Extremal Problems in Codes, Finite Sets and Geometries

Thesis by

Moya Michelle Mazorow

In Partial Fulfillment of the Requirements

for the Degree of

Doctor of Philosophy

California Institute of Technology

Pasadena, California

1991

(Submitted May 21, 1991)

ACKNOWLEDGMENT

I would like first to thank my advisor, R. M. Wilson, for introducing me to the field of Combinatorics, for patiently answering all of my questions as I worked on this thesis, and for his many helpful suggestions and pointers. I also want to thank my husband Dale for encouraging me to continue with my studies. He has provided me with love, hugs, and support during my entire time at Caltech. I dedicate this thesis to my family, Dale and Heather.

Abstract

This thesis covers some extremal problems in the areas of coding theory, finite set systems, and projective geometry. It was completed under the supervision of Professor R. M. Wilson.

Bounds on the dimension of a binary linear code C are derived when constraints are placed on the weights of words in C. It is known if C is a binary linear code of length $a2^\alpha$ and dimension 2^α, then C contains a nonzero word of weight divisible by 2^α. A code of length 18 and dimension 7 is constructed that contains no nonzero word of weight divisible by 6. Let p be an odd prime and α a positive integer. It is shown that if p^α is large, then a code of length $6p^\alpha$ that contains no nonzero words of weight divisible by $2p^\alpha$ has dimension at most $[1.95007]2p^\alpha$. This is a slight improvement over the known bound. For an infinite family of even b, codes of length $3b$ containing no nonzero words of weight divisible by b are constructed whose dimensions are approximately $\frac{11b}{8}$.

Coloring problems on graphs and hypergraphs are also studied. Let $G = K_9$ be the complete graph on 9 vertices. A coloring $C = \{C_i : i \leq 42\}$ of the subgraphs K_4 is constructed with the property that no edge of G is contained in two K_4's of the same color. It is also shown if the edges of K_n are three colored then for large n there are at least $0.4\binom{n}{3}$ triangles whose edges are colored differently.

We consider coloring problems in projective geometry similar to the statement above on triangles. If the points of $\mathrm{PG}(3, q)$ are partitioned into $q + 1$ classes, then there are at most $q^4 + 1$ lines tranverse to the partition. Also included is a much easier result that if the points of a projective $(n-1)$-space of order q are partitioned into $p = \frac{q^{n-1}-1}{q-1}$ classes, then there are at most q^{n-1} hyperplanes that are transverse to the partition. In both cases, up to isomorphism, it is shown that there is a unique partition that achieves the upper bound.

TABLE OF CONTENTS

Introduction and Summary. 1

1. A form for Binary Matrices. 10

2. Restricted Distances in Binary Linear Codes. 21

2. Forbidding Words of Weight about $\frac{1}{2}n$ 30

3. Bounds on $\omega(n, \{n-k, k, n\})$ for $n < 2k$ 37

4. Lower Bounds on $\omega(ab, \{ib : 1 \leq i \leq a\})$ 42

3. Colorings of Sets. 47

2. Packings 51

3. Lifting Packings 54

4. Packings of Points and Pairs 57

5. The Chromatic Number $\chi(2, k, 3k-3)$ 62

6. Some Values of $m(\binom{s}{k}; k, s, n)$ 64

7. Chromatic Triangles 71

4. Projective Geometries. 75

2. Point Colorings 79

3. Balanced Lines 83

4. Projective 3-space, PG$(3, q)$ 95

Bibliography. 104

Introduction and Summary

In this thesis, I present results on extremal problems in binary codes, finite set systems, and finite projective geometry.

The first topic I present concerns binary linear codes, i.e., subspaces of the vector space F^n where $\mathsf{F} = \{0, 1\}$ is the field of two elements. A code C of dimension k is referred to as a $[n, k]$ code. For application purposes, one is interested in the maximum dimension a code C may have subject to the restraint that all codewords in C have weight at least d, (i.e., all codewords contain at least d ones). While it may not be critical for practical error-correcting codes, it is combinatorially interesting to ask for the maximum dimension subject to other weights not occurring.

Let S be a set of disallowed weights. Let $\omega(n, S)$ be the maximum dimension of a binary code none of whose codewords have weight in the set S. Let $\varpi(n, S)$ be the maximum dimension of a binary code none of whose codewords have weight in the set S and which in addition contains at least one word of odd weight. The following two results have been shown in [7].

THEOREM 2.6. *If C is a $[4t, 2t]$ binary linear code, then C has a nonzero codeword $\mathbf{z}$ with $wt(\mathbf{z}) \equiv 0 \pmod{2t}$. In fact, $\omega(4t, \{2t, 4t\}) = 2t - 1$.*

LEMMA 2.18. *For a an odd integer and b a power of 2,*

$$\omega(ab, \{ib : 1 \leq i \leq a\}) = b - 1.$$

Since we are studying linear codes, we may associate to each code a binary matrix whose row space is the code. A parity check matrix of a code C is a matrix whose rows span the dual code of C. Finding a word in a code C of weight w is equivalent to finding a set of w columns of the parity check matrix for C that sum to the zero vector. Naturally then we are led to study matrices. In [7] a form for matrices called binormal form was introduced. It was useful since a $k \times n$ matrix in binormal form has k columns summing to the zero vector. In this paper we generalize binormal form. Before we present the definition we will need some terminology.

Given integers α, i, n satisfying $\alpha i \leq n$, let $\mathbf{f}_i = (f_t)$ be the binary vector of length n where

$$f_t = \begin{cases} 1 & \text{for } (i-1)\alpha + 1 \leq t \leq i\alpha, \\ 0 & \text{otherwise.} \end{cases}$$

For $\alpha k \leq n$ let $\Delta(\alpha, k, n)$ be the $n \times k$ matrix whose columns are the $\mathbf{f}_i$'s.

DEFINITION: A $k \times n$ binary matrix M with $\alpha k \leq n$ for some positive integer α, is in *α-normal form* if

$$M\Delta(\alpha, k, n) = I_k.$$

EXAMPLE. 2-normal form

$$M = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

We develop sufficient and necessary conditions for when a matrix may be brought into α-normal form by row operations and column permutations.

