) = 2^k - 2^{(k-1)-f_2(w)}$ if and only if $(k-1) - f_2(w) \geq 0$, $w = t2^{f_2(w)}$, where $t \geq (k-1) - f_2(w)$, and $n \geq 2w - t + (k-1) - f_2(w)$.*

Proof. Suppose $(k-1) - f_2(w) \geq 0$, $w = t2^{f_2(w)}$, where $t \geq (k-1) - f_2(w)$, and $n \geq 2w - t + (k-1) - f_2(w)$. Set $l = (k-1) - f_2(w)$. Then $t \geq l$, $w = t2^{k-l-1}$, and $n \geq 2w - t + l$. Thus by Lemma 4.4.3, there is a space $V < \mathbb{F}_2^n$ whose non-weight-w vectors have rank at most l. Thus $m(n,k,w) \geq 2^k - 2^l = 2^k - 2^{(k-1)-f_2(w)}$. By Lemma 4.4.2, we have $m(n,k,w) = 2^k - 2^{(k-1)-f_2(w)}$.

Now we prove the other direction. Suppose $m(n,k,w) = 2^k - 2^{(k-1)-f_2(w)}$. Since $m(n,k,w)$ is an integer, we have

$$(k-1) - f_2(w) \geq 0.$$

For some $t \in \mathbb{N}$, we have

$$w = t2^{f_2(w)}.$$

Let $V < \mathbb{F}_2^n$ be a k-dimensional code with $A_w(V) = 2^k - 2^{(k-1)-f_2(w)}$. Let S be the set of non-zero non-weight-w vectors in V. Notice that

$$|S| = 2^{(k-1)-f_2(w)} - 1 < 2^{k-f_2(w)} - 1 = \frac{2^k}{2^{(f_2(w)+1)-1}} - 1.$$

Thus by Lemma 4.4.1, there is a subspace $\mathcal{C} \subseteq V \setminus S$ of dimension $f_2(w) + 1$. This is a constant weight code whose nonzero vectors have weight w.

Choose $U < V$ to have $\dim U = k - f_2(w) - 1$ and $\mathcal{C} + U = V$. Let $u \in U \setminus \{\vec{0}\}$. Consider

$$\mathcal{C}_u = \mathcal{C} + \{\vec{0}, u\}.$$

By the characterization of constant weight codes, this code cannot be constant weight, since it has dimension $f_2(w) + 2$. This means that $\mathcal{C}_u$ has at least one nonzero non-weight-w vector. We now show that it cannot have two nonzero non-weight-w vectors. Let $T \subseteq \mathbb{F}_2^n$, and define $B_w(T)$ to be the number of non-weight-w vectors in T. Let $\mathcal{C} + u$ be the coset of $\mathcal{C}$ containing u. By our choice of U we have that for all u,$v \in U$ where $u \neq v$ it is the case that $(\mathcal{C} + v) \cap (\mathcal{C} + u) = \emptyset$. Thus,

$$B_w(V) = \sum_{u \in U} B_w(\mathcal{C} + u).$$

Thus, if some coset has more than one non-weight-w vector then

$$B_w(V) > |U| = 2^{(k-1)-f_2(w)},$$

a contradiction.

Now, we consider $\dim \pi_{R_{00\ldots0}(\mathcal{C})}(U)$, the dimension of the projection of U onto the zero-valued coordinates of $\mathcal{C}$. We claim that $\pi_{R_{00\ldots0}(\mathcal{C})}$ is injective on U. If not, then there is some $u \in U \setminus \{\vec{0}\}$ such that $\pi_{R_{00\ldots0}(\mathcal{C})}(u) = \vec{0}$. But consider $\mathcal{C}_u$. It contains one nonzero non-weight-w vector. Call this vector b. Then $\mathcal{C}_u = \mathcal{C}_b$. Recall that $\mathrm{supp}(b)$

is the set of coordinates where b is nonzero. Given any vector $c \in \mathcal{C}$, we have

$$\begin{aligned}
\operatorname{wt}(\pi_{\operatorname{supp}(b)}(c)) + \operatorname{wt}(\pi_{[n]\setminus\operatorname{supp}(b)}(c)) \\
&= \operatorname{wt}(c) \\
&= w \\
&= \operatorname{wt}(b+c) \\
&= \operatorname{wt}(b) - \operatorname{wt}(\pi_{\operatorname{supp}(b)}(c)) + \operatorname{wt}(\pi_{[n]\setminus\operatorname{supp}(b)}(c)).
\end{aligned}$$

Thus

$$\operatorname{wt}(\pi_{\operatorname{supp}(b)}(c)) = \frac{1}{2}\operatorname{wt}(b).$$

In particular, $\pi_{\operatorname{supp}(b)}(\mathcal{C})$ is a constant weight code of dimension $\dim \mathcal{C} = f_2(w) + 1$. By Corollary 4.2.3 we have that, up to permutation of entries,

$$\pi_{\operatorname{supp}(b)}(\mathcal{C}) = \mathcal{S}(f_2(w)+1, \frac{1}{2^{f_2(w)+1}}\operatorname{wt}(b), \operatorname{wt}(b)).$$

In particular, the number of zero coordinates of $\pi_{\operatorname{supp}(b)}(\mathcal{C})$ is

$$\operatorname{wt}(b) - \frac{1}{2^{f_2(w)+1}}\operatorname{wt}(b)(2^{f_2(w)+1} - 1) = \frac{\operatorname{wt}(b)}{2^{f_2(w)+1}}.$$

This is a contradiction, since by our choice of u, no element of $\mathcal{C}_u$ (including b) has support where $\mathcal{C}$ does not. We have established that $\pi_{R_{00\ldots0}(\mathcal{C})}$ is injective on U, and hence $\pi_{R_{00\ldots0}(\mathcal{C})}(U)$ has dimension equal to $\dim U = k - f_2(w) - 1$. Thus $\left|\operatorname{supp}(\pi_{R_{00\ldots0}(\mathcal{C})}(U))\right| \geq k - f_2(w) - 1$. By Proposition 4.2.1 (the characterization of constant weight codes), $\text{supp}(\mathcal{C}) = (2^{f_2(w)+1} - 1)w2^{-f_2(w)} = 2w - t$. Thus

$$\begin{aligned} n &\geq |\text{supp}(V)| \\ &= |\text{supp}(C)| + \left|\text{supp}(\pi_{R_{00\ldots0}(\mathcal{C})}(U))\right| \\ &\geq 2w - t + k - f_2(w) - 1. \end{aligned}$$

Now, suppose $T < \mathbb{F}_2^n$ has dimension l. Then T has some codeword of weight at least l. To see this, just consider that T is permutation equivalent to a code with a generator matrix of the form

$$\left[\begin{array}{c|c} I_l & A \end{array} \right],$$

where A is an $l \times (n-l)$ matrix. The sum of the first l rows has weight at least l.

In particular, $\pi_{R_{00\ldots0}(\mathcal{C})}(U)$ has a vector u' with $\text{wt}(u') \geq k - f_2(w) - 1$. Consider the corresponding vector, $u \in U$. Then $\mathcal{C} + u$ contains a non-zero, non-weight-w vector u.

We established above that the number of zero coordinates of $\pi_{\text{supp}(u)}(\mathcal{C})$ is

$$\text{wt}(u)2^{-f_2(w)-1}.$$

Therefore, by our choice of u, we have

$$\begin{aligned} \text{wt}(u)2^{-f_2(w)-1} &\geq wt(u') \\ &\geq k - f_2(w) - 1, \end{aligned}$$

and so

$$\text{wt}(u) \geq (k - f_2(w) - 1)2^{f_2(w)+1}.$$

Let $c \in \mathcal{C} \setminus \{\vec{0}\}$ and recall that above we established

$$\mathrm{wt}(\pi_{\mathrm{supp}(u)}(c)) = \frac{1}{2}\,\mathrm{wt}(u),$$

and so we have

$$\begin{aligned} t2^{f_2(w)} &= w, \\ &\geq \mathrm{wt}(\pi_{\mathrm{supp}(u)}(c)) \\ &= \frac{1}{2}\,\mathrm{wt}(u) \\ &\geq (k - f_2(w) - 1)2^{f_2(w)}. \end{aligned}$$

Therefore

$$t \geq k - f_2(w) - 1,$$

as desired. □

4.5 Killers

4.5.1 Introduction

To answer some questions about $m(n, k, w)$, one can study linear maps that decrease the weight of a nonzero vector by a fixed constant, c. We call such a map a *c-killer*. The problem of determining the structure of c-killers is interesting in its own right. In this section we give and prove a structure theorem for c-killers. We first prove it for $\mathbb{F}_2$ vector spaces. Using this proof as a model, we then prove it for general finite fields.

Our characterization is a generalization of Theorem 4.1.2, the MacWilliams Extension Theorem. That theorem characterizes weight-preserving linear maps (i.e. 0-killers). Though our proof uses the MacWilliams Extension Theorem, we are able to use the machinery of our proof to give a new elementary proof of the MacWilliams Extension Theorem.

We will use the c-killer characterization to classify the small set of parameters for which w is odd and $m(n,k,w) = 2^{k-1} - 1$.

4.5.2 Binary c-killers

Let $V, W < \mathbb{F}_2^n$ and let $c \in \mathbb{N}$. We say a linear map $\phi : V \to W$ is a *c-killer* if for all $v \in V \setminus \{\vec{0}\}$,

$$\mathrm{wt}(\phi(v)) = \mathrm{wt}(v) - c.$$

We have the following theorem.

Theorem 4.5.1. *Let $V, W < \mathbb{F}_2^n$. If $\phi : V \to W$ is a c-killer, then ϕ is a coordinate permutation followed by a coordinate projection.*

Before we prove the theorem, we need to establish some supporting facts. We use a formula for the size of the symmetric difference of a collection of sets. Let $S_1, S_2, \ldots, S_k$ be subsets of $[n]$. The *symmetric difference* of $S_1, S_2, \ldots, S_k$ is the set of elements of $[n]$ that occur in an odd number of S_i. We denote this

$$\bigoplus_{i\in[k]} S_i = \{i \in [n] \,:\, |\{j \in [k] \,:\, i \in S_j\}| \equiv 1 (\mathrm{mod}\ 2)\}\,.$$

Given $I \subseteq [k]$, denote

$$S(I) = \bigcap_{i\in I} S_i.$$

We have the following fact, which is roughly analogous to the principle of inclusion and exclusion.

Theorem 4.5.2.
$$\left|\bigoplus_{i\in[k]} S_i\right| = \sum_{\substack{I\subseteq[k]\\ I\neq\emptyset}} (-2)^{|I|-1}|S(I)|.$$

Proof. We'll prove the statement by induction. The case $k = 1$ is trivial.

Assume $k > 1$. Let $A, B \subseteq [n]$. Then $|A \oplus B|$ (the size of the symmetric difference of A and B) is $|A| + |B| - 2|A \cap B|$. In particular,

$$\begin{aligned}\left|\bigoplus_{i\in[k]} S_i\right| &= \left|\left(\bigoplus_{i\in[k-1]} S_i\right) \oplus S_k\right| \\ &= \left|\bigoplus_{i\in[k-1]} S_i\right| - 2\left|\left(\bigoplus_{i\in[k-1]} S_i\right) \cap S_k\right| + |S_k|. \end{aligned} \tag{4.5.1}$$

By induction,

$$\left|\bigoplus_{i\in[k-1]} S_i\right| = \sum_{\substack{I\subseteq[k-1]\\ I\neq\emptyset}} (-2)^{|I|-1}|S(I)| = \sum_{\substack{I\subseteq[k]\\ I\neq\emptyset\\ k\notin I}} (-2)^{|I|-1}|S(I)|.$$

Now we consider the second term in (4.5.1). Let $i \in [n]$. Define $S'_i = S_i \cap S_k$. Similarly, for $I \subseteq [n]$, $S'(I) = S(I) \cap S_k = S(I \cup \{k\})$. Then

$$\left(\bigoplus_{i\in[k-1]} S_i\right) \cap S_k = \bigoplus_{i\in[k-1]} S'_i.$$

Thus, by induction

$$
\begin{aligned}
-2\left|\left(\bigoplus_{i\in[k-1]} S_i\right)\cap S_k\right| &= -2\sum_{\substack{I\subseteq[k-1]\\ I\neq\emptyset}}(-2)^{|I|-1}|S'(I)| \\
&= \sum_{\substack{I\subseteq[k-1]\\ I\neq\emptyset}}(-2)^{|I|}|S'(I)| \\
&= \sum_{\substack{I\subseteq[k]\\ |I|\geq 2\\ k\in I}}(-2)^{|I|-1}|S(I)|.
\end{aligned}
$$

Putting this all together, expression (4.5.1) becomes

$$
\begin{aligned}
\left|\bigoplus_{i\in[k-1]} S_i\right| - 2\left|\left(\bigoplus_{i\in[k-1]} S_i\right)\cap S_k\right| + |S_k| &= \sum_{\substack{I\subseteq[k]\\ I\neq\emptyset\\ k\notin I}}(-2)^{|I|-1}|S(I)| \\
&\quad + \sum_{\substack{I\subseteq[k]\\ |I|\geq 2\\ k\in I}}(-2)^{|I|-1}|S(I)| \\
&\quad + |S_k| \\
&= \sum_{\substack{I\subseteq[k]\\ I\neq\emptyset}}(-2)^{|I|-1}|S(I)|.
\end{aligned}
$$

□

Let $S\subset\mathbb{F}_2^n$. We define $O(S)$ to be the size of the set of bit positions where all of the vectors of S overlap. More precisely,

$$O(S) = \left|\{i\in[n] \,:\, \pi_i\left(v\right) = 1\,\forall\, v\in S\}\right|.$$

As the next lemma shows, we can determine the effect of a c-killer on the sizes of overlaps.

Lemma 4.5.3. *Let $V, W < \mathbb{F}_2^n$ be subspaces. Let $\phi : V \to W$ be a c-killer. If B is a set of k linearly independent vectors from V then*

$$O(\phi(B)) = O(B) - c/2^{k-1}.$$

Proof. We proceed by induction on k. The case when $k = 1$ is clear by the definition of a c-killer.

Say $k > 1$. Let B be a set of k linearly independent vectors in $\mathbb{F}_2^n$. By noting that the sum of vectors in $\mathbb{F}_2^n$ corresponds to the symmetric difference of the associated sets, and by applying Lemma 4.5.2, we see that

$$\mathrm{wt}\left(\sum_{v\in B} v\right) = \sum_{\substack{I\subseteq B\\ I\neq\emptyset}} (-2)^{|I|-1} O(I) \tag{4.5.2}$$

and similarly

$$\mathrm{wt}\left(\sum_{v\in B} \phi(v)\right) = \sum_{\substack{I\subseteq B\\ I\neq\emptyset}} (-2)^{|I|-1} O(\phi(I)). \tag{4.5.3}$$

By induction,

$$
\begin{aligned}
\mathrm{wt}\left(\sum_{v\in B}\phi(v)\right) &= \sum_{\substack{I\subseteq B\\ I\neq\emptyset}}(-2)^{|I|-1}O(\phi(I))\\
&= (-2)^{|B|-1}O(\phi(B)) + \sum_{\substack{I\subseteq B\\ I\neq\emptyset,B}}(-2)^{|I|-1}O(\phi(I))\\
&= (-2)^{|B|-1}O(\phi(B)) + \sum_{\substack{I\subseteq B\\ I\neq\emptyset,B}}(-2)^{|I|-1}(O(I)-c/2^{|I|-1})\\
&= (-2)^{|B|-1}O(\phi(B)) + \sum_{\substack{I\subseteq B\\ I\neq\emptyset,B}}[(-2)^{|I|-1}O(I)+(-1)^{|I|}c]\\
&= (-2)^{|B|-1}O(\phi(B)) + c[(1-1)^{|B|}-1-(-1)^{|B|}]\\
&\qquad + \sum_{\substack{I\subseteq B\\ I\neq\emptyset,B}}(-2)^{|I|-1}O(I)\\
&= (-2)^{|B|-1}O(\phi(B)) + c[-1-(-1)^{|B|}]\\
&\qquad + \mathrm{wt}(\sum_{v\in B}v) - (-2)^{|B|-1}O(B).
\end{aligned}
$$

On the other hand,

$$
\mathrm{wt}\left(\sum_{v\in B}\phi(v)\right) = \mathrm{wt}(\phi(\sum_{v\in B}v)) = \mathrm{wt}(\sum_{v\in B}v) - c.
$$

Thus we have

$$
\begin{aligned}
\mathrm{wt}\left(\sum_{v\in B}v\right) - c &= (-2)^{|B|-1}O(\phi(B)) + c[-1-(-1)^{|B|}]\\
&\qquad + \mathrm{wt}(\sum_{v\in B}v) - (-2)^{|B|-1}O(B)
\end{aligned}
$$

therefore

$$-c = -(-2)^{|B|-1}O(\phi(B)) + c[-1 - (-1)^{|B|}] + (-2)^{|B|-1}O(B)$$

and so

$$(-2)^{|B|-1}O(B) = (-2)^{|B|-1}O(\phi(B)) - c(-1)^{|B|}.$$

Finally,

$$O(B) - c/2^{|B|-1} = O(\phi(B)).$$

□

Lemma 4.5.4. *Suppose $c > 1$ is an integer. If $\phi : V \to W$ is a c-killer then there is a constant weight code $\mathcal{C} < \mathbb{F}_2^{2c}$ of dimension $\dim V$, where the weight of a nonzero vector is c.*

Proof. Let B be a basis for V. By Lemma 4.5.3,

$$O(B) - c/2^{|B|-1} = O(\phi(B)).$$

In particular, $c/2^{|B|-1}$ is an integer. The lemma then follows from Proposition 4.2.1 (the characterization of constant weight codes). □

We are now ready to prove our characterization of c-killers.

Proof of Theorem 4.5.1. Let V,W be subspaces of $\mathbb{F}_2^n$, where $\dim V = k$, and suppose that $\phi : V \to W$ is a c-killer. If $c = 0$, then we are done by Theorem 4.1.2, the MacWilliams Extension Theorem. Thus we assume that $c \geq 1$.

By Lemma 4.5.4, there is a k-dimensional constant weight code, $\mathcal{C} < \mathbb{F}_2^{2c}$, whose nonzero weight is c. Since V and $\mathcal{C}$ are both k-dimensional vector spaces over $\mathbb{F}_2$, there is a linear bijection

$$\psi : V \to \mathcal{C}.$$

Define $W \times \mathcal{C} < \mathbb{F}_2^{n+2c}$ by

$$W \times \mathcal{C} = \{wv \,:\, w \in W, v \in \mathcal{C}\},$$

where wv is the vector formed by concatenating w and v. Consider $\phi \times \psi : V \to W \times \mathcal{C}$, defined by

$$(\phi \times \psi)(v) = \phi(v)\psi(v).$$

Notice that $\mathrm{wt}((\phi \times \psi)(\vec{0})) = 0 = \mathrm{wt}(\vec{0})$. Moreover, given $v \in V \setminus \{\vec{0}\}$, we have

$$\mathrm{wt}((\phi \times \psi)(v)) = \mathrm{wt}(\phi(v)) + \mathrm{wt}(\psi(v)) = wt(v) - c + c = wt(v).$$

Thus $\phi \times \psi$ preserves weight. By the MacWilliams Extension Theorem, $\phi \times \psi$ is a coordinate permutation. But

$$\phi = \pi_{[n]} \circ (\phi \times \psi).$$

Thus ϕ is a coordinate permutation followed by a coordinate projection. $\square$

4.5.3 General c-killers

We now prove the c-killer classification theorem for spaces over general finite fields. Let q be a prime power and define $\mathbb{F}_q$ to be the field with q elements. Let $n, c \in \mathbb{N}$ be positive integers and let $V, W < \mathbb{F}_q^n$. We say a linear map $\phi : V \to W$ is a *c-killer* if for all $v \in V \setminus \{\vec{0}\}$ we have

$$\mathrm{wt}(\phi(v)) = \mathrm{wt}(v) - c.$$

We have the following theorem.

Theorem 4.5.5. *Let $n, c \in \mathbb{N}$, and let $V, W < \mathbb{F}_q^n$ be subspaces. If $\phi : V \to W$ is a c-killer, then ϕ is a monomial equivalence followed by a coordinate projection.*

Recall that we introduced the concept of monomial equivalence in Section 4.1.2. The theorem above says that ϕ is equivalent to matrix multiplication by a square matrix, every row and column of which has at most 1 nonzero entry. The proof technique will be a more careful version of the proof for the binary case; by determining the (integer) size of a particular object, we will see that given a basis $\mathcal{B}$ of V, the expression $c\left((q-1)/q\right)^{|\mathcal{B}|-1}$ is an integer. In particular, c is divisible by $q^{|\mathcal{B}|-1}$. We will see that this implies that there is a $|\mathcal{B}|$-dimensional constant weight code of weight c. We then "stitch" this code onto W, making ϕ a 0-killer. We then apply the MacWilliams Extension Theorem to determine that this new map is a monomial equivalence. This implies that the original map has the desired structure.

We will define the analogue for the overlap sizes that appear in Lemma 4.5.2 (the symmetric difference formula). Given I, a multiset consisting of vectors from $\mathbb{F}_q^n$, we define the *common support* of I to be

$$\mathrm{cs}(I) = \{x \in [n] \,:\, \pi_x(v) \neq 0 \text{ for all } v \in I\}\,.$$

Given J, a multiset consisting of vectors from $\mathbb{F}_q^n$, we define the *zero sum set* of J to be

$$\mathrm{zs}(J) = \left\{x \in [n] \,:\, \pi_x\left(\sum_{v \in J} v\right) = 0\right\}.$$

Further, we define

$$O_J(I) \quad = \quad |\mathrm{cs}(I) \cap \mathrm{zs}(J)|$$

In words, $O_J(I)$ is the number of coordinates in the common support of I where the sum of the vectors in J is 0. In particular, if $S = \{s\}$ then $O_{\emptyset}(S) = \mathrm{wt}(s)$ and $O_S(S) = 0$.

Given $S \subseteq \mathbb{F}_q^n$, we may express the weight of the sum of the elements in S in terms of these $O_J(I)$. In order to facilitate the proof we introduce some notation. Given a multiset $S \subseteq \mathbb{F}_q^n$ and a coordinate $x \in [n]$, we define $\mathrm{nz}(x)$ to be the set of vectors in S which are nonzero at coordinate x. That is,

$$\mathrm{nz}(x) = \{s \in S \,:\, \pi_x(s) \neq 0\}.$$

Lemma 4.5.6. *Let S be a multiset of vectors in $\mathbb{F}_q^n$. Then*

$$\mathrm{wt}\left(\sum_{s \in S} s\right) = \sum_{\substack{I \subseteq S \\ I \neq \emptyset}} \sum_{J \subseteq I} (-1)^{|I|+|J|+1} O_J(I).$$

Proof. We have

$$\begin{aligned}
\sum_{\substack{I\subseteq S\\ I\neq\emptyset}}\sum_{J\subseteq I}(-1)^{|I|+|J|+1}O_J(I) &= \sum_{\substack{I\subseteq S\\ I\neq\emptyset}}\sum_{J\subseteq I}(-1)^{|I|+|J|+1}\sum_{\substack{x\in[n]\\ I\subseteq \mathrm{nz}(x)\\ x\in \mathrm{zs}(J)}} 1 \\
&= \sum_{\substack{I\subseteq S\\ I\neq\emptyset}}\sum_{J\subseteq I}\sum_{\substack{x\in[n]\\ I\subseteq \mathrm{nz}(x)\\ x\in \mathrm{zs}(J)}} (-1)^{|I|+|J|+1} \\
&= \sum_{x\in[n]}\sum_{\substack{J\subseteq \mathrm{nz}(x)\\ x\in \mathrm{zs}(J)}}\sum_{\substack{I\subseteq S\\ J\subseteq I\subseteq \mathrm{nz}(x)\\ I\neq\emptyset}} (-1)^{|I|+|J|+1}.
\end{aligned}$$

If $J \neq \mathrm{nz}(x)$, then the number of odd size subsets, I, with $J \subseteq I \subseteq \mathrm{nz}(x)$ is equal to the number of such subsets with even size. Thus, if $\mathrm{nz}(x) \neq \emptyset$ we have

$$\sum_{\substack{I\subseteq S\\ J\subseteq I\subseteq \mathrm{nz}(x)\\ I\neq\emptyset}} (-1)^{|I|+|J|+1} = \begin{cases} 1 & \text{if } J=\emptyset; \\ -1 & \text{if } J = \mathrm{nz}(x); \\ 0 & \text{otherwise.} \end{cases}$$

If $\mathrm{nz}(x) = \emptyset$, then

$$\sum_{\substack{I\subseteq S\\ J\subseteq I\subseteq \mathrm{nz}(x)\\ I\neq\emptyset}} (-1)^{|I|+|J|+1} = 0.$$

Thus

$$\sum_{x\in[n]}\sum_{\substack{J\subseteq \mathrm{nz}(x)\\ x\in \mathrm{zs}(J)}}\sum_{\substack{I\subseteq S\\ J\subseteq I\subseteq \mathrm{nz}(x)\\ I\neq\emptyset}} (-1)^{|I|+|J|+1} = \sum_{\substack{x\in[n]\\ \mathrm{nz}(x)\neq\emptyset}}\sum_{\substack{J\in\{\emptyset,\mathrm{nz}(x)\}\\ x\in \mathrm{zs}(J)}}\sum_{\substack{I\subseteq S\\ J\subseteq I\subseteq \mathrm{nz}(x)\\ I\neq\emptyset}} (-1)^{|I|+|J|+1}.$$

Notice, that the term corresponding to $J = \mathrm{nz}(x)$ is only added to this sum if

$x \in \mathrm{zs}(J)$. That is, only if $x \notin \mathrm{supp}(\sum_{s\in S} s)$. Now define

$$\chi(x) = \begin{cases} 1, & \text{if } x \in \mathrm{supp}\left(\sum_{s\in S} s\right); \\ 0, & \text{otherwise.} \end{cases}$$

Then we have

$$\begin{aligned} \sum_{\substack{I\subseteq S \\ I\neq\emptyset}} \sum_{J\subseteq I} (-1)^{|I|+|J|+1} O_J(I) &= \sum_{\substack{x\in[n] \\ \mathrm{nz}(x)\neq\emptyset}} (1-(1-\chi(x))) \\ &= \sum_{\substack{x\in[n] \\ \mathrm{nz}(x)\neq\emptyset}} \chi(x) \\ &= \sum_{x\in[n]} \chi(x) \\ &= \mathrm{wt}\left(\sum_{s\in S} s\right). \end{aligned}$$

□

We may now prove the following.