LEMMA 1.2. *Let α be a positive even integer, and let M be a $k \times n$ binary matrix such that $\alpha k \leq n$. If M can be brought into α-normal form by elementary row operations and column permutations, then the all ones vector, $\mathbf{1}_n$, is not in the row space of M.*

THEOREM 1.3. *Let M be a $k \times n$ binary matrix of rank k, and assume that $\alpha k < n$ for some positive integer α. If α is even, assume in addition that $\mathbf{1}_n$ is not in the row space of M. Then M can be brought into α-normal form by elementary row operations and column permutations.*

COROLLARY 1.5. *Let M be a $k \times \alpha k$ binary matrix of rank k for some positive integer α. Then M can be brought into α-normal form by elementary row operations and column permutations if and only if there exists a row of M not orthogonal to $\mathbf{1}_{\alpha k}$ and, additionally, if α is even, $\mathbf{1}_{\alpha k}$ is not in the row space of M.*

Suppose a subset $S \subseteq \{1, \ldots, n-1\}$ satisfies $j \in S$ if and only if $n - j \in S$. Using the results on matrices, I am able to derive upper bounds on codes whose weight set does not intersect the set S. In particular, I show

THEOREM 2.8. *If C is a $[4t+2, 2t+1]$ binary linear code that does not have $\mathbf{1}_{4t+2}$ in its dual, then C has a nonzero codeword $\mathbf{z}$ with $wt(\mathbf{z}) \equiv 0 \pmod{2t+1}$. In fact, $\varpi(4t+2, \{2t+1, 4t+2\}) = 2t$.*

COROLLARY 2.16.

(1) *If b is an odd integer,* $\omega(3b, \{b, 2b, 3b\}) = 2b - 2$;

(2) *If b is an even integer,* $b - 1 \leq \omega(3b, \{b, 2b, 3b\}) \leq 2b - 2$.

Notice in Lemma 2.18 that the lower bound is trivial. So it seems surprising that it is best possible. But if one looks at Theorem 2.6 and Theorem 2.8, both

of these lower bounds are also trivial. In view of Corollary 2.16, it is natural to ask if Lemma 2.18 holds for any even b. In fact it does not. In [7] the authors remarked that I had informed them of this, but they did not list my example. (I was cited under my maiden name Klementis.) The following is an example with $a = 3$ and $b = 6$ for which the bound in Lemma 2.18 fails to hold.

Let C be the [18,7] code which is generated by

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Nonzero words in C have weights in the set $\{1, 2, 3, 8, 9, 10, 11\}$. Thus

$$\omega(18, \{6, 12, 18\}) \geq 7 > 6 - 1.$$

For an infinite family of even b, codes of length $3b$ containing no nonzero words of weight divisible by b are constructed whose dimensions are approximately $\frac{11b}{8}$. Using Theorem 2.6 when b is even and a is odd, one can show that a code of length ab containing no nonzero words of weight divisible by b has dimension at most $\frac{a+1}{2}b - 2$. We improve this bound slightly.

PROPOSITION 2.23. *Let p be an odd prime, α a positive integer, and a an odd integer. If $b = 2p^{\alpha}$, then*

$$\omega(ab, \{ib : 1 \leq i \leq a\}) < \left(\frac{1}{2}\log_2 \frac{(2a)^{2a}}{(2a-1)^{2a-1}} + \frac{\log_2 b - 1}{2b}\right) b.$$

In particular, for large b,

$$\omega(3b, \{b, 2b, 3b\}) \leq 1.95008\, b.$$

The second part of my thesis involves the study of finite sets. Let X be an n-set and $P_k(X)$ the collection of all k-subsets of X. Many problems can be asked concerning the decomposition of $P_k(X)$ into classes each of which has some property. Questions of this form have been posed and investigated before, cf. [4].

A set $P \subseteq P_k(X)$ is called a *packing* of t-sets when every t-subset of X is contained in at most one element of P. A Steiner system $S(t,k,n)$ is a special kind of packing in which every t-set is contained in exactly one element of the packing. What is the minimum number of classes $\chi(t,k,n)$ needed to decompose $P_k(X)$ into classes each of which is a packing of t-sets? This is not a new problem. The case $t = 1$ was handled by Baranyai [4] who showed

LEMMA 1.11 (BARANYAI). *One can partition the k-sets of an n-set into*

$$\left\lceil \binom{n}{k} / \lfloor \frac{n}{k} \rfloor \right\rceil$$

classes in which each element of our n-set occurs at most once.

When the parameters t, k, n are such that an $S(t,k,n)$ exists, investigations have been primarily limited to partitioning $P_k(X)$ into classes each of which is an $S(t,k,n)$, cf. [**8, 9, 13, 14, 20**].

We show

THEOREM 3.9. *If $S(k-1,k,v)$ exists then the following are equivalent.*

(1) *A large set of disjoint $S(k-1,k,v)$ exists;*

(2) $\chi(k-1,k,v) = v-k+1$;

(3) $\chi(k-1,k,v-1) = v-k+1$.

We give constructions showing

$$\chi(2,4,9) = 42;$$

$$\chi(2,5,12) = 264.$$

We also study a related question. Notice that in a partition of $P_k(X)$ into packings of t-sets all k-subsets of a $(2k-t)$-set are in different elements of our partition. Our question then could have been phrased as a coloring problem on hypergraphs. Given a n-set X, define a hypergraph $H = (\mathcal{V}, \mathcal{E})$; $\mathcal{V}$ is the collection of k-sets of $\mathcal{P}$, and $\mathcal{E}$ is the collection of s-sets. A vertex K is on a hyperedge E if $K \subseteq E$.

A *strong* p-coloring of H is a partition $C = \{C_i : i \leq p\}$ of the vertices of H so that every edge E satisfies $\mid C_i \cap E \mid \leq 1$, for all i. An edge with this property is called *polychromatic*. If $s = 2k - t$, then $\chi(t,k,n)$ is the minimum number of colors needed to guarantee the existence of a strong coloring of H.

Instead of varying the number of colors and requiring all s-sets to be polychromatic, one may fix the number of colors and ask for the maximum number of polychromatic s-sets. Let $m(p;k,s,n)$ be the maximum number of polychromatic s-sets over all p-colorings of H. Of course if $p < \binom{s}{k}$, one trivially has $m(p;k,s,n) = 0$. I am interested in $p = \binom{s}{k}$. For example I show the following two results.