Lemma 4.5.7. *Let $c, n, q \in \mathbb{N}$, where q is a prime power, and let $V, W < \mathbb{F}_q^n$ be subspaces. If $S \subseteq V$ is linearly independent and $\phi : V \to W$ is a c-killer then*

$$\sum_{J\subseteq S} (-1)^{|J|} O_J(S) = \sum_{J\subseteq S} (-1)^{|J|} O_{\phi(J)}(\phi(S)) + c \tag{4.5.4}$$

Proof. We proceed by induction on $|S|$. We first consider $|S| = 1$. Suppose $S = \{s\}$, where $s \in V$. We want to verify that $O_\emptyset(S) - O_{\{s\}}(S) = O_\emptyset(\phi(S)) - O_{\{\phi(s)\}}(\phi(S)) + c$. Notice that $O_\emptyset(S) = \mathrm{wt}(s)$, $O_\emptyset(\phi(S)) = \mathrm{wt}(\phi(s))$, and $O_s(S) = O_{\phi(s)}(\phi(S)) = 0$. Thus, we are trying to show that $\mathrm{wt}(s) = \mathrm{wt}(\phi(s)) + c$, which is true by the definition of c-killer.

Now suppose $|S| > 1$ and assume that the lemma is true for all smaller linearly independent sets. Since S is linearly independent, we have $\sum_{s\in S} s \neq 0$ and so

$$\begin{aligned}
\mathrm{wt}\left(\sum_{s\in S} s\right) &= c + \mathrm{wt}\left(\phi\left(\sum_{s\in S} s\right)\right) \\
&= c + \mathrm{wt}\left(\sum_{s\in S} \phi\left(s\right)\right) \\
&= c + \sum_{\substack{I\subseteq S \\ I\neq\emptyset}} \sum_{J\subseteq I} (-1)^{|I|+|J|+1} O_{\phi(J)}(\phi(I)) \\
&= c + \sum_{J\subseteq S} (-1)^{|S|+|J|+1} O_{\phi(J)}(\phi(S)) \\
&\quad + \sum_{\substack{I\subseteq S \\ I\neq\emptyset \\ I\neq S}} \sum_{J\subseteq I} (-1)^{|I|+|J|+1} O_{\phi(J)}(\phi(I)) \\
&= c + \sum_{J\subseteq S} (-1)^{|S|+|J|+1} O_{\phi(J)}(\phi(S)) \\
&\quad + \sum_{\substack{I\subseteq S \\ I\neq\emptyset \\ I\neq S}} (-1)^{|I|+1} \sum_{J\subseteq I} (-1)^{|J|} O_{\phi(J)}(\phi(I)).
\end{aligned}$$

By induction, this is

$$
\begin{aligned}
&c + \sum_{J \subseteq S} (-1)^{|S|+|J|+1} O_{\phi(J)}(\phi(S)) \\
&\quad + \sum_{\substack{I \subseteq S \\ I \neq \emptyset \\ I \neq S}} (-1)^{|I|+1} \left[-c + \sum_{J \subseteq I} (-1)^{|J|} O_J(I) \right] \\
= {}& c + \sum_{J \subseteq S} (-1)^{|S|+|J|+1} O_{\phi(J)}(\phi(S)) \\
&\quad + \sum_{\substack{I \subseteq S \\ I \neq \emptyset \\ I \neq S}} (-1)^{|I|} c + \sum_{\substack{I \subseteq S \\ I \neq \emptyset \\ I \neq S}} \sum_{J \subseteq I} (-1)^{|J|+|I|+1} O_J(I) \\
= {}& c + \sum_{J \subseteq S} (-1)^{|S|+|J|+1} O_{\phi(J)}(\phi(S)) \\
&\quad + (-1)^{|S|+1} c - c + \mathrm{wt}\left(\sum_{s \in S} s \right) - \sum_{J \subseteq S} (-1)^{|S|+|J|+1} O_J(S).
\end{aligned}
$$

Therefore, by adding $\sum_{J \subseteq S} (-1)^{|S|+|J|+1} O_J(S) - \mathrm{wt}\left(\sum_{s \in S} s\right)$ to both sides and canceling the c's, we get

$$
\sum_{J \subseteq S} (-1)^{|S|+|J|+1} O_J(S) = \sum_{J \subseteq S} (-1)^{|S|+|J|+1} O_{\phi(J)}(\phi(S)) + (-1)^{|S|+1} c.
$$

Dividing by $(-1)^{|S|+1}$ we have

$$
\sum_{J \subseteq S} (-1)^{|J|} O_J(S) = \sum_{J \subseteq S} (-1)^{|J|} O_{\phi(J)}(\phi(S)) + c,
$$

as desired. $\square$

Notice that we may multiply the vectors in S by nonzero scalars to arrive at a different independent set in V. We may then apply Lemma 4.5.7 to this new independent set. In this way, the lemma gives us $(q-1)^{|S|}$ equations. As we will see, adding these equations together allows us to express $O_{\emptyset}(S)$ in terms of $O_{\emptyset}(\phi(S))$. In order to facilitate the discussion we introduce some notation. Let $S \subseteq \mathbb{F}_q^n$, and let $\alpha = (\alpha_v)_{v\in S} \in \left(\mathbb{F}_q^{\times}\right)^S$ (recall that $\mathbb{F}_q^{\times} = \mathbb{F}_q - \{0\}$, and $\left(\mathbb{F}_q^{\times}\right)^S$ is the set of functions from S to $\mathbb{F}_q^{\times}$). Given $J \subseteq S$, we define

$$\alpha J = \{\alpha_v v \,:\, v \in J\},$$

and

$$\alpha \cdot J = \sum_{v\in J} \alpha_v v.$$

We are now ready to prove the following lemma.

Lemma 4.5.8. *With the setup in Lemma 4.5.7, we have*

$$O_{\emptyset}(S) = O_{\emptyset}(\phi(S)) + c\left(\frac{q-1}{q}\right)^{|S|-1}.$$

Proof. Let $j = \{v_1, \ldots, v_j\} \subseteq S$. For a fixed $\alpha \in \left(\mathbb{F}_q^{\times}\right)^{j\setminus\{v_j\}}$, we have

$$\begin{aligned}\sum_{\alpha_{v_j}\in\mathbb{F}_q^{\times}} O_{(\alpha,\alpha_{v_j})J}(S) &= \sum_{\alpha_{v_j}\in\mathbb{F}_q^{\times}} \sum_{\substack{x\in\mathrm{cs}(S)\\ \pi_x\left((\alpha,\alpha_{v_j})\cdot J\right)=0}} 1\\ &= \sum_{x\in\mathrm{cs}(S)} \sum_{\substack{\alpha_{v_j}\in\mathbb{F}_q^{\times}\\ \pi_x\left((\alpha,\alpha_{v_j})\cdot J\right)=0}} 1.\end{aligned}$$

Notice that for x in the common support of S, $\pi_x(v_j) \neq 0$ and hence if $\pi_x(\alpha \cdot (J \setminus \{v_j\})) \neq 0$ then there is exactly one nonzero solution to

$$\pi_x\left((\alpha, \alpha_{v_j}) \cdot J\right) = 0.$$

Otherwise there is no nonzero solution. Thus

$$\begin{aligned}\sum_{\alpha_j \in \mathbb{F}_q^\times} O_{(\alpha,\alpha_j)J}(S) &= |\{x \in \mathrm{cs}(S) \,:\, \pi_x(\alpha \cdot (J \setminus \{v_j\})) \neq 0\}| \\ &= O_\emptyset(S) - O_{\alpha(J\setminus\{v_j\})}(S).\end{aligned}$$

Hence

$$\begin{aligned}\sum_{\beta \in (\mathbb{F}_q^\times)^J} O_{\beta J}(S) &= \sum_{\alpha \in (\mathbb{F}_q^\times)^{J\setminus\{v_j\}}} \sum_{\alpha_{v_j} \in \mathbb{F}_q^\times} O_{(\alpha,\alpha_{v_j})J}(S) \\ &= \sum_{\alpha \in (\mathbb{F}_q^\times)^{J\setminus\{v_j\}}} \left[O_\emptyset(S) - O_{\alpha(J\setminus\{v_j\})}(S)\right] \\ &= (q-1)^{j-1} O_\emptyset(S) - \sum_{\alpha \in (\mathbb{F}_q^\times)^{J\setminus\{v_j\}}} O_{\alpha(J\setminus\{v_j\})}(S).\end{aligned}$$

Notice that the rightmost sum is in exactly the same form as the leftmost sum. Thus, by induction, we have

$$\begin{aligned}\sum_{\alpha \in (\mathbb{F}_q^\times)^j} O_{\alpha J}(S) &= \sum_{i=2}^{|J|} (-1)^{|J|+i} (q-1)^{i-1} O_\emptyset(S) \\ &= \frac{(q-1)}{q}\left[(q-1)^{|J|-1} + (-1)^{|J|}\right] O_\emptyset(S).\end{aligned}$$

Summing the left hand side of equation 4.5.4 over all $\alpha \in (\mathbb{F}_q^\times)^S$, we have

$$
\begin{aligned}
&\sum_{\alpha\in(\mathbb{F}_q^\times)^S} \sum_{J\subseteq S} (-1)^{|J|} O_{\alpha J}(S) \\
&\qquad = \sum_{J\subseteq S} (-1)^{|J|} \sum_{\alpha\in(\mathbb{F}_q^\times)^S} O_{\alpha J}(S) \\
&\qquad = \sum_{J\subseteq S} (-1)^{|J|} \sum_{\beta\in(\mathbb{F}_q^\times)^{S\setminus J}} \sum_{\gamma\in(\mathbb{F}_q^\times)^J} O_{\gamma J}(S) \\
&\qquad = \sum_{J\subseteq S} (-1)^{|J|} (q-1)^{|S|-|J|} \frac{(q-1)}{q} \left[(q-1)^{|J|-1} + (-1)^{|J|}\right] O_\emptyset(S) \\
&\qquad = \frac{q-1}{q} O_\emptyset(S) \left[\sum_{J\subseteq S} (-1)^{|J|} (q-1)^{|S|-1} + \sum_{J\subseteq S} (q-1)^{|S|-|J|}\right] \\
&\qquad = \frac{q-1}{q} O_\emptyset(S) \left[0 + q^{|S|}\right] \\
&\qquad = (q-1) q^{|S|-1} O_\emptyset(S).
\end{aligned}
$$

Thus, summing equation (4.5.4) over all $\alpha \in (\mathbb{F}_q^\times)^{|S|}$, we get

$$
(q-1)q^{|S|-1} O_\emptyset(S) = (q-1)q^{|S|-1} O_\emptyset(\phi(S)) + (q-1)^{|S|} c
$$

and hence

$$
O_\emptyset(S) = O_\emptyset(\phi(S)) + c\left(\frac{q-1}{q}\right)^{|S|-1}.
$$

□

The lemma above establishes that if $\phi : V \to W$ is a c-killer and S is a basis for V then c is divisible by $q^{|S|-1}$. The following result of Bonisoli [12] implies the existence of an $|S|$-dimensional constant weight code of weight c.

Theorem 4.5.9. *There exists a k-dimensional subspace $\mathcal{C} < \mathbb{F}_q^n$, all of whose nonzero* *vectors have weight w, if and only if there exists $t \in \mathbb{N}$ such that*

$$w = tq^{k-1}$$

and

$$n \geq t\frac{q^k - 1}{q - 1}.$$

We may now prove the main theorem of this section, which characterizes c-killers.

Proof of Theorem 4.5.5. Let $c, n, q \in \mathbb{N}$, where q is a prime power. Let $V, W < \mathbb{F}_q^n$ and suppose that $\phi : V \to W$ is a c-killer. We want to establish that ϕ is a monomial equivalence followed by a coordinate projection. By Lemma 4.5.8 and Theorem 4.5.9, there is a constant weight code, $\mathcal{C} < \mathbb{F}_q^{2c}$, with nonzero weight c and with $\dim \mathcal{C} = \dim V$. We may form the code

$$W \times \mathcal{C} = \{uc \,:\, u \in W, c \in \mathcal{C}\}.$$

Since $\dim \mathcal{C} = \dim V$, there is a linear bijection $\psi : V \to \mathcal{C}$. We define

$$\begin{array}{rcccc} \phi \times \psi & : & V & \to & W \times C \\ \text{by} & & v & \mapsto & \phi(v)\psi(v). \end{array}$$

We show that $\phi \times \psi$ preserves weight. Any linear map preserves the weight of $\vec{0}$, so consider $v \in V \setminus \{\vec{0}\}$. We have

$$\mathrm{wt}((\phi \times \psi)(v)) = \mathrm{wt}(\phi(v)\psi(v)) = \mathrm{wt}(\phi(v)) + \mathrm{wt}(\psi(v)) = \mathrm{wt}(v) - c + c = \mathrm{wt}(v).$$

By the MacWilliams Extension Theorem, $\phi \times \psi$ is a monomial equivalence. Now define the coordinate projection

$$\begin{array}{rcrcl} \pi & : & W \times C & \to & W \\ \text{by} & & uc & \mapsto & u. \end{array}$$

Clearly $\phi = \pi \circ (\phi \times \psi)$, so the map has the desired form. $\square$

4.5.4 Proof of the MacWilliams Extension Theorem

Notice that we do not use the MacWilliams Extension Theorem until the proof of Theorem 4.5.5. In particular, we do not use it to prove Lemma 4.5.8. In that Lemma, the assumption that the elements in S are linearly independent is only used to ensure that $\sum_{s\in S} s \neq \vec{0}$ so that

$$\mathrm{wt}\left(\phi\left(\sum_{s\in S} s\right)\right) = \mathrm{wt}\left(\sum_{s\in S} s\right) - c.$$

For $c = 0$, this fact is true even if $\sum_{s\in S} s = \vec{0}$. Therefore we have the following lemma.

Lemma 4.5.10. *Suppose $V, W < \mathbb{F}_q^n$ and $\phi : V \to W$ is a weight preserving linear map. Given $S \subseteq V$, we have*

$$O_\emptyset(S) = O_\emptyset(\phi(S)).$$

$\square$

As it turns out, this lemma is enough to prove the MacWilliams Extension Theorem without much trouble. First we need some notation. Let $k \in \mathbb{N}$ and let q be a prime power. Given $\alpha \in \mathbb{F}_q^k$, define

$$[\alpha] = \left\{\gamma\alpha \,:\, \gamma \in \mathbb{F}_q^\times\right\}.$$

We also define

$$\mathbb{PF}_q^k = \left\{[\alpha] \,:\, \alpha \in \mathbb{F}_q^k\right\}.$$

Let $n \in \mathbb{N}$ and suppose $V < \mathbb{F}_q^n$ is vector space with an ordered spanning set

$$\mathcal{G} = (v_i)_{i=1}^k.$$

Thinking of v_i as a row vector, let

$$M = M_{\mathcal{G}} = \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_k \end{bmatrix},$$

a $k \times n$ matrix. Given $i \in [n]$, define c_i to be the i^{th} column of M. Given $[\alpha] \in \mathbb{PF}_q^k$, we define

$$R_{[\alpha],\mathcal{G}} = \{i \in [n] \,:\, [c_i] = [\alpha]\}.$$

We want to show that $\left|R_{[\alpha],\mathcal{G}}\right|$ can be determined if you know the size of $O_\emptyset(S)$ for all $S \subseteq V$. From this the MacWilliams Extension Theorem will easily follow. We make this idea precise below. Define

$$\mathbb{N}^{2^{\left(\mathbb{F}_q^k\right)}} = \left\{f : 2^{\left(\mathbb{F}_q^k\right)} \to \mathbb{N}\right\}.$$

That is, $\mathbb{N}^{2^{\left(\mathbb{F}_q^k\right)}}$ is the collection of functions from the powerset of $\mathbb{F}_q^k$ to $\mathbb{N}$. Finally, define $f_{\mathcal{G}} \in \mathbb{N}^{2^{\left(\mathbb{F}_q^k\right)}}$ by

$$f_{\mathcal{G}}(S) = O_\emptyset(SM) \text{ for all } S \subseteq \mathbb{F}_q^k,$$

where

$$SM = \{\alpha M \, : \, \alpha \in S\} \, .$$

Notice that for $\alpha \in \mathbb{F}_q^k$ we have, by the definition of M,

$$\alpha M = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_k v_k.$$

We have the following lemma.

Lemma 4.5.11. *Given $n, k \in \mathbb{N}$, and $[\alpha] \in \mathbb{PF}_q^k$, there is a function*

$$T_{[\alpha],n,k} : \mathbb{N}^{2^{\left(\mathbb{F}_q^k\right)}} \to \mathbb{N}$$

such that, given an ordered spanning set $\mathcal{G} = (v_i)_{i=1}^k$ for some $V < \mathbb{F}_q^n$ (with $\dim V \leq k$), we have

$$T_{[\alpha],n,k}(f_{\mathcal{G}}) = \left| R_{[\alpha],\mathcal{G}} \right| .$$

In other words, if we known $O_\emptyset(S)$ for all $S \subseteq \mathbb{F}_q^k$, then we can determine $\left| R_{[\alpha],\mathcal{G}} \right|$ for all $[\alpha] \in \mathbb{PF}_q^k$.

Proof. We proceed by induction on n. If $n = 1$, then M has only one column, and hence there is exactly one $[\alpha] \in \mathbb{PF}_q^k$ with $\left| R_{[\alpha],\mathcal{G}} \right| = 1$. If we can determine $[\alpha]$ from $f_{\mathcal{G}}$, then given $[\beta] \in \mathbb{PF}_q^k$, we can set

$$T_{[\beta],n,k}(f_{\mathcal{G}}) = \begin{cases} 1 & \text{if } [\beta] = [\alpha]; \\ 0 & \text{otherwise.} \end{cases}$$

As it turns out, we *can* determine $[\alpha]$ from $f_{\mathcal{G}}$. For each $i \in [k]$, we have that $v_i = \vec{0} = 0$ if and only if $O_\emptyset(\{v_i\}) = 0$. That is, $v_i = 0$ if and only if $f_{\mathcal{G}}(\{e_i\}) = 0$, where e_i is the vector with a one in the i^{th} entry and zeroes everywhere else. Thus we can determine the first coordinate $i \in [k]$ where $\pi_i(\alpha) \neq 0$. We are now ready to determine all of $[\alpha]$. If there is no nonzero coordinate, then $[\alpha] = 0$. Otherwise, for all $j \neq i$, there is exactly one $\gamma_j \in \mathbb{F}_q$ such that

$$\pi_j(\alpha) = \gamma_j \pi_i(\alpha).$$

In other words, there is one $\gamma_j \in \mathbb{F}_q$ such that $f_{\mathcal{G}}(\{e_i, e_j - \gamma_j e_i\}) = 0$. Thus, we can determine γ_j from $f_{\mathcal{G}}$. If we define $\gamma_i = 1$, then

$$[\alpha] = [(\gamma_1, \gamma_2, \ldots, \gamma_k)].$$

We now handle the case $n > 1$. First suppose that for all $v \in V$ we have $\mathrm{wt}(v) \in \{0, n\}$. This fact is encoded in $f_{\mathcal{G}}$; for all $\alpha \in F_q^k \setminus \{\vec{0}\}$, we have $f_{\mathcal{G}}(\alpha) \in \{0, n\}$. We claim that $\dim V \leq 1$. This is true because an l-dimensional vector space is monomially equivalent to a space with a generator matrix of the form

$$\left[\begin{array}{c|c} I_l & A \end{array}\right],$$

where I_l is the $l \times l$ identity matrix. In particular, if v is the top row of this matrix, then $1 \leq \mathrm{wt}(v) \leq n - (l-1)$. If $l > 1$ then $\mathrm{wt}(v) \notin \{0, n\}$. Hence $\dim V \leq 1$. Therefore, every nonzero vector of V is a constant multiple of any other nonzero vector of V. Thus, there exists a vector $\alpha \in \mathbb{F}_q^k$ such that

$$[c_i] = [\alpha] \text{ for all } i \in [n].$$

We may use essentially the same reasoning given for the case $n = 1$ to reconstruct

$[\alpha]$ from $f_{\mathcal{G}}$, so we are able to define

$$T_{[\beta],n,k}(f_{\mathcal{G}}) = \begin{cases} n & \text{if } [\beta] = [\alpha]; \\ 0 & \text{otherwise.} \end{cases}$$

Thus, we may assume that $n > 1$ and that there exists a nonzero vector $v \in V$ with

$$1 \leq \mathrm{wt}(v) < n.$$

Of course, there exists a nonzero $\alpha_1 \in \mathbb{F}_q^k$ with $v = \alpha_1 M$. Extend $\{\alpha_1\}$ to a basis,

$$\mathcal{B} = \{\alpha_1, \alpha_2, \ldots, \alpha_k\},$$

of $\mathbb{F}_q^k$. Now set

$$\mathcal{G}' = (v_i' = \alpha_i M_{\mathcal{G}})_{i=1}^{k}.$$

Notice that $\mathcal{G}'$ is an ordered spanning set for V. Moreover, $f_{\mathcal{G}'}$ can be determined from $f_{\mathcal{G}}$. To see this, let C be the $k \times k$ matrix

$$C = \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_k \end{bmatrix}.$$

Given $S \subseteq \mathbb{F}_q^k$, we have

$$\begin{aligned} f_{\mathcal{G}'}(S) &= O_\emptyset(SM_{\mathcal{G}'}) \\ &= O_\emptyset(S(CM_{\mathcal{G}})) \\ &= O_\emptyset((SC)M_{\mathcal{G}}) \\ &= f_{\mathcal{G}}(SC). \end{aligned}$$

Now set $A = \operatorname{supp}(v)$ and define

$$\mathcal{G}'_A = \left(\pi_A\left(v'_i\right)\right)_{i=1}^k,$$

an ordered spanning set for $\pi_A(V)$. Notice that given $\alpha \in \mathbb{F}_q^k$ with $\pi_1(\alpha) \neq 0$, we have

$$\left|R_{[\alpha],\mathcal{G}'_A}\right| = \left|R_{[\alpha],\mathcal{G}'}\right|.$$

Furthermore, $f_{\mathcal{G}'_A}$ is determined by $f_{\mathcal{G}'}$: given $S \subseteq \mathbb{F}_q^k$, we have

$$\begin{aligned} f_{\mathcal{G}'_A}(S) &= O_\emptyset(SM_{\mathcal{G}'_A}) \\ &= O_\emptyset(v \cup SM_{\mathcal{G}'}) \\ &= O_\emptyset((S \cup \{e_1\})M_{\mathcal{G}'}) \\ &= f_{\mathcal{G}'}(S \cup \{e_1\}). \end{aligned} \tag{4.5.5}$$

By our choice of v, we have that $|A| < n$. By induction we have that, for all $\alpha \in \mathbb{F}_q^k$, there exists

$$T_{[\alpha],|A|,k} : \mathbb{N}^{2^{F_q^k}} \to \mathbb{N}$$

such that for any sequence $\mathcal{H}$ of k vectors from $\mathbb{F}_q^{|S|}$, we have

$$T_{[\alpha],|A|,k}(f_{\mathcal{H}}) = \left|R_{[\alpha],\mathcal{H}}\right|.$$

Let $\alpha \in \mathbb{F}_q^k$ with $\pi_1(\alpha) \neq 0$. From (4.5.5), the following is well-defined:

$$T_{[\alpha],n,k}(f_{\mathcal{G}'}) = T_{[\alpha],|A|,k}(f_{\mathcal{G}'_A}).$$

Moreover, we have

$$\begin{aligned} T_{[\alpha],n,k}(f_{\mathcal{G}'}) &= T_{[\alpha],|A|,k}(f_{\mathcal{G}'_A}) \\ &= \left|R_{[\alpha],\mathcal{G}'_A}\right| \\ &= \left|R_{[\alpha],\mathcal{G}'}\right|. \end{aligned}$$

By setting $U = [n] \setminus \mathrm{supp}(v)$ and considering $\pi_U(V)$, we may use reasoning very similar to that above to determine that for $\alpha \in \mathbb{F}_q^k$ with $\pi_1(\alpha) = 0$, we have that $\left|R_{[\alpha],\mathcal{G}'}\right|$ is a function of $f_{\mathcal{G}'}$. Thus for all $\alpha \in \mathbb{F}_q^k$, the following is well-defined:

$$T_{[\alpha],n,k}(f_{\mathcal{G}'}) = \left|R_{[\alpha],\mathcal{G}'}\right|.$$

All that is left to show is that we can use this information to determine $\left|R_{[\alpha],\mathcal{G}}\right|$ for all $\alpha \in \mathbb{F}_q^k$. We claim that

$$R_{[\alpha],\mathcal{G}} = R_{[C\alpha],\mathcal{G}'}.$$

To see this, first recall that $M_{\mathcal{G}'} = CM_{\mathcal{G}}$. Now let $i \in R_{[\alpha],\mathcal{G}}$. We have that c_i (the i^{th} column of $M_{\mathcal{G}}$) satisfies $[c_i] = [\alpha]$. But the i^{th} column of $M_{\mathcal{G}'}$ is Cc_i. We have

$[Cc_i] = [C[\alpha]]$. Thus, $i \in R_{C[\alpha],\mathcal{G}'}$. Thus,

$$\left|R_{[\alpha],\mathcal{G}}\right| \leq \left|R_{[C\alpha],\mathcal{G}'}\right|.$$

But since C is invertible, $M_{\mathcal{G}} = C^{-1}M_{\mathcal{G}'}$. By symmetry,

$$\left|R_{[C\alpha],\mathcal{G}'}\right| \leq \left|R_{[\alpha],\mathcal{G}}\right|.$$

□

We are now ready to prove the MacWilliams Extension Theorem.