COROLLARY 3.15. *Assume* $4 \leq n$, *and* $2 \leq k < \frac{n}{2}$. *Then*

$$m\left(\binom{n-1}{k}; k, n-1, n\right) = 2.$$

COROLLARY 3.17. *Assume* d *is defined by*

$$\left\lfloor \frac{n}{n-k} \right\rfloor = \frac{n-d}{n-k}$$

and that for all t, $0 \leq t \leq d$ *we have* $(n-k-t) \mid (n-d)$. *Then*

$$m\left(\binom{n-1}{k}; k, n-1, n\right) = n - d.$$

For fixed k and s it is shown that the sequence

$$\frac{m(p;k,s,n)}{\binom{n}{s}}$$

is a bounded decreasing sequence. I study its behavior when $p = 3, k = 2$, and $s = 3$. I show for $n \geq 8$ that

$$0.40 \leq \frac{m(3;2,3,n)}{\binom{n}{3}} \leq \frac{4}{7}.$$

I conjecture that

$$\lim_{n\to\infty} \frac{m(3;2,3,n)}{\binom{n}{3}} = 0.40.$$

In the third part of my thesis, I make the natural generalization from questions on sets and subsets to questions on vector spaces and subspaces. In particular one may generalize a coloring of subsets of an n-set to a coloring of subspaces of $\mathcal{P}$, a projective $(n-1)$-space. As for sets I study partitions of the set of k-flats of $\mathcal{P}$, i.e. partitions of the set of projective $(k-1)$-dimensional subspaces. Given a partition, a s-flat is *polychromatic* if no two of its k-subflats lie in the same element of the partition. B. Rothschild and P. Frankl [**18**] asked if one were to partition the points of projective $(n-1)$-space into $q+1$ classes, how many lines would be transverse to this partition. This is the projective space analogue to finding $m(p;1,2,n)$; therefore, let $m_q(p;k,s,n)$ be the maximum number of polychromatic s-flats over all p-colorings of k-flats of a projective $(n-1)$-space of order q. I only study $m_q(\frac{q^s-1}{q-1};1,s,n)$. The results are summarized in Theorem 4.5 and Theorem 4.12. I state them here in words.

If the points of a projective $(n-1)$-space $\mathcal{P}$ of order q are colored with $\frac{q^{n-1}-1}{q-1}$ colors, then there are at most q^{n-1} polychromatic hyperplanes. Up to isomorphism, there is a unique coloring which attains this upper bound.

If the points of $PG(3,q)$ are partitioned into $q+1$ classes, then there are at most q^4+1 polychromatic lines. Up to isomorphism, there is a unique partition that achieves this upper bound.

In proving Theorem 4.12, I actually proved a slightly different result. Instead of coloring the points with $q+1$ colors, they are colored with $r > 1$ colors where r is a divisor of $q+1$. A *balanced* line is a line with equal number of points of each color. The results are summarized in Theorem 4.10 and Theorem 4.11. I state them here in words.

If the points of a projective plane of order q are colored with r colors, then there are at most q^2 balanced lines. Moreover, up to isomorphism, the extremal coloring is unique.

If the points of $PG(3,q)$ are partitioned into r equal size classes, then there are at most q^4+1 balanced lines. Up to isomorphism, there is a unique partition that achieves this upper bound.

Although I originally was studying the situation in Theorem 4.12, I think these two results are worth mentioning.

Let us say how this thesis is organized. In Chapter 1, I develop conditions on a matrix that will be needed to prove the dimension bounds of Chapter 2. The first section of Chapter 2 is devoted to definitions and presentation of terminology and simple results. In Section 2 the disallowed set of weights contains only integers that are approximately half the length of the code. Section 3 and Section 4 are devoted to codes when the restricted weight set is all multiples of some divisor of the length. Upper bounds are developed in Section 3 while lower bounds are constructed in Section 4.

In Section 1 of Chapter 3, I state a coloring problem on sets and develop some bounds. Section 2 summarizes results known on packings. Section 3 concerns when it is possible to lift a coloring on $n-1$ points to one on n points. In Sections 4 and 5, I give various constructions. Section 6 specializes to colorings with p-colors and presents lower and upper bounds for $m(\binom{s}{k}; k, s, n)$ when $k = 1$ and when $s = n - 1$. Section 7 deals with $k = 2$ and $s = 3$.

Section 1 of Chapter 4 is devoted to defining projective spaces. The remaining sections consider point colorings. Section 2 gives constructions of lower bounds on $m_q(s; 1, s, n)$ and shows that the construction is optimal for hyperplanes. In Section 3 bounds are developed that will be needed in Section 4 to prove the results on optimality for polychromatic lines in 2-space and 3-space.

1

A Form for Binary Matrices

We wish to develop a form for matrices that will be helpful in studying the weight distribution of a code. In this section, we wish to familiarize the reader with a form on $(0,1)$-matrices which generalizes one first introduced by Enomoto, Frankl, Ito, and Nomura [7]. The results will be needed in the next section. First we need some terminology.

Let M be a $k \times n$ binary matrix. Throughout this section $\mathbf{r}_i$ or $\mathbf{c}_j$ will always be used to denote the i^{th} row or j^{th} column of M. The *weight* of a binary vector $\mathbf{x}$ is the number of nonzero coordinates of $\mathbf{x}$. For positive integers α and i satisfying $\alpha i \leq n$, we define the i^{th} *block* of M with respect to α as the $k \times \alpha$ submatrix of M whose columns are indexed by $\alpha(i-1)+1, \ldots, \alpha i$. When the choice of α is unambiguous, we denote the i^{th} block by M_i. We have

$$M_i := \begin{pmatrix} | & | & & | \\ \mathbf{c}_{\alpha(i-1)+1} & \mathbf{c}_{\alpha(i-1)+2} & \cdots & \mathbf{c}_{\alpha i} \\ | & | & & | \end{pmatrix}.$$

EXAMPLE 1.1. Blocks of a matrix with respect to $\alpha = 2$.

If

$$M = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \end{pmatrix},$$

then the blocks of M are

$$M_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 1 \\ 1 & 1 \end{pmatrix}, \quad M_2 = \begin{pmatrix} 1 & 1 \\ 1 & 1 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad M_3 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{pmatrix}, \quad M_4 = \begin{pmatrix} 0 & 0 \\ 1 & 1 \\ 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Given integers α, i, n satisfying $\alpha i \leq n$ we denote by $\mathbf{f}_i = \mathbf{f}_i^{(\alpha)}$ the $1 \times n$ matrix with all ones in the i^{th} block and zeros elsewhere. So

$$\mathbf{f}_1 = (1 \quad \ldots \quad 1 \quad 0 \quad \ldots \quad 0 \quad 0 \quad \ldots \quad 0),$$

$$\mathbf{f}_2 = (0 \quad \ldots \quad 0 \quad 1 \quad \ldots \quad 1 \quad 0 \quad \ldots \quad 0),$$

and in general

$$\mathbf{f}_i = (0 \quad \ldots \quad 0 \quad 0 \quad \ldots \quad 0 \quad 1 \quad \ldots \quad 1 \quad 0 \quad \ldots \quad 0).$$

For $\alpha k \leq n$ let $\Delta(\alpha, k, n)$ be the $n \times k$ matrix whose columns are the $\mathbf{f}_i$'s. That is

$$\Delta(\alpha, k, n) := \begin{pmatrix} | & | & & | \\ \mathbf{f}_1^\top & \mathbf{f}_2^\top & \ldots & \mathbf{f}_k^\top \\ | & | & & | \end{pmatrix}.$$

DEFINITION: A $k \times n$ binary matrix M with $\alpha k \leq n$ for some positive integer α, is in *α-normal form* if

$$M\Delta(\alpha, k, n) = I_k.$$

When $\alpha = 2$ we say *binormal form* instead of 2-normal form.