Proof of the MacWilliams Extension Theorem. Let $n, q \in \mathbb{N}$, where q is a prime power. Suppose that $V, W < \mathbb{F}_q^n$ are k-dimensional subspaces and that $\phi : V \to W$ is a weight-preserving linear map. Suppose V has dimension k. Let

$$\mathcal{B} = (v_i)_{i=1}^k$$

be an ordered basis for V. Define

$$\mathcal{C} = (\phi(v_i))_{i=1}^k.$$

Then $\mathcal{C}$ is a basis for W. By Lemma 4.5.10, we have that for all $S \subseteq V$,

$$O_{\emptyset}(S) = O_{\emptyset}(\phi(S)).$$

Thus, given $T \subseteq \mathbb{F}_q^k$, we have that

$$\begin{aligned} f_{\mathcal{B}}(T) &= O_{\emptyset}(TM_{\mathcal{B}}) \\ &= O_{\emptyset}(TM_{\mathcal{C}}) \\ &= f_{\mathcal{C}}(T), \end{aligned}$$

and so

$$f_{\mathcal{B}} = f_{\mathcal{C}}.$$

Thus we may apply Lemma 4.5.11 to establish that for all $\alpha \in \mathbb{F}_q^k$,

$$\begin{aligned} \left|R_{[\alpha],\mathcal{B}}\right| &= T_{[\alpha],n,k}(f_{\mathcal{B}}) \\ &= T_{[\alpha],n,k}(f_{\mathcal{C}}) \\ &= \left|R_{[\alpha],\mathcal{C}}\right|. \end{aligned}$$

But then there is a permutation $\sigma : [n] \to [n]$ such that for every $j \in [n]$, we have

$$[c_j] = [c'_{\sigma(j)}],$$

where c_j is the j^{th} column of $M_{\mathcal{B}}$, and $c'_{\sigma(j)}$ is the $\sigma(j)^{th}$ column of $M_{\mathcal{C}}$. But this means there is vector of nonzero coefficients $(\gamma_1, \gamma_1, \ldots, \gamma_n) \in \mathbb{F}_q^n$ such that for all $j \in [n]$,

$$\gamma_j c_j = c'_{\sigma(j)}.$$

Now let $v_i \in \mathcal{B}$. We have that for all $j \in [n]$,

$$\pi_j\left(\phi(v_i)\right) = \gamma_j \pi_{\sigma^{-1}(j)}\left(v_i\right).$$

Thus ϕ is a monomial equivalence. $\square$

4.5.5 An Application of c-Killers

We will now apply the characterization of binary c-killers to determine the parameters for which w is odd and $m(n,k,w) = 2^{k-1} - 1$. We've already determined when $m(n,k,w) = 2^{k-1}$, so this is a next natural question.

Proposition 4.5.12. *Let $k, n, w \in \mathbb{N}$ where w is odd, $k \geq 1$, and $n \geq 1$. There is a k-dimensional subspace $V < \mathbb{F}_2^n$ with $A_w(V) = 2^{k-1} - 1$ if and only if one of the following properties holds.*

$$w = 1 \textit{ and either a) } k = 1 \textit{ and } n \geq 2 \textit{ or b) } k = 2, 3 \textit{ and } n \geq 3 \tag{4.5.6}$$

$$w \geq 3 \textit{ and } k = 1 \tag{4.5.7}$$

$$w \geq 3 \textit{ and } 2 \leq k \leq \lfloor \log_2 w \rfloor + 2 \textit{ and } n \geq w + 2^{k-2} - 1 \tag{4.5.8}$$

$$w \geq 3 \textit{ and } 2 \leq k \leq \lfloor \log_2 (w+1) \rfloor + 2 \textit{ and } n \geq w + 2^{k-2}. \tag{4.5.9}$$

Proof. Suppose w is odd and there is a k-dimensional subspace $V < \mathbb{F}_2^n$ with $2^{k-1} - 1$ weight w vectors. When $k \geq 2$, we define v to be the single odd weight vector of V that does not have weight w. We further define $l = \mathrm{wt}(v)$. Without loss of generality,

$$v = \underbrace{\overbrace{1 \dots 1}^{R_1}}_{l} \overbrace{0 \dots 0}^{R_0} \in V.$$

Let $\mathcal{E}$ be the subspace of even weight vectors from V.

Case 1: $w = 1$.

In this case V has $2^{k-1} - 1$ weight one vectors in V. But the dimension of V is at least as big as the number of weight one vectors in V. Thus $2^{k-1} - 1 \leq k$. This equation implies that $k \leq 3$.

- If $k = 1$ then V has $2^{1-1} - 1 = 0$ weight one vectors. Thus the nonzero vector in V has weight at least 2, and hence $n \geq 2$, so (4.5.6) is satisfied.

- If $k = 2$ then V has $2^{2-1} - 1 = 1$ weight one vector. Since $k = 2$, $n \geq 2$. If $n = 2$, then $V = \mathbb{F}_2^2$, which has 2 weight one vectors. Thus $n \geq 3$, so (4.5.6) is satisfied.

- If $k = 3$ then certainly $n \geq 3$, so (4.5.6) is satisified.

Case 2: $w \geq 3$ **and** $k = 1$.

In this case (4.5.7) is satisfied.

Case 3: $w \geq 3$**,** $k \geq 2$**, and** $w > l$.

Let $e \in \mathcal{E} \setminus \{\vec{0}\}$ and notice that

$$\begin{aligned} w &= \mathrm{wt}(e + v) \\ &= \mathrm{wt}(\pi_{R_1}(e + v)) + \mathrm{wt}(\pi_{R_0}(e + v)) \\ &= l - \mathrm{wt}(\pi_{R_1}(e)) + \mathrm{wt}(\pi_{R_0}(e)), \end{aligned}$$

and thus

$$\mathrm{wt}(\pi_{R_1}(e)) = \mathrm{wt}(\pi_{R_0}(e)) - (w - l). \tag{4.5.10}$$

Furthermore, π_{R_0} is injective on $\mathcal{E}$; if $e \in \mathcal{E} \setminus \{\vec{0}\}$, has $\pi_{R_0}(e) = \vec{0}$, then $\mathrm{wt}(\pi_{R_1}(e)) = \mathrm{wt}(\pi_{R_0}(e)) - (w - l) = -(w - l) < 0$, which is absurd. Thus we may define $\phi : \pi_{R_0}(\mathcal{E}) \to \pi_{R_1}(\mathcal{E})$ by

$$\phi = \pi_{R_1} \circ {\pi_{R_0}}^{-1}.$$

(ϕ simply assigns the right hand side of $e \in \mathcal{E}$ to its left hand side). By equation (4.5.10), ϕ is a $(w - l)$-killer. By Theorem 4.5.1 (the characterization of c-killers), there is a set of coordinates $S \subseteq R_0$ such that $\pi_S(\mathcal{E})$ is a constant weight code with nonzero weight $w-l$ and dimension equal to $\dim \pi_{R_0}(\mathcal{E}) = \dim \mathcal{E} = k-1$. Thus, by Proposition 4.2.1,

$$\begin{aligned} k-1 &\leq f_2(w-l)+1 \\ &\leq \lfloor \log_2(w-l) \rfloor + 1 \\ &\leq \lfloor \log_2(w) \rfloor + 1. \end{aligned}$$

Thus

$$k \leq \lfloor \log_2(w) \rfloor + 2.$$

Also by Proposition 4.2.1,

$$|R_0| \geq 2(w-l) - (w-l)/2^{k-2}. \tag{4.5.11}$$

Since 2^{k-2} divides $(w-l)$, we have

$$2^{k-2} \leq w-1.$$

Thus

$$l \leq w - 2^{k-2}. \tag{4.5.12}$$

Combining (4.5.11) and (4.5.12), we have

$$
\begin{aligned}
n &= |R_1| + |R_0| \\
&= l + |R_0| \\
&\geq l + 2(w-l) - (w-l)/2^{k-2} \\
&= 2w - w/2^{k-2} - l(1 - 1/2^{k-2}) \\
&\geq 2w - w/2^{k-2} - (w - 2^{k-2})(1 - 1/2^{k-2}) \\
&= w + 2^{k-2} - 1.
\end{aligned}
$$

Thus (4.5.8) is satisfied.

Case 4: $w \geq 3$**,** $k \geq 2$**, and** $w < l$.

By applying arguments similar to those above, π_{R_1} is injective on $\mathcal{E}$, and we may construct $\phi : \pi_{R_1}(\mathcal{E}) \to \pi_{R_0}(\mathcal{E})$ which assigns the left hand side of $e \in \mathcal{E}$ to its right hand side. Again by using similar arguments to those above, ϕ is an $(l-w)$-killer. Thus there is some set of coordinates $S \subseteq R_1$ such that $\pi_S(\mathcal{E})$ is a $(k-1)$-dimensional constant weight code with nonzero weight $(l-w)$. This implies that 2^{k-2} divides $(l-w)$. Thus

$$
l - w \geq 2^{k-2},
$$

and so

$$
l \geq w + 2^{k-2}.
$$

Notice that

$$
n = |R_1| + |R_0| \geq |R_1| = l \geq w + 2^{k-2}.
$$

Furthermore,

$$\begin{aligned} l &= |R_1| \\ &\geq 2(l-w) - (l-w)/2^{k-2} \end{aligned}$$

and therefore

$$\begin{aligned} 0 &\geq -l + 2l - 2w - l/2^{k-2} + w/2^{k-2} \\ &= l - l/2^{k-2} - 2w + w/2^{k-2} \\ &= l(1 - 1/2^{k-2}) - 2w + w/2^{k-2} \\ &\geq (w + 2^{k-2})(1 - 1/2^{k-2}) - 2w + w/2^{k-2} \\ &= -w + 2^{k-2} - 1 \end{aligned}$$

thus

$$w + 1 \geq 2^{k-2}$$

and so

$$\lfloor \log_2(w+1) \rfloor + 2 \geq k.$$

Thus (4.5.9) is satisfied.

Now we handle the other direction. Suppose that one of the clauses (4.5.6) - (4.5.9) is satisfied. We need to show that there is a k-dimensional subspace $V < \mathbb{F}_2^n$ with $2^{k-1} - 1$ weight w vectors.

Case 1: $w = 1$ **and either a)** $k = 1$ **and** $n \geq 2$ **or b)** $k = 2, 3$ **and** $n \geq 3$**.**

- In the case $k = 1$ and $n \geq 2$, we let $V < \mathbb{F}_2^n$ be $\{\vec{0}, v\}$, where v is any vector with $\mathrm{wt}(v) = 2$. This has $0 = 2^{1-1} - 1$ weight one vectors.

- In the case $k = 2$ and $n \geq 3$ we take V to be the space

$$V = \{0000\ldots0000, 1000\ldots0000, 1110\ldots0000, 0110\ldots0000\}.$$

This has $1 = 2^{2-1} - 1$ weight one vector.

- In the case $k = 3$ and $n \geq 3$, we let

$$V = \left\{v000\ldots000 \,:\, v \in \mathbb{F}_2^3\right\}$$

This has $3 = 2^{3-1} - 1$ weight one vectors.

Case 2: $w \geq 3$ **and** $k = 1$ **and** $n \geq 1$**.**

In this case, we are looking for a subspace $V < \mathbb{F}_2^n$ with no vectors of weight w. We are assuming that $w \geq 3$, so we may take any subspace whose single nonzero vector has weight 1.

Case 3: $w \geq 3$ **and** $2 \leq k \leq \lfloor \log_2 w \rfloor + 2$ **and** $n \geq w + 2^{k-2} - 1$**.**

If $k = 2$ then set

$$\begin{aligned} V = \Big\{ & \underbrace{111\ldots111}_{w}\underbrace{000\ldots000}_{n-w}, \\ & \underbrace{100\ldots000}_{w}\underbrace{000\ldots000}_{n-w}, \\ & \underbrace{011\ldots111}_{w}\underbrace{000\ldots000}_{n-w}, \\ & \underbrace{000\ldots000}_{w}\underbrace{000\ldots000}_{n-w} \Big\}. \end{aligned}$$

If $k \geq 3$ then set

$$l = w - 2^{k-2},$$

and define

$$v = \underbrace{111\ldots111}_{l}\underbrace{000\ldots000}_{n-l}.$$

This is possible, since $l \leq w - 1 < w \leq n$. Recall that $\mathcal{S}_{k-1} < \mathbb{F}_2^{2^{k-1}-1}$ is a constant weight code of dimension $k-1$ and nonzero weight 2^{k-2}. Now set

$$\mathcal{E} = \left\{ \underbrace{000\ldots000}_{l}\, s\, \underbrace{000\ldots000}_{n-l-2^{k-1}+1} \,:\, s \in \mathcal{S}_{k-1} \right\}.$$

Notice that this is possible because $n - l - 2^{k-1} + 1 = n - (w + 2^{k-2} - 1) \geq 0$. Finally, let

$$V = \mathcal{E} + \{\vec{0}, v\}.$$

Notice that the set of odd weight vectors in V is

$$O = \left\{ \underbrace{111\ldots111}_{l}\, s\, \underbrace{000\ldots000}_{n-l-2^{k-1}+1} \,:\, s \in \mathcal{S}_{k-1} \right\}.$$

When $s = \vec{0}$, we have that the corresponding vector in O has weight l, which is not w. If $s \in \mathcal{S}_{k-1} \setminus \{\vec{0}\}$, then the weight of the corresponding vector in O is $l + 2^{k-2} = w - 2^{k-2} + 2^{k-2} = w$.

Case 4: $w \geq 3$ **and** $2 \leq k \leq \lfloor \log_2 (w+1) \rfloor + 2$ **and** $n \geq w + 2^{k-2}$**.**

First notice that if $k = 2$ then the conditions for Case 3 are met, and we have already handled Case 3. Thus we can assume $k \geq 3$. Define

$$l = w + 2^{k-2}.$$

Notice that $k \leq \lfloor \log_2 (w+1) \rfloor + 2$ implies

$$w \geq 2^{k-2} - 1$$

and hence

$$l = w + 2^{k-2} \geq 2^{k-2} - 1 + 2^{k-2} = 2^{k-1} - 1.$$

In particular, there exists $\mathcal{S}(k-1,1,l) < \mathbb{F}_2^l$, a constant weight code of dimension $k-1$, and nonzero weight 2^{k-2}. Set

$$V = \left\{ s\underbrace{0\ldots0}_{n-l} \,:\, s \in \mathcal{S}(k-1,1,l) \right\} \cup \left\{ \overline{s}\underbrace{0\ldots0}_{n-l} \,:\, s \in \mathcal{S}(k-1,1,l) \right\}.$$

Notice that V is a k-dimensional subspace of $\mathbb{F}_2^n$. Let $s \in \mathcal{S}(k-1,1,l)$. If $s = \vec{0}$ then

$$\mathrm{wt}(\overline{s}\underbrace{0\ldots0}_{n-l}) = l \neq w.$$

On the other hand, if $s \neq \vec{0}$, we have

$$\mathrm{wt}(\overline{s}\underbrace{0\ldots0}_{n-l}) = l - \mathrm{wt}(s) = w + 2^{k-2} - 2^{k-2} = w.$$

Thus exactly one of the odd weight vectors does not have weight w, and we are done. $\square$

As it turns out, the bounds on n and k in Proposition 4.5.12 are very restrictive. In particular, it is usually the case that if these bounds are met then we also have $k \leq w+1$ and $n \geq w+k-1$ and so by Proposition 4.3.1, we have $m(n,k,w) = 2^{k-1}$. The following proposition establishes the small set of parameters for which $m(n,k,w) = 2^{k-1} - 1$.

Proposition 4.5.13. *Let $n, k, w \in \mathbb{N}$ where $1 \leq k, w \leq n$ and w is odd. If $m(n,k,w) = 2^{k-1} - 1$, then $k \leq 3$. Furthermore, we have*

- $m(n,1,w) = 2^{1-1} - 1 = 0$ *is impossible.*
- $m(n,2,w) = 2^{2-1} - 1 = 1$ *if and only if* $n = w$.
- $m(n,3,w) = 2^{3-1} - 1 = 3$ *if and only if* $w = 1$ *or* $n = w + 1$.

Proof. Suppose that $m(n,k,w) = 2^{k-1} - 1$. First we show that $k \leq 3$. Suppose to the contrary that $k > 3$. Since one of the clauses (4.5.6)-(4.5.9) must be satisfied and clauses (4.5.6) and (4.5.7) specify $k \leq 3$, it must be that (4.5.8) or (4.5.9) is satisfied.

We have $m(n,k,w) \neq 2^{k-1}$. Thus by Proposition 4.3.1, either $k > w + 1$ or $n < w + k - 1$. First consider $k > w + 1$. Since one of (4.5.8) or (4.5.9) is true, it must be the case that

$$k \leq \max\left\{\lfloor \log_2 w \rfloor + 2, \lfloor \log_2 (w+1) \rfloor + 2\right\} = \lfloor \log_2 (w+1) \rfloor + 2,$$

and hence

$$w + 1 < k \leq \lfloor \log_2 (w+1) \rfloor + 2.$$

As it turns out, $w = 2$ is the largest w for which $w + 1 < \lfloor \log_2 (w+1) \rfloor + 2$. Thus

$$k \leq \lfloor \log_2 (2+1) \rfloor + 2 = 3.$$

On the other hand, suppose $n < w + k - 1$. Since one of (4.5.8) or (4.5.9) is true, we have

$$n \geq \min\left\{w + 2^{k-2} - 1, w + 2^{k-2}\right\} = w + 2^{k-2} - 1.$$

Thus,

$$w + 2^{k-2} - 1 \leq n < w + k - 1.$$

Therefore

$$2^{k-2} < k.$$

As it turns out, the largest k for which this is true is $k = 3$.

We have established that $k \leq 3$. If $m(n, 1, w) = 0$ then n is not large enough to accommodate a single weight w vector. Thus $n < w$. This violates the assumption that $w \leq n$, so it is impossible to have $m(n, 1, w) = 0$.

If $m(n, 2, w) = 1$, then n is large enough to accommodate a weight w vector, but not two of them. Thus $n = w$. If $n = w$, then there is exactly one weight w vector in $\mathbb{F}_2^n$. Any two dimensional subspace containing that vector establishes $m(n, 2, w) = 1$.

If $m(n, 3, w) = 3$ then by Proposition 4.3.1, either $k > w + 1$ or $n < w + k - 1$. In the first case we have $3 > w + 1$, and hence $w < 2$. Since w is odd, this implies $w = 1$. If $n < w + k - 1$, then $n < w + 2$, so $n \leq w + 1$. But $m(n, 3, w) > 1$ implies $n > w$. Thus $n = w + 1$.

On the other hand, if $w = 1$, then we may take

$$V = \left\{ v000\ldots000 \,:\, v \in \mathbb{F}_2^3 \right\}.$$

If $n = w + 1$, we may take the code, V, generated by the following $3 \times n$ matrix.

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

The odd weight vectors in V are the three rows of this matrix, which have weight w, and the sum of these rows, which has weight $w - 2$. $\square$

4.6 Conjectures

4.6.1 The Behavior of $m(n,k,w)$ as $k \to \infty$

From empirical evidence, we have the following conjecture.

Conjecture 4.6.1. *For $n \geq k$ and $k \geq 2w$, we have*

$$m(n,k,w) = \begin{cases} \binom{k+1}{w} & \text{if } w \text{ is even;} \\ \binom{k}{w} & \text{if } w \text{ is odd.} \end{cases}$$

$\square$

We will establish this in the case $n = k+1$. We will also establish it for w odd and $n = k+2$. First we need the following lemma.

Lemma 4.6.2. *If $0 < w < n$ and $V < \mathbb{F}_2^n$ is the space generated by the weight w vectors of $\mathbb{F}_2^n$ then*

$$\dim V = \begin{cases} n-1 & w \text{ even;} \\ n & w \text{ odd.} \end{cases}$$

Proof. The collection of even-weight vectors is a subspace of $\mathbb{F}_2^n$. Call this set $\mathcal{E}$. We have that $\dim \mathcal{E} = n-1$. We claim that $\mathcal{E} < V$. To prove this, we establish that all weight 2 vectors are in V. Clearly, the collection of weight 2 vectors spans $\mathcal{E}$.

Let p_1 and p_2 be two bit positions. We demonstrate that the vector with ones exactly at p_1 and p_2 is in V. WLOG, p_1 and p_2 are the first two bit positions. Then

$$v = 10\underbrace{1\ldots1}_{w-1}\underbrace{0\ldots0}_{n-w-1}$$

and

$$u = 01\underbrace{1\ldots1}_{w-1}\underbrace{0\ldots0}_{n-w-1}$$

are weight w vectors, and

$$u + v = 110\ldots0.$$

The claim is proved.

Now, if w is even then clearly $V < \mathcal{E}$. By the claim, we have $V = \mathcal{E}$. Therefore

$$\dim V = \dim \mathcal{E} = n - 1, \text{ when } w \text{ is even.}$$

If w is odd then V contains odd weight vectors, and so $V \neq \mathcal{E}$. By the claim, $V \gneqq \mathcal{E}$. Therefore

$$\dim V = \dim \mathbb{F}_2^n = n, \text{ when } w \text{ is odd.}$$

$\square$

Recall that, given $V < \mathbb{F}_2^n$, we defined $A_w(V)$ to be the number of weight w vectors in V. If V is k-dimensional and $m(n,k,w) = A_w(V)$ then the following lemma tells us that (usually) V has a basis of weight w vectors.

Lemma 4.6.3. *Let $n, k, w \in \mathbb{N}$, with $w, k \leq n$ and let $V < \mathbb{F}_2^n$ be a k-dimensional subspace with $A_w(V) = m(n,k,w)$. There is a basis $\mathcal{B}$ for V consisting of Hamming weight w vectors if and only if w is odd or $k < n$.*

Proof. We first prove the contrapositive of the forward direction. Suppose w is even and $n = k$. Then $V = \mathbb{F}_2^n$, which has dimension n. By Lemma 4.6.2, the space spanned by the weight w vectors of $\mathbb{F}_2^n$ has dimension $n-1$. Therefore, at least one vector in a basis for V has weight not equal to w.

Suppose that w is odd or $n > k$. We want to show that there exists a basis $\mathcal{B} \subset V$ consisting of weight w vectors. Suppose not. Let V' be the span of the weight w vectors of V. It has dimension $\dim V' < k \leq n$. If w is odd then by Lemma 4.6.2, there is $v \in \mathbb{F}_2^n \backslash V'$ with $\mathrm{wt}(v) = w$. If $n > k$, then $\dim V < k \leq n-1$, and again there is $v \in \mathbb{F}_2^n \setminus V'$ with $\mathrm{wt}(v) = w$. But V' contains all of the weight w vectors of V, so we have that $V' + \{\vec{0}, v\}$ has more weight w vectors than V. But $\dim(V' + \{\vec{0}, v\}) \leq k$. Thus we may extend $V' + \{\vec{0}, v\}$ to a dimension k subspace of $\mathbb{F}_2^n$ with more weight w vectors than V. This contradicts our choice of V. □

We are now ready to show that Conjecture 4.6.1 is true for $n = k + 1$.

Lemma 4.6.4. *If $k, w \in \mathbb{N}$ and $k \geq 2w$ then*

$$m(k+1, k, w) = \begin{cases} \binom{k+1}{w} & w \ \textit{even} \\ \binom{k}{w} & w \ \textit{odd} \end{cases}$$

Proof. Suppose w is even. By Lemma 4.6.2, the span of all of the weight-w vectors in $\mathbb{F}_2^{k+1}$ (there are $\binom{k+1}{w}$ of them in total) has dimension k, so we're done. Thus we may assume that w is odd.

Let $V < \mathbb{F}_2^{k+1}$ have $A_w(V) = m(k+1, k, w)$. Since V has dimension k, it is monomially equivalent to a vector space having a generator matrix of the form

$$G = \left[\begin{array}{c|c} I_k & c \end{array} \right].$$

Here c is a column vector. By permuting rows and columns of G we may assume that c is of the form

$$c = (\underbrace{0, 0, 0, \ldots, 0, 0, 0}_{a}, \underbrace{1, 1, 1, \ldots, 1, 1, 1}_{b}).$$

Notice that $a + b = k$.

If we drop c from G, how many weight-w vectors are lost, and how many are gained? That is, are there more weight-w vectors in V or in $V' = \mathbb{F}_2^k \times \{0\}$, the code with generator matrix

$$G' = \left[\begin{array}{c|c} I_k & \vec{0} \end{array} \right]?$$

Let L be the *lost* vectors. That is,

$$L = \{v \in V \,:\, v \notin V'\}.$$

Let F be the *found* vectors. That is,

$$F = \{v' \in V' \,:\, v' \notin V\}.$$

We will construct an injective function $f : L \to F$. This will establish that $|L| \leq |F|$ and thus,

$$A_w(V') = A_w(V) - |L| + |F| \geq A_w(V).$$

Set

$$B = \{a+1, a+2, \ldots, a+b=k\}.$$

Notice that for $v \in V$, we have

$$\mathrm{wt}(\pi_{B\cup\{k+1\}}(v)) \equiv 0 (\mathrm{mod}\ 2).$$

In particular, $b \neq k$, since this would imply that every vector in V has even weight. This is a contradiction, since w is odd, and $A_w(V) = m(n,k,w) > 0$. Note that

$$L = \left\{v \in V \,:\, \mathrm{wt}(\pi_{[k]}(v)) = w-1 \text{ and } \mathrm{wt}(\pi_B(v)) \equiv 1 (\mathrm{mod}\ 2)\right\}$$

and

$$F = \left\{v' \in V' \,:\, \mathrm{wt}(\pi_{[k]}(v')) = w \text{ and } \mathrm{wt}(\pi_B(v)) \equiv 1 (\mathrm{mod}\ 2)\right\}. \tag{4.6.1}$$

We will now define f. The definition will depend (slightly) on the parity of a.

Case 1: a is odd.

Given $l \in L$, define

$$g(l) = \min \left\{ i \ : \ \mathrm{wt}\left(\overline{\pi_{[i]}\left(l\right)} \pi_{\{i+1,\ldots,k\}}\left(l\right) \right) = w \right\},$$

and set

$$f(l) = \overline{\pi_{[g(l)]}\left(l\right)} \pi_{\{g(l)+1,\ldots,k\}}\left(l\right) 0.$$

In words: we scan across l from left to right, inverting bits one at a time. We stop when the weight on $[k]$ is w, and we change the last bit to 0. We have three things to show: that $g(l) < \infty$ (so that f is well-defined), that $f(l) \in F$, and that f is injective.

First we show that $g(l) < \infty$. In fact, $g(l) < k$. Notice that

$$\begin{aligned}
\mathrm{wt}\left(\overline{\pi_{[k]}\left(l\right)} \right) &= k - \mathrm{wt}(\pi_{[k]}\left(l\right)) \\
&= k - (w-1) \\
&\geq 2w - (w-1) \\
&= w + 1.
\end{aligned}$$

We have that $\mathrm{wt}\left(\pi_{[k]}\left(l\right)\right) = w - 1$, and $\mathrm{wt}\left(\overline{\pi_{[k]}\left(l\right)} \right) \geq w + 1$. Since inverting a single bit in a vector changes its weight by one, one of the intermediate inversions considered in the definition of g must have weight w. Hence $g(l) < k$.

Now we show that $f(l) \in F$. By Equation (4.6.1), we need only show that $f(l) \in V'$, that $\mathrm{wt}(\pi_{[k]}\left(f(l)\right)) = w$, and $\mathrm{wt}(\pi_B\left(f(l)\right)) \equiv 1 (\mathrm{mod}\ 2)$. The only requirement for $f(l) \in V'$ is that $\pi_{k+1}\left(f(l)\right) = 0$. This is true by definition of f. By definition of g, it is clearly true that $\mathrm{wt}(\pi_{[k]}\left(f(l)\right)) = w$. It is left to show that $\mathrm{wt}(\pi_B\left(f(l)\right)) \equiv 1 (\mathrm{mod}\ 2)$.