EXAMPLE 1.2. Binormal Form

Let $k = 4$ and $n = 9$. By definition then

$$\Delta(2, 4, 9) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

If

$$M = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \end{pmatrix},$$

then

$$M\Delta(2,4,9) = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \vdots & 0 \\ \vdots & \vdots & \vdots & \ddots & 0 \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}.$$

So M is in binormal form.

EXAMPLE 1.3. 3-Normal Form.

$$A = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Now if $\langle \mathbf{r_i}, \mathbf{f_j} \rangle$ is the standard vector dot product our definition just requires that

$$\langle \mathbf{r_i}, \mathbf{f_j} \rangle \pmod 2 = \delta_{ij} \quad \text{for all } 1 \leq i, j \leq k. \tag{1.1}$$

Equivalently M is in α-normal form when for all j, $1 \leq j \leq k$,

$$\mathbf{c}_{\alpha(j-1)+1} + \mathbf{c}_{\alpha(j-1)+2} + \cdots + \mathbf{c}_{\alpha j} = \mathbf{e}_j = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \tag{1.2}$$

where e_j is the binary vector of whose only nonzero entry is in the j^{th} coordinate.

Once a form has been defined one usually wants to find the sufficient and necessary conditions for when M is row equivalent to a matrix in that form. For

our purposes though the order of the columns is unimportant. We will instead find sufficient and necessary conditions on a matrix M so that there exists column permutations and elementary row operations that transform M into a matrix M' in α-normal form. To this end let us make the following observation.

LEMMA 1.1. *Let α be a positive integer. A $k \times n$ binary matrix with $\alpha k \leq n$ can be brought into α-normal form by elementary row operations and column permutations if and only if there exists a partition of the multiset of columns into $k+1$ sets $S_1, S_2, \ldots, S_{k+1}$ such that:*

(a) $|S_i| = \alpha$ *for* $1 \leq i \leq k$;

(b) $\left\{\mathbf{t}_i = \sum_{\mathbf{c} \in S_i} \mathbf{c} : 1 \leq i \leq k\right\}$ *forms a basis for the column space of the matrix.*

PROOF: The forward direction is trivial. For the other direction let M be the given matrix. By permuting the columns one can consider M to have S_1 as its first block, S_2 as its second block, etc. Let T denote the matrix whose columns are $\mathbf{t}_1, \mathbf{t}_2, \ldots, \mathbf{t}_k$. Since these columns are independent there exists row operations to transform T into the identity matrix; i.e. there exists A such that $AT = I_k$. Let $M^* = AM$. If the i^{th} block of M^* is S_i^*, then $S_i^* = \{A\mathbf{c} : \mathbf{c} \in S_i\}$. Thus the columns in the i^{th} block of M^* sum to $A\mathbf{t}_i = e_i$. It follows from (1.2) that the matrix M^* is in α-normal form. □

In Example 1.2, it is evident that the all ones vector is not in the row space of M. When α is even this is always true.

LEMMA 1.2. *Let α be a positive even integer, and let M be a $k \times n$ binary matrix such that $\alpha k \leq n$. If M can be brought into α-normal form by elementary row operations and column permutations, then the all ones vector $\mathbf{1}_n$ is not in the row space of M.*

PROOF: Let M' be the matrix in α-normal form obtained from M by performing elementary row operations and column permutations. If $\mathbf{1}_n$ were in the row space of M, $\mathbf{1}_n$ is in the row space of M' too; hence, we may assume our matrix is in α-normal form. Now if $\mathbf{1}_n$ were in the row space there would exist a nonempty set I so that $\mathbf{1}_n = \sum_{i \in I} \mathbf{r}_i$. Since α is even by choosing $j \in I$ we find

$$\langle \mathbf{1}_n, \mathbf{f}_j \rangle = \alpha \equiv 0 \pmod 2,$$

but

$$\sum_{i \in I} \langle \mathbf{r}_i, \mathbf{f}_j \rangle = \langle \mathbf{r}_j, \mathbf{f}_j \rangle \equiv 1 \pmod 2.$$

We remark that this argument does not hold when α is odd. □

THEOREM 1.3. *Let M be a $k \times n$ binary matrix of rank k, and assume that $\alpha k < n$ for some positive integer α. If α is even, assume in addition that $\mathbf{1}_n$ is not in the row space of M. Then M can be brought into α-normal form by elementary row operations and column permutations.*

Notice that Lemma 1.2 and Theorem 1.3 together give sufficient and necessary conditions for being able to bring a $k \times n$ binary matrix of rank k, $n > \alpha k$ for some positive integer α, into α-normal form by elementary row operations and column permutations. We will postpone the proof until later so that we may state some corollaries. Corollary 1.4 for the case $\alpha = 2$ appeared in [7]. Corollary 1.5 gives sufficient and necessary conditions when $n = \alpha k$.

COROLLARY 1.4. *Let M be a $k \times n$ binary matrix of rank k with $n > \alpha k$ for some even integer α. If n is odd and M has all even weight rows, then M can be brought into α-normal form by elementary row operations and column permutations.*

PROOF: The sum of even weight binary vectors has even weight. Now as all our rows have even weight and as n is odd, $\mathbf{1}_n$ cannot be in the row space of M; consequently, Theorem 1.3 implies M can be brought into α-normal form by elementary row operations and column permutations. □

COROLLARY 1.5. *Let M be a $k \times \alpha k$ binary matrix of rank k for some positive integer α. Then M can be brought into α-normal form by elementary row operations and column permutations if and only if there exists a row of M not orthogonal to $\mathbf{1}_{\alpha k}$ and, additionally, if α is even, $\mathbf{1}_{\alpha k}$ is not in the row space of M.*

PROOF:

($\Rightarrow$) Let M' be the matrix in α-normal form equivalent to M. Now by definition of α-normal form we know that the columns of M' sum to $\mathbf{1}_{\alpha k}$ which in particular implies each row of M' contains an odd number of ones. Now if all rows of M had even weight, elementary row operations and column permutations would not affect this; thus the rows of M' would all have even weight. So some row of M has odd weight. In addition, when α is even, it follows from Lemma 1.2 that $\mathbf{1}_{\alpha k}$ is not in the row space of M.

($\Leftarrow$) If $k = 1$ the single row of M has an odd number of ones; moreover, when α is even it has at least one zero. The statement is then immediate from Lemma 1.1. So we assume $k \geq 2$. Notice that the parity of the sum of two binary vectors is odd if and only if the vectors had different parities. Now we have assumed that we have at least one row of odd weight. By elementary row operations we may then assume that the first $k-1$ rows of M have even weight and that the last row has odd weight. Notice then that the columns of M sum to $\mathbf{e}_k$. If the k^{th} row is never added to the previous rows, then column permutations and row

operations do not affect the column sum. By Theorem 1.3, the submatrix of M formed by its first $k-1$ rows can be brought into α-normal form.