Either $g(l) \leq a$ or $g(l) > a$. In the first case,

$$\mathrm{wt}(\pi_B\left(f(l)\right)) = \mathrm{wt}(\pi_B\left(l\right)) \equiv 1 \bmod 2.$$

Consider $g(l) > a$. Inversion of a single bit changes the parity of the weight of a vector. Since $\mathrm{wt}(\pi_{[k]}\left(l\right)) = w - 1$ and $\mathrm{wt}(\pi_{[k]}\left(f(l)\right)) = w$ (they have different parities), $g(l)$ must be odd. Since a is odd and f inverts all bits on $[a]$, $f(l)$ inverts an even number of bits on B. Thus

$$\mathrm{wt}(\pi_B\left(f(l)\right)) \equiv \mathrm{wt}(\pi_B\left(l\right)) \equiv 1 \bmod 2.$$

Finally, we show that f is injective. Let $l \in L$. We show how to construct l from $f(l)$. Given $m \in F$, define

$$g'(m) = \min\left\{i \,:\, \mathrm{wt}\left(\overline{\pi_{[i]}\left(m\right)}\pi_{\{i+1,\ldots,k\}}\left(m\right)\right) = w - 1\right\},$$

and set

$$f'(m) = \overline{\pi_{[g(m)]}\left(m\right)}\pi_{\{g(m)+1,\ldots,k\}}\left(m\right)1.$$

Now, it is not necessarily the case that $g'(m) < \infty$. On the other hand, it is certainly the case that $g'(f(l)) \leq g(l)$, since

$$\begin{aligned}
\mathrm{wt}\left(\overline{\pi_{[g(l)]}\left(f(l)\right)}\pi_{\{g(l)+1,\ldots,k\}}\left(f(l)\right)\right) &= \mathrm{wt}\left(\overline{\overline{\pi_{[g(l)]}\left(l\right)}}\pi_{\{g(l)+1,\ldots,k\}}\left(l\right)\right) \\
&= \mathrm{wt}\left(\pi_{[k]}\left(l\right)\right) \\
&= w - 1.
\end{aligned}$$

In fact, $g'(f(l)) = g(l)$. If $g'(f(l))$ were less than $g(l)$, then

$$\begin{aligned}
\mathrm{wt}\left(\pi_{[g'(f(l))]}\left(f(l)\right)\right) + \mathrm{wt}\left(\pi_{\{g'(f(l))+1,\ldots,k\}}\left(f(l)\right)\right)& \\
&= \mathrm{wt}\left(\pi_{[k]}\left(f(l)\right)\right) \\
&= w \\
&= (w-1)+1 \\
&= \mathrm{wt}\left(f'(f(l))\right)+1 \\
&= \mathrm{wt}\left(\overline{\pi_{[g'(f(l))]}\left(f(l)\right)}\right) + \mathrm{wt}\left(\pi_{\{g'(f(l))+1,\ldots,k\}}\left(f(l)\right)\right)+1.
\end{aligned}$$

Thus

$$\mathrm{wt}\left(\pi_{[g'(f(l))]}\left(f(l)\right)\right) = \mathrm{wt}\left(\overline{\pi_{[g'(f(l))]}\left(f(l)\right)}\right)+1.$$

But this implies

$$\begin{aligned}
\mathrm{wt}\left(\overline{\pi_{[g'(f(l))]}\left(l\right)}\pi_{\{g'(f(l))+1,\ldots,k\}}\left(l\right)\right)& \\
&= \mathrm{wt}\left(\overline{\pi_{[g'(f(l))]}\left(l\right)}\right) + \mathrm{wt}\left(\pi_{\{g'(f(l))+1,\ldots,k\}}\left(l\right)\right) \\
&= \mathrm{wt}\left(\pi_{[g'(f(l))]}\left(f(l)\right)\right) + \mathrm{wt}\left(\pi_{\{g'(f(l))+1,\ldots,k\}}\left(l\right)\right) \\
&= \mathrm{wt}\left(\overline{\pi_{[g'(f(l))]}\left(f(l)\right)}\right)+1 + \mathrm{wt}\left(\pi_{\{g'(f(l))+1,\ldots,k\}}\left(l\right)\right) \\
&= \mathrm{wt}\left(\pi_{[g'(f(l))]}\left(l\right)\right)+1 + \mathrm{wt}\left(\pi_{\{g'(f(l))+1,\ldots,k\}}\left(l\right)\right) \\
&= \mathrm{wt}(\pi_{[k]}\left(l\right))+1 \\
&= (w-1)+1 \\
&= w.
\end{aligned}$$

This contradicts the minimality of $g(l)$. We have established that $g'(f(l)) = g(l)$.

Thus

$$\begin{aligned} f'(f(l)) &= f'\left(\overline{\pi_{[g(l)]}(l)}\pi_{\{g(l)+1,\ldots,k\}}(l)\,0\right) \\ &= \overline{\overline{\pi_{[g(l)]}(l)}}\pi_{\{g(l)+1,\ldots,k\}}(l)\,1 \\ &= l. \end{aligned}$$

Case 2: a is even.

This case is very similar to the case where a is odd, but we do not invert the first bit of $[a]$. That is, given $l \in L$ we define

$$g(l) = \min\left\{i \,:\, \mathrm{wt}\left(\pi_1(l)\,\overline{\pi_{\{2,\ldots,i\}}(l)}\pi_{\{i+1,\ldots,k\}}(l)\right) = w\right\},$$

and

$$f(l) = \pi_1(l)\,\overline{\pi_{\{2,\ldots,g(l)\}}(l)}\pi_{\{g(l+1,\ldots,k\}}(l)\,.$$

Notice that

$$\begin{aligned} \mathrm{wt}\left(\pi_1(l)\,\overline{\pi_{\{2,\ldots,k\}}(l)}\right) &\geq \mathrm{wt}\left(\overline{\pi_{\{2,\ldots,k\}}(l)}\right) \\ &= k-1-\mathrm{wt}\left(\pi_{\{2,\ldots,k\}}(l)\right) \\ &\geq k-1-(w-1) \\ &= w. \end{aligned}$$

Hence $g(l) \leq k$. The rest is very similar to the proof for a odd. $\square$

We extend this a bit further.

Lemma 4.6.5. *If $k, w \in \mathbb{N}$ where w is odd, and $k \geq 2w$ then*

$$m(k+2, k, w) = \binom{k}{w}.$$

Proof. Let $V < \mathbb{F}_2^{k+2}$ have $A_w(V) = m(k+2, k, w)$. Up to permutation of entries, V has a generator matrix of the form

$$G = \begin{array}{c} \left[\begin{array}{cccccccccccc|cc} 1 & & & & & & & & & & & & 0 & 0 \\ & \ddots & & & & & & & & & & & \vdots & \\ & & 1 & & & & & & & & & & 0 & 0 \\ & & & 1 & & & & & & & & & 0 & 1 \\ & & & & \ddots & & & & & & & & \vdots & \\ & & & & & 1 & & & & & & & 0 & 1 \\ & & & & & & 1 & & & & & & 1 & 0 \\ & & & & & & & \ddots & & & & & \vdots & \\ & & & & & & & & 1 & & & & 1 & 0 \\ & & & & & & & & & 1 & & & 1 & 1 \\ & & & & & & & & & & \ddots & & \vdots & \\ & & & & & & & & & & & 1 & 1 & 1 \end{array}\right] \\ \leftarrow A \rightarrow \quad \leftarrow B \rightarrow \quad \leftarrow C \rightarrow \quad \leftarrow D \rightarrow \end{array}$$

The spirit of the proof is very similar to that of Lemma 4.6.4. First let us assume that at least one of $|A|$,$|B|$,$|C|$, or $|D|$ is even. Remove the last two columns of G to yield G', the generator matrix for a code V'. We compare the vectors lost to the vectors gained via an injective map that depends (slightly) on the parities of $|A|$, $|B|$, $|C|$, and $|D|$, and that inverts bits one at a time until the proper weight is achieved. We now make this precise.

Let L be the set of lost weight w vectors in V, and let F be the set of found weight w vectors in V'. We now construct an injective map $f : L \to F$. Let $l \in L$. Notice that $\mathrm{wt}\,\pi_{\{k+1,k+2\}}(l) > 0$ or else $l \in V'$. We define f differently depending on whether this weight is 1 or 2.

Case 1: $\mathrm{wt}(\pi_{\{k+1,k+2\}}(l)) = 1$**.**

Notice that since w is odd, there are some odd weight vectors in V. Hence

$$|A \cup D| > 0.$$

Invert each bit of $\pi_{[k]}(l)\,00$ in succession, starting with the coordinates of A then the coordinates of D. If $|A \cup D|$ is even, do not invert the last bit of $A \cup D$. Proceed to invert the bits of B, and then those of C. Stop when the resulting vector has weight w. Do not invert either of the last two bits (as we'll see, inverting these bits is not necessary). Define $f(l)$ to be the vector obtained from the process above.

Let $h(l)$ be the vector resulting from the process above if we do not stop when the weight becomes w. Then

$$\begin{aligned}
\mathrm{wt}\,(h(l)) &= \mathrm{wt}(\pi_A\,(h(l))) + \mathrm{wt}(\pi_B\,(h(l))) + \mathrm{wt}(\pi_C\,(h(l))) + \mathrm{wt}(\pi_D\,(h(l))) \\
&\geq |A| + |D| - 1 - \mathrm{wt}(\pi_{A\cup D\setminus \max(A\cup D)}\,(l)) \\
&\quad + |B| - \mathrm{wt}(\pi_B\,(l)) \\
&\quad + |C| - \mathrm{wt}(\pi_C\,(l)) \\
&= k - 1 - \mathrm{wt}(\pi_{A\cup D\setminus \max(A\cup D)}\,(l)) - \mathrm{wt}(\pi_B\,(l)) - \mathrm{wt}(\pi_C\,(l)) \\
&\geq 2w - 1 - \mathrm{wt}(\pi_{[k]}\,(l)) \\
&= 2w - 1 - (w-1) \\
&= w.
\end{aligned}$$

Thus the process will terminate, and $\mathrm{wt}(f(l)) = w$. Let

$$v = \pi_{[k]}\left(f(l)\right) G.$$

Notice that $v \in V$ is the unique vector in V with $\pi_{[k]}(v) = \pi_{[k]}(f(l))$. Thus to show that $f(l)$ is a found vector, we need only show that $v \neq f(l)$. To show this, we need only point out that $\pi_{\{k+1,k+2\}}(v) \neq \pi_{\{k+1,k+2\}}(f(l)) = 00$. Since $w-1$ and w have opposite parity, an odd number of bits must have been inverted in the process described above. But then we have guaranteed that the number of inverted bits in $A \cup D$ is odd, and the number of inverted bits in $B \cup C$ is even. Therefore $\pi_{\{k+1,k+2\}}(v)$ is $\pi_{\{k+1,k+2\}}(l)$ plus an odd number of even weight vectors (00 or 11) plus an even number of odd weight vectors (01 or 10). Thus $\mathrm{wt}(\pi_{\{k+1,k+2\}}(v))$ has the same parity as $\mathrm{wt}(\pi_{\{k+1,k+2\}}(l))$, which is odd. Hence $\pi_{\{k+1,k+2\}}(v) \neq 00$, as desired.

By reasoning similar to that given in the proof of Lemma 4.6.4, f is injective when restricted to the set

$$L_1 = \left\{ l \in L \,:\, \mathrm{wt}(\pi_{\{k+1,k+2\}}(l)) = 2 \right\}.$$

Case 2: $\mathrm{wt}(\pi_{\{k+1,k+2\}}(l)) = 2$

We are assuming that one of $|A|$,$|B|$,$|C|$, or $|D|$ is even. Suppose it is $|A|$. Define

$$l' = \pi_{[k]}(l)\, 00,$$

the vector derived from l by replacing the last two digits with zeroes. We produce $f(l)$ by inverting the bits of l' one at time: first in A, then in B, skipping the last bit of B if $|B|$ is odd. We then invert the bits of C, skipping the last bit of C if $|C|$ is odd. Finally, we invert the bits of D one at a time, possibly inverting the last bit of

D. We stop when the weight of the vector is w. We do not invert either of the last two bits (we will see that inverting the last two bits is not necessary). Define $f(l)$ to be the vector resulting from this process. To see that the inversion eventually stops, define $h(l)$ to be vector produced by this process if we do not stop when the weight reaches w. Then

$$\begin{aligned}
\mathrm{wt}(h(l)) &= \mathrm{wt}(\pi_A\,(h(l))) + \mathrm{wt}(\pi_B\,(h(l))) + \mathrm{wt}(\pi_C\,(h(l))) + \mathrm{wt}(\pi_D\,(h(l))) \\
&\geq |A| - \mathrm{wt}(\pi_A\,(l)) \\
&\quad + |B| - 1 - \mathrm{wt}(\pi_{B\setminus \max B}\,(l)) \\
&\quad + |C| - 1 - \mathrm{wt}(\pi_{C\setminus \max C}\,(l)) \\
&\quad + |D| - \mathrm{wt}(\pi_D\,(l)) \\
&\geq |A| - \mathrm{wt}(\pi_A\,(l)) \\
&\quad + |B| - 1 - \mathrm{wt}(\pi_B\,(l)) \\
&\quad + |C| - 1 - \mathrm{wt}(\pi_C\,(l)) \\
&\quad + |D| - \mathrm{wt}(\pi_D\,(l)) \\
&= k - 2 - \mathrm{wt}(\pi_{[k]}\,(l)) \\
&= k - 2 - (w-2) \\
&\geq 2w - 2 - (w-2) \\
&= w.
\end{aligned}$$

Thus at some point, the weight of our vector is w. To prove that $f(l)$ is in F, we use an argument similar to the one used in the previous case. We need only show that $f(l)$ does not equal

$$v = \pi_{[k]}\,(f(l))\,G.$$

Notice that v the vector in V with the same first k digits as $f(l)$. Further Notice that $\pi_{\{k+1,k+2\}}(v)$ is the sum of $\pi_{\{k+1,k+2\}}(l) = 11$ and an even number of each of 00,10, and 01. Thus $\pi_{\{k+1,k+2\}}(v) = 11 \neq 00 = \pi_{\{k+1,k+2\}}(l)$, and so $f(l) \neq v$ and $f(l) \in F$.