If for some j, $1 \leq j \leq k-1$, the k^{th} row of the j^{th} block has odd weight, add the j^{th} row to the k^{th} row. Thus (1.1) implies

$$\langle \mathbf{r}_i, \mathbf{f}_j \rangle \pmod 2 = \delta_{ij} \quad \text{for all } 1 \leq i \leq k,\ 1 \leq j \leq k-1.$$

For $1 \leq i \leq k$, let $\mathbf{t}_i$ denote the sum of the columns in the i^{th} block of M. We have therefore that $\mathbf{t}_i = \mathbf{e}_i$ for $1 \leq i \leq k-1$. It follows that $\mathbf{t}_k = \mathbf{1}_k$. Therefore the set $\{\mathbf{t}_1, \ldots, \mathbf{t}_k\}$ is an independent set of k vectors. By Lemma 1.1, M can be brought into α-normal form by elementary row operations and column permutations. □

It is evident from Corollary 1.5 and Theorem 1.3 that:

COROLLARY 1.6. *Let M be a $k \times \alpha k$ binary matrix for some even integer α that can be brought into α-normal form by elementary row operations and column permutations. Then M can be brought into s-normal form by elementary row operations and column permutations for all positive integers $s \leq \alpha$.*

Our motivation for introducing α-normal form was to study the weight distribution of codes. So far we have said nothing on how these may be connected to codes. We do so now. The following was shown in [7]. We include the proof for completeness.

LEMMA 1.7. *Let M be a $k \times n$ binary matrix $2k \leq n$ in binormal form. For each binary k-tuple $\mathbf{x}$, there exists a unique binary k-tuple $\mathbf{y}$ such that $\mathbf{x} = \sum_{i=1}^{k} \mathbf{c}_{2i-y_i}$ where the $\mathbf{c}_j$'s are the columns of M. In particular there exists k columns of M summing to the vector of all zeros, $\mathbf{0}_k$.*

Notice in particular this shows M has rank k. It also shows that the dual of the row space contains a word of weight k. This is why binormal form is useful in studying codes with restricted weight sets.

PROOF: Assume M is in binormal form. There are 2^k ways to choose a k-tuple of columns of M so that there is exactly one column from each of the k blocks of M. We need only show that for each distinct choice of this k-tuple we obtain a distinct sum. To this end suppose we have two different k-tuples. Since they are different there is some i so that in the i^{th}-block the columns chosen are different. Now in the i^{th} row the entries in the two columns of the j^{th} block are the same when $j \neq i$. We conclude that the sum over our two different k-tuples must differ in the i^{th} coordinate. □

When α is even any matrix that may be brought into α-normal form may also be brought into binormal form. In the modified matrix there are k columns summing to $\mathbf{0}$. This is unaffected by row operations. Column permutations simply change which columns sum to $\mathbf{0}$. We have shown:

COROLLARY 1.8. *Let M be a binary $k \times n$ matrix with $\alpha k \leq n$ for some even integer $\alpha \geq 2$. Then if M can be brought into α-normal form there exists k columns of M which sum to $\mathbf{0}_k$.*

We conclude this chapter with the proof of Theorem 1.3.

PROOF OF THEOREM 1.3: As mentioned before, Corollary 1.4 for the special case of $\alpha = 2$ was proven in [7]. The proof of Theorem 1.3 is similiar to that proof. Let $M = (m_{i,j})$ satisfy the hypothesis. Proceed by induction on k.

$k = 1$: Now $\text{rank}(M) = 1$ implies that the only row of M has a nonzero number of ones. If α is even, we know also that the only row of M has at least one zero

as $\mathbf{1}_n$ is not in the row space of M. The result follows since $\alpha < n$.

$k \geq 2$: Suppose the theorem has been proven for lesser values of k, and let us now show it holds for k. If all the rows of M have even weight, then the columns of M sum to $\mathbf{0}_k$. If not there is at least one row of odd weight. By elementary row operations, we may assume that the first $k-1$ rows of M have even weight and that the k^{th} row has odd weight. Notice then that the columns of M sum to $\mathbf{e}_k$ in this case. In either case by applying our induction hypothesis to the $(k-1) \times n$ submatrix of M formed from the first $k-1$ rows of M we may assume that this submatrix is in α-normal form. Now since the k^{th} row is never added to the previous rows, the sum of the columns remains $\mathbf{e}_k$ when M contains an odd weight row and $\mathbf{0}_k$ otherwise. We proceed in a manner similiar to the proof of Corollary 1.5. If for some j, $1 \leq j \leq k-1$, the k^{th} row of the j^{th} block has odd weight, add the j^{th} row to the k^{th} row. We have then

$$\langle \mathbf{r_i}, \mathbf{f_j} \rangle \pmod 2 = \delta_{ij} \quad \text{for all } 1 \leq i \leq k,\ 1 \leq j \leq k-1.$$

For $1 \leq i \leq k$ let $\mathbf{t}_i$ denote the sum of the columns in the i^{th} block of M. So $\mathbf{t}_i = \mathbf{e}_i$ for $1 \leq i \leq k-1$. Let $\mathbf{b}_i$ be a vector of length $n - \alpha(k-1)$ whose j^{th} entry is $m_{i,\alpha(k-1)+j}$. Notice that the above remarks imply that

$$\mathrm{wt}(\mathbf{b}_i) \equiv 1 \pmod 2 \qquad \text{for } 1 \leq i \leq k-1;$$

and

$$\mathrm{wt}(\mathbf{b}_k) \equiv \begin{cases} 0 \pmod 2 & \text{if all rows of } M \text{ have even weight} \\ 1 \pmod 2 & \text{if some row of } M \text{ has odd weight.} \end{cases} \tag{1.3}$$

Now $\mathbf{b}_k$ is a $1 \times (n - \alpha(k-1))$ matrix with $n - \alpha(k-1) > \alpha$. If $\mathbf{b}_k$ satisfies the hypothesis of Theorem 1.3, there exists a permutation of the columns of

$\mathbf{b}_k$ bringing $\mathbf{b}_k$ into α-normal form. By applying this same permutation to the columns of M beyond the $\alpha(k-1)^{st}$ column, we find that $\mathbf{t}_k$ is some vector whose k^{th} entry is one. Therefore the set $\{\mathbf{t}_1, \ldots, \mathbf{t}_k\}$ is an independent set of k vectors. The proof is then completed by appealing to Lemma 1.1. It suffices then to consider only the following two cases.

CASE I: $\mathrm{wt}(\mathbf{b}_k) = n - \alpha(k-1)$ and α is even.

Since α is even, the vector of all ones is not in the row space of M; therefore, there must exist at least one zero in the k^{th} row of M. After performing any necessary block permutations and row permutations we may assume by (1.1) that $\langle \mathbf{r}_k, \mathbf{f}_i \rangle \pmod 2 = 0$ for $1 \leq i \leq k-1$ and that $m_{k,\alpha(k-1)} = 0$.

If $\mathbf{b}_{k-1} \neq \mathbf{1}_{n-\alpha(k-1)}$, then $\mathbf{b}_{k-1}$ satisfies the hypothesis of Theorem 1.3 so there exists a permutation of the columns fixing the first $\alpha(k-1)$ columns such that the first α columns of $\mathbf{b}_{k-1}$ have odd weight. This forces $\mathbf{t}_k$ to be a vector with a one as its $(k-1)^{st}$ entry and a zero as its k^{th} entry. Permuting columns $\mathbf{c}_n$ and $\mathbf{c}_{\alpha(k-1)}$ leaves $\mathbf{t}_i$ unchanged for $i \neq k-1, 1 \leq i \leq k$ but changes $\mathbf{t}_{k-1}$ to a vector having a one as its k^{th} entry. The set $\{\mathbf{t}_i : 1 \leq i \leq k\}$ is an independent set of k vectors.

If $\mathbf{b}_{k-1} = \mathbf{1}_{n-\alpha(k-1)}$, then by permuting columns $\mathbf{c}_{\alpha k}$ and $\mathbf{c}_{\alpha(k-1)}$ leaves $\mathbf{t}_i$ unchanged for $1 \leq i \leq k-2$ but changes $\mathbf{t}_{k-1}$ and $\mathbf{t}_k$. Let $\epsilon = m_{k-1,\alpha(k-1)}$ then both $\mathbf{t}_{k-1}$ and $\mathbf{t}_k$ have a one as their k^{th} entry, but $\mathbf{t}_{k-1}$ has ϵ as its $(k-1)^{st}$ entry while $\mathbf{t}_k$ has $\epsilon+1$ as its $(k-1)^{st}$ entry. We again find that the set $\{\mathbf{t}_i : 1 \leq i \leq k\}$ is an independent set of k vectors.

CASE II: $\mathrm{wt}(\mathbf{b}_k) = 0$.

Since $\mathrm{rank}(M) = k$, we have from (1.3) that all rows of M have even weight and that there exists at least one nonzero entry in the k^{th} row of M. After

performing any necessary block permutations and row permutations we may assume that $\langle \mathbf{r}_k, \mathbf{f}_i \rangle \pmod 2 = 0$ for $1 \leq i \leq k-1$, $m_{k,\alpha(k-1)} = 1$, and that the first entry of $\mathbf{b}_{k-1}$ is one.

If the first α columns of $\mathbf{b}_{k-1}$ have odd weight, then $\mathbf{t}_k$ is a vector with a one as its $(k-1)^{st}$ entry and a zero as its k^{th} entry. Permuting columns $\mathbf{c}_n$ and $\mathbf{c}_{\alpha(k-1)}$ leaves $\mathbf{t}_i$ unchanged for $i \neq k-1, 1 \leq i \leq k$ but changes $\mathbf{t}_{k-1}$ to a vector having one as its k^{th} entry. The set $\{\mathbf{t}_i : 1 \leq i \leq k\}$ is an independent set of k vectors.

On the other hand if the first α columns of $\mathbf{b}_{k-1}$ have even weight, then permuting columns $\mathbf{c}_{\alpha(k-1)+1}$ and $\mathbf{c}_{\alpha(k-1)}$ leaves $\mathbf{t}_i$ unchanged for $1 \leq i \leq k-2$ but changes $\mathbf{t}_{k-1}$ and $\mathbf{t}_k$. Let $\epsilon = m_{k-1,\alpha(k-1)}$ then both $\mathbf{t}_{k-1}$ and $\mathbf{t}_k$ have a one as their k^{th} entry, but $\mathbf{t}_{k-1}$ has ϵ as its $(k-1)^{st}$ entry while $\mathbf{t}_k$ has $\epsilon + 1$ as its $(k-1)^{st}$ entry. We again find that the set $\{\mathbf{t}_i : 1 \leq i \leq k\}$ is an independent set of k vectors. □

2

Restricted Distances in Binary Linear Codes

Let $\mathsf{F} = \mathbb{Z}_2$ be the finite field on two elements. The set of binary n-tuples form an n-dimensional vector space over F which we will denote by F^n. A binary vector in F^n is often refered to as a *word* and will be written $\mathbf{x} = (x_i : 1 \leq i \leq n)$. We will let $\mathbf{1}_n$ and $\mathbf{0}_n$ denote the n-tuple of all ones and all zeros, respectively. The *weight* of a word $\mathbf{x}$ is the number of coordinates of $\mathbf{x}$ which are nonzero:

$$\mathrm{wt}(\mathbf{x}) = |\{i : x_i \neq 0\}|.$$

The *Hamming distance* between two words

$$\mathbf{x} = (x_1, \ldots, x_n) \text{ and } \mathbf{y} = (y_1, \ldots, y_n)$$

is defined to be the number of coordinates in which they differ:

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

If $\mathbf{x} \cdot \mathbf{y} = \sum_1^n x_i y_i$ is the standard vector dot product over $\mathbb{R}$, then $\mathbf{x} \cdot \mathbf{y}$ is the number of nonzero coordinates in which the words $\mathbf{x}$ and $\mathbf{y}$ agree. Remembering that $-1 = +1 \pmod 2$, we find

$$d(\mathbf{x}, \mathbf{y}) = \mathrm{wt}(\mathbf{x} + \mathbf{y}) = \mathrm{wt}(\mathbf{x}) + \mathrm{wt}(\mathbf{y}) - 2(\mathbf{x} \cdot \mathbf{y}).$$

The parity of $\mathrm{wt}(\mathbf{x}+\mathbf{y})$ is even if and only if the parities of the weights of $\mathbf{x}$ and $\mathbf{y}$ are the same. Let F_e^n denote the collection of even weight vectors; notice this is an $(n-1)$-dimensional subspace of F^n.

The dual $C^\perp$ of a subset $C \subseteq \mathsf{F}^n$ is the set of vectors orthogonal to C:

$$C^\perp = \{\mathbf{y} \in \mathsf{F}^n : \mathbf{x} \cdot \mathbf{y} \equiv 0 \pmod 2 \text{ for all } \mathbf{x} \in C\}.$$

Notice that the dual of a set C is always a linear subspace.

An arbitrary subset $C \subseteq \mathsf{F}^n$ is called a *code* of length n over F. Elements in C are called *codewords*. The *minimum distance* d of a code C is the minimum distance occurring between distinct codewords:

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

For a fixed binary code C the *weight set* $W(C) \subseteq \{1,\ldots,n\}$ is the set of all positive integers which are weights of nonzero codewords in C:

$$W(C) = \{\mathrm{wt}(\mathbf{x}) : \mathbf{x} \in C \setminus \{0\}\}.$$

Similiarly we define the *distance set* $D(C) \subseteq \{1,\ldots,n\}$ by

$$D(C) = \{d(\mathbf{x},\mathbf{y}) : \mathbf{x},\mathbf{y} \in C, \mathbf{x} \neq \mathbf{y}\}.$$

More generally coordinates of the vectors can be taken from any alphabet instead of from $\mathbb{Z}_2$. When the alphabet has cardinality q, the codes are called q-ary codes. We will only be considering binary codes. When the alphabet chosen is $\mathrm{GF}(q)$, the finite field on q elements, many of our initial observations with slight modifications in the terminology remain true. The proof of our main results, however, do not generalize to the nonbinary case.

Codes were originally developed to correct errors that occurred when information was sent across a less than perfect channel. Suppose one wishes to send M messages from earth to a camera located on a satellite. To accomplish this you associate to each message a set of binary vectors. This set represents how you might encode your message. For many purposes this is just a single element. The receiver must have a method for determining which message was sent given a string of 0's and 1's that has been received. Since you want to be able to distinguish messages, vectors of length at least $\log_2 M$ are needed. When these messages are transmitted across space it is possible occasionally that a single bit will flip say from a 0 to a 1. One wants to encode the messages so that, even if errors occur, the receiver will correctly interpret the message. Let C be your set of encoded messages. Suppose the minimum distance in C is at least $2e+1$. Then for every two distinct codewords $\mathbf{c}, \mathbf{y}$ we have

$$\{\mathbf{z} : d(\mathbf{z}, \mathbf{c}) \leq e\} \cap \{\mathbf{z} : d(\mathbf{z}, \mathbf{y}) \leq e\} = \emptyset.$$

In other words, the spheres of radius e about codewords do not intersect. To decode the message, the receiver simply chooses the codeword closest to the received word. If fewer then e-errors occurred, the message is correctly interpreted. In view of this, an e-error correcting code is a code C with minimum distance $d \geq 2e+1$.

SPHERE-PACKING BOUND. *Let C be an e-error correcting code then*

$$|C| \sum_{i=0}^{e} \binom{n}{i} \leq 2^n.$$

An e-error correcting binary code that achieves this bound is said to be *perfect.*

PROOF: Count the number of ordered pairs $(\mathbf{x}, \mathbf{c})$ where $\mathbf{c}$ is a codeword and $\mathbf{x}$ is a word whose distance from $\mathbf{c}$ is at most e. Since the spheres of radius e do not

intersect this number is at most the total number of words which is 2^n. Given a codeword $\mathbf{c}$ any word at distance i from it is obtained by flipping i of its bits; there are $\binom{n}{i}$ different ways to do this. So the number of words contained in the sphere of radius e about $\mathbf{c}$ is $\sum_{i=0}^{e}\binom{n}{i}$. □

The above is an example of a more general phenomena. If we in any way restrict the weight set or distance set of a code, we have limited the choice of codewords we may have and have therefore imposed restrictions on the cardinality of the code.

We will restrict our attention to a special class of codes, the so called *linear* codes. In this case the set C is required to be a linear subspace of $\mathbb{F}^n$. If C is a linear subspace of dimension k, we say C is a $[n,k]$ code. Notice the dual of C is a $[n,n-k]$ code. We will assume all of our codes are linear. Notice then that the weight set and the distance set of C are equal.

Let S be a set of disallowed weights. We want to find the maximum dimension of a binary linear code of length n whose codewords satisfy $\mathrm{wt}(\mathbf{c}) \notin S$ for all codewords $\mathbf{c}$. For any set $S \subseteq \{1,\ldots,n\}$, we wish to investigate

$$\omega(n,S) = \max\{\dim(C) : C \subseteq \mathbb{F}^n, W(C) \cap S = \emptyset\}.$$

In this new terminology the sphere packing bound becomes

$$\omega(n,\{1,\ldots,2e\}) \leq n - \log_2\left(\sum_{i=1}^{e}\binom{n}{i}\right).$$

Equality is possible only if there exists a perfect binary linear e-error correcting code.

The set of all even weight words in $\mathbb{F}^n$ form a $(n-1)$-dimensional code whose weight set by definition does not include any odd integers. It is then evident that

$$\textit{If } S \subseteq \{1,3,5,\ldots,2\left\lfloor\frac{n+1}{2}\right\rfloor - 1\}, \textit{ then } \omega(n,S) = n-1.$$

With S as above, any code C whose codewords all have even weight will satisfy $W(C) \cap S = \emptyset$. We wish to study codes that contain words of odd weight and that satisfy $W(C) \cap S = \emptyset$. Let E_n be the set of even integers less than or equal to n; i.e.,

$$E_n = \left\{2, 4, \ldots, 2\left\lfloor \frac{n}{2} \right\rfloor\right\}.$$

Let

$$\varpi(n, S) = \max\{\dim(C) : C \subseteq \mathsf{F}^n, W(C) \cap S = \emptyset, W(C) \not\subseteq E_n\}.$$

A code with dimension $\omega(n, S)$ and whose weight set intersects S trivially will be called an *extremal configuration* for $\omega(n, S)$. An extremal configuration for $\varpi(n, S)$ is defined similiarly. To prove lower bounds for these functions we must construct codes containing no words in the disallowed set. In the study of ϖ, we must also show the code has a word of odd weight.

Given one code it is possible to construct other codes in several simple ways. Given a code C of length n, by adjoining m zeros to all elements in a code C, we can view C to be a code of length $n + m$ for any nonnegative integer m. If we apply a permutation to the coordinates of codewords in C, we obtain a possibly different code. These codes are considered *equivalent*, and we will not make any distinction between them. We may *extend* a code C of length n to a code of length $n + 1$ by appending a parity check bit to all codewords. By adding a parity check bit to each codeword, we mean adding a 0 or 1 as necessary so that the weight of the codeword is even. This does not affect the dimension of the code, but it does affect the weight set. Alternatively we may *puncture* a code of length n at any coordinate by removing this coordinate to obtain a code of length $n - 1$.

EXAMPLE 2.1. [7,4] HAMMING CODE AND EXTENDED [8,4] HAMMING CODE.

The Hamming [7,4] code C_1 is the row space of the matrix

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

This is a perfect code. From the definition it is evident that the extended Hamming code $\overline{C_1}$ is a dimension 4, length 8 code which is the row space of the matrix

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

The weight set of $\overline{C_1}$ is $\{4, 8\}$.

EXAMPLE 2.2. [23,12] GOLAY CODE AND [24,12] EXTENDED GOLAY CODE. Let C^* be the code obtained from C_1 by reading the coordinates from right to left. Let $\overline{C^*}$ be the extended code of C^*. The code

$$G(24, 12) := \{(\mathbf{a} + \mathbf{x}, \mathbf{b} + \mathbf{x}, \mathbf{a} + \mathbf{b} + \mathbf{x}) : \mathbf{a}, \mathbf{b} \in \overline{C_1}, \mathbf{x} \in \overline{C^*}\}$$

is a [24,12] code with weight set

$$W = \{8, 12, 16, 24\}.$$

For details on this construction see [**21**]. For alternate constructions see [**15, 16**]. If we puncture this code at any coordinate, we obtain a new code of length 23 whose dimension remains 12. This is the [23,12] binary Golay code; it is a perfect code. If we extend this code we get back the code $G(24, 12)$.

Now suppose we wanted a code C of length 8 with no words of weight 4 or 8. Clearly then C has no words in common with the extended Hamming code of

length 8. Thus the space spanned by C and $\overline{C_1}$ has dimension equal $\dim(C)+4$. So C has dimension at most 4. We will use binormal form developed in the previous chapter to show in fact that C has dimension at most 3.

We would like to make a series of observations on the behavior of the functions ω and ϖ. Notice it is immediate that

$$\varpi(n,S) \leq \omega(n,S). \tag{2.1}$$

LEMMA 2.1. *If $m \geq n$ are positive integers, and $S \subseteq \{1,\ldots,n\}$, then*

(1) $\omega(m,S) \leq m-n+\omega(n,S)$;

(2) $\varpi(m,S) \leq m-n+\varpi(n,S)$.

PROOF: We proceed by induction. Notice that both statements are true for $m=n$. We consider an upper bound first for $\omega(m,S)$. Assume the result has been shown for codes of length $m-1$. Let C be a binary linear code of length m satisfying $W(C)\cap S=\emptyset$. Let

$$C_m = \{\mathbf{v}=(v_1,\ldots,v_{m-1}) : (v_1,\ldots,v_{m-1},0)\in C\}.$$

The dimension of C_m is at most one less than the dimension of C. Furthermore, since $W(C_m)\cap S=\emptyset$, our induction hypothesis implies that

$$\dim(C_m) \leq m-1-n-\omega(n,S).$$

Let $m>n$ and assume the result on ϖ has been shown for codes of length $m-1$. Let C be a binary linear code with length m and dimension $m-n+1+\varpi(n,S)$. Assume C contains at least one word of odd weight and satisfies $W(C)\cap S=\emptyset$. Since $\dim(C)\geq 2$, there exists a word $\mathbf{c}$ of odd weight that is not the vector of all ones. Choose i a coordinate of $\mathbf{c}$ such that $c_i=0$. Let

$$C_i = \{(v_1,\ldots,v_{i-1},v_{i+1},\ldots,v_m) : (v_1,\ldots,v_{i-1},0,v_{i+1},\ldots,v_m)\in C\}.$$

Clearly C_i contains a word of odd weight and satisfies $W(C_i) \cap S = \emptyset$. Repeating our argument above we arrive at a contradiction. □

LEMMA 2.2. *Let $n \leq m$ and $S \subseteq U \subseteq \{1, \ldots, n\}$ and $T \subseteq \{n+1, \ldots, m\}$ be given. Then*

(1) $\omega(n, S) \leq \omega(m, S \cup T)$;

(2) $\varpi(n, S) \leq \varpi(m, S \cup T)$;

(3) $\omega(n, U) \leq \omega(n, S)$;

(4) $\varpi(n, U) \leq \varpi(n, S)$.

PROOF: Let C be a extremal configuration. We may view C as a code of length m by adding on $m-n$ zeros to the end of each codeword. The codewords in this new code C' all have weight at most n; thus, it satisfies $W(C') \cap (S \cup T) = \emptyset$. The last two are immediate. □

LEMMA 2.3. *Let $S \subseteq \{1, 2, \ldots, n\}$ and let e represent the least even integer in S and m the least integer in S, then*

(1) $m - 1 \leq \varpi(n, S)$;

(2) $\max\{m-1, e-2\} \leq \omega(n, S)$.

PROOF: The set of all even weight words of length $e-1$ form a $(e-2)$-dimensional code. The set of all vectors of length $m-1$ form a $(m-1)$-dimensional code. The weight set of both codes intersect the set S trivially. The result follows from Lemma 2.2. □

PROPOSITION 2.4. *Let $S \subseteq E_n$ and suppose that C is a binary linear code of length n such that $W(C) \cap S = \emptyset$ then either $\dim(C) < \omega(n, S)$ or $\mathbf{1}_n \notin C^{\perp}$.*

PROOF: If $\mathbf{1}_n \in C^{\perp}$, then all codewords have even weight. For any odd weight word $\mathbf{x}$ the code generated by C and $\mathbf{x}$ has dimension $1 + \dim(C)$. Since the

sum of a word of even weight and a word of odd weight has odd weight, our new code has no new words of even weight. We thus have created a code of a higher dimension whose weight set intersects the set S trivially. □

Putting this together with (2.1) we have

(2.2) *If* $S \subseteq E_n$ *then,* $\omega(n,S) = \varpi(n,S)$.

LEMMA 2.5. *Let* n *be a positive integer. Let* $S \subseteq \{1,2,\ldots,n-1\}$ *satisfying* $j \in S$ *if and only if* $n-j \in S$. *Then*

(1) $\varpi(n, S \cup \{n\}) + 1 \leq \varpi(n,S)$;

(2) $\omega(n, S \cup \{n\}) = \omega(n,S) - 1$;

(3) *if* n *is even, then* $\varpi(n, S \cup \{n\}) = \varpi(n,S) - 1$.

PROOF: Let C be a code of length n with $W(C) \cap (S \cup \{n\}) = \emptyset$. Since $\mathbf{1}_n \notin C$ the code C_1 generated by C and $\mathbf{1}_n$ has dimension $\dim(C)+1$. Assume $W(C_1) \cap S$ is nonempty. Then there exists $j \in S$ such that either $j \in W(C)$ or $n-j \in W(C)$. Our hypothesis on S implies that $n-j \in S$. So $j \in W(C) \cap S$ or $n-j \in W(C) \cap S$. This contradicts our choice of C. Therefore $W(C_1) \cap S = \emptyset$. We have shown $\dim(C)+1 \leq \omega(n,S)$. If $W(C) \not\subseteq E_n$, then $W(C_1) \not\subseteq E_n$ which implies $\varpi(n, S \cup