By arguments similar to one already given, f is injective when restricted to

$$L_2 = \left\{ l \in L \,:\, \operatorname{wt} \pi_{\{k+1,k+2\}}(l) = 2 \right\}.$$

We've defined $f : L \to F$, and we've shown that it is injective when restricted to L_1 or L_2. On the other hand, given $l_1 \in L_1$, we've seen that if we set

$$v_1 = \pi_{[k]}(f(l_1))\, G,$$

then

$$\operatorname{wt}(\pi_{k+1,k+2}(v_1)) = 1.$$

On the other hand, if we let $l_2 \in L_2$ then we've seen that if we set

$$v_2 = \pi_{[k]}(f(l_2))\, G,$$

then

$$\operatorname{wt}(\pi_{k+1,k+2}(v_2)) = 2.$$

Thus $f(l_1) \neq f(l_2)$, and so f is injective.

We must now handle the case where $|A|$,$|B|$,$|C|$, and $|D|$ are all odd. This time we will delete only the last column of G to produce G', a generator matrix for V'. Since the support of this vector space is at most $k+1$, we may apply Lemma 4.6.4 to establish that $A_w(V') \leq \binom{k}{w}$. Thus if we establish that $A_w(V') \geq A_w(V)$, we are done. Let L be the collection of lost vectors and let F be the collection of found vectors. We will construct an injective function $f : L \to F$.

Let $l \in L$. Define

$$l' = \pi_{[k+1]}(l)\,0,$$

the vector derived from l by replacing the last bit with a zero. Invert the bits of l' one at a time starting in A, then C, then the bit in position $k+1$, then D skipping its last bit, then B. Do not invert the bit in position $k+2$. Stop when the weight becomes w. To see that this weight does eventually become w, define $h(l)$ to be the vector produced by this process if we do not stop when the weight becomes w. Then

$$\begin{aligned}
\mathrm{wt}(h(l)) &= \mathrm{wt}(\pi_A(h(l))) + \mathrm{wt}(\pi_B(h(l))) + \mathrm{wt}(\pi_{C\cup\{k+1\}}(h(l))) + \mathrm{wt}(\pi_D(h(l))) \\
&\geq |A| - \mathrm{wt}(\pi_A(l)) \\
&\quad + |B| - \mathrm{wt}(\pi_B(l)) \\
&\quad + |C \cup \{k+1\}| - \mathrm{wt}(\pi_{C\cup\{k+1\}}(l)) \\
&\quad + |D| - 1 - \mathrm{wt}(\pi_{D\setminus \max D}(l)) \\
&\geq |A| - \mathrm{wt}(\pi_A(l)) \\
&\quad + |B| - \mathrm{wt}(\pi_B(l)) \\
&\quad + |C \cup \{k+1\}| - \mathrm{wt}(\pi_{C\cup\{k+1\}}(l)) \\
&\quad + |D| - 1 - \mathrm{wt}(\pi_D(l)) \\
&= (k+1) - 1 - \mathrm{wt}(\pi_{[k+1]}(l)) \\
&= k - (w-1) \\
&\geq 2w - (w-1) \\
&= w+1.
\end{aligned}$$

As with the other proofs, f is injective. We need only show that $f(l) \in F$. There are two things we must establish: $f(l) \in V'$ and $f(l) \notin V$. To see that $f(l) \in V'$, notice that V' is exactly the collection of vectors in $\mathbb{F}_2^{k+2}$ that are 0 at bit position $k+2$ and have even weight on $C \cup D \cup \{k+1\}$. By construction, $\pi_{k+2}(f(l)) = 0$. The process described above inverts an even number of bits in $C \cup D \cup \{k+2\}$. But since $l \in V$, we have that $\mathrm{wt}(\pi_{C\cup D\cup\{k+2\}}(l))$ is even, and thus so is $\mathrm{wt}(\pi_{C\cup D\cup\{k+2\}}(f(l)))$. To show that $f(l) \notin V$, we need only point out that in V, $k+2$ is a parity-check bit for $B \cup D$. Since $l \in L$, we have that $\pi_{k+2}(l) = 1$. But an even number of bits were inverted in B and in D. Thus the unique vector $v = \pi_{[k]}(f(l))G \in V$ that has $\pi_{[k]}(v) = \pi_{[k]}(f(v))$ has $\pi_{k+2}(v) = 1$, and so $v \neq f(v)$, and $f(v) \notin V'$. □

4.6.2 A Complete Conjecture for the Case Where w is Odd

From empirical evidence, we have the following conjecture.

Conjecture 4.6.6. *If $n, k, w \in \mathbb{N}$ and w is odd then*

$$m(n,k,w) = M(n,k,w).$$

□

Notice that by Theorem 4.1.1 (the formula for $M(n,k,w)$), whenever we have been able to establish exact values for $m(n,k,w)$, they agree with $M(n,k,w)$. In particular, suppose $k \leq w+1$ and $n \geq w+k-1$ (the conditions given in Lemma 4.3.1 that imply $m(n,k,w) = 2^{k-1}$). Either $w \leq n/2$ and (by the first condition above) $k-1 \leq w$, or $w > n/2$, in which case $n-w \leq n/2$, and since $n \geq w+k-1$, we have $k-1 \leq n-w$. Thus by Theorem 4.1.1,

$$m(n,k,w) = 2^{k-1} = M(n,k,w).$$

Furthermore, for $k, w \in \mathbb{N}$ with $k \geq 2w$ and w odd, we have

$$\begin{aligned} m(k,k,w) = m(k+1,k,w) &= m(k+2,k,w) \\ &= \binom{k}{w} \\ &= M(k,k,w) = M(k+1,k,w) = M(k+2,k,w). \end{aligned}$$

If w is odd and n is even then $n - w$ is odd. If Conjecture 4.6.6 is true then we would have

$$m(n,k,w) = M(n,k,w) = M(n,k,n-w) = m(n,k,n-w).$$

In fact, $m(n,k,w)$ does have this symmetry.

Proposition 4.6.7. *If $n, k, w \in \mathbb{N}$ where n is even and w is odd then*

$$m(n,k,w) = m(n,k,n-w).$$

Proof. Let $V < \mathbb{F}_2^n$ be a k-dimensional subspace with $A_w(V) = m(n,k,w)$. There exists $\mathcal{B} = \{b_1, b_2, \ldots, b_k\}$, a basis for V consisting of odd weight vectors (in fact, by Lemma 4.6.3 there is a basis of weight-w vectors). Consider the set of vectors

$$\mathcal{B}' = \left\{ \bar{b} : b \in \mathcal{B} \right\},$$

and let V' be the vector space generated by this collection. Let $v \in V$ have $\mathrm{wt}(v) = w$. There is a unique sequence $\lambda_1, \lambda_2, \ldots, \lambda_k \in \mathbb{F}_2$ such that

$$v = \lambda_1 b_1 + \lambda_2 b_2 + \cdots + \lambda_k b_k.$$

Since v has odd weight and b_i has odd weight for each $i \in [k]$, the number of coefficients $b_1, b_2, \ldots, b_k$ that are 1 is odd. Hence

$$\lambda_1 \overline{b_1} + \lambda_2 \overline{b_2} + \cdots + \lambda_k \overline{b_k} = \overline{v},$$

which has weight $n - w$. Thus $A_{n-w}(V') \geq A_w(V) = m(n, k, w)$. Furthermore, since V' is generated by k vectors, $\dim V' \leq k$. Thus

$$m(n, k, n - w) \geq m(n, \dim V', n - w) \geq m(n, k, w).$$

By symmetry, $m(n, k, w) = m(n, k, n - w)$ as desired. □

Besides the theoretical similarity of these objects, we have tested the conjecture for $n \leq 14$ by brute force.

Bibliography

[1] R. Ahlswede: Simple hypergraphs with maximal number of adjacent pairs of edges, *J. Combinatorial Theory (B)* **28** (1980), 164–167.

[2] R. Ahlswede, H. Aydinian, and L.H. Khachatrian: Extremal problems under dimension constraints, *Discrete Mathematics* **273** (2003), 9–21.

[3] R. Ahlswede, H. Aydinian, and L. Khachatrian: Maximum number of constant weight vertices of the unit n-cube contained in a k-dimensional subspace, *Combinatorica* **23** (2003), 5–22.

[4] R. Ahlswede and L. Khachatrian: The complete intersection theorem for systems of finite sets, *European J. Combin.* **18** (1997), 125–136.

[5] R. Ahlswede and L. Khachatrian: Katona's Intersection Theorem: Four Proofs, *Combinatorica* **25** (1) (2005), 105-110.

[6] B. Bollobás: On generalized graphs, *Acta Math. Acad. Sci. Hungar.* **16** (1965), 447–452.

[7] B. Bollobás: *Combinatorics: Set Systems, Hypergraphs, Families of Vectors, and Combinatorial Probability*, Cambridge Univ. Press, (1986).

[8] B. Bollobás and I. Leader: Compressions and isoperimetric inequalities, *J. Combinatorial Theory (A)* **56** (1991), 47–62.

[9] B. Bollobás and I. Leader: Isoperimetric inequalties and fractional set systems, *J. Combinatorial Theory (A)* **56** (1991), 63–74.

[10] B. Bollobás and I. Leader: Set systems with few disjoint pairs, *Combinatorica* **23** (4) (2003), 559–570.

[11] B. Bollobás *Extremal Graph Theory*, Dover Publications, Incorporated, (2004).

[12] A. Bonisoli: Every equidistant linear code is a sequence of dual Hamming codes, *Ars Combinatorica* **18** (1984), 181–186.

[13] C. Colbourn and J. Dinitz (Eds): *The CRC Handbook of Combinatorial Designs*, CRC Press, Boca Raton, (1996).

[14] V. Chvátal: *Linear Programming*, W. H. Freeman and Company, (1983).

[15] P. Erdős, Chao Ko, and R. Rado: Intersection theorems for systems of finite sets, *Quart. J. Math. (2)* **12** (1961), 313–320.

[16] P. Frankl: On the minimum number of disjoint pairs in a family of finite sets, *J. Combinatorial Theory (A)* **22** (1977), 249–251.

[17] P. Frankl: The shifting technique in extremal set theory, in *Surveys in Combinatorics 1987* (C Whitehead, ed.), London Math. Soc. Lecture Note Series 123, Cambridge University Press (1987), 81–110.

[18] W. C. Huffman and V. Pless: *Fundamentals of error-correcting codes*, Cambridge Univ. Press, (2003).

[19] J. L. W. V. Jensen: Sur les fonctions convexes et les ingalits entre les valeurs moyennes, *Acta Mathematica* **30** (1906), 175-193.

[20] S. Jukna: *Extremal combinatorics : with applications in computer science*, Springer, Berlin, 2001.

[21] G. O. H. Katona: Intersection theorems for systems of finite sets, *Acta Math. Acad. Sci. Hungar.* **15** (1964), 329-337.

[22] D. Lubell: A short proof of Sperner's lemma, *J. Combinatorial Theory* **1** (1966), 299.

[23] F. J. MacWilliams: Combinatorial problems of elementary abelian groups, Ph.D. Thesis, Harvard University, (1962).

[24] F.J. MacWilliams and N.J.A. Sloane: *The theory of Error Correcting Codes*, North-Holland, Amsterdam, (1977).

[25] L. D. Meshalkin: A generalisation of Sperner's theorem on the number of subsets of a finite set (in Russian), *Teor. Probab. Ver. Primen.* **8**, (1963), 219–220; English translation in *Theory of Probab. and its Applns* **8** (1964), 204–205.

[26] S. Radziszowski: Dynamic Survey DS1: Small Ramsey Numbers, *The Electronic Journal of Combinatorics*, (2006).

[27] F. P. Ramsey: On a problem of formal logic, *Proc. Lond. Math. Soc.* **30** (1930), 264-286

[28] E. Sperner: Ein Satz ber Untermengen einer endlichen Menge, *Math. Z.* **27** (1928), 554–548.

[29] J. van Lint and R. Wilson: *A Course in Combinatorics*, Cambridge University Press, Cambridge, (1992).

[30] D.-L. Wang and P. Wang: Discrete isomperimetric problems, *SIAM J. Appl. Math* **32** (1977), 860–870.

[31] K. Yamamoto: Logarithmic order of free distributive lattices, *Math. Soc. Japan* **6**, (1954) 343–353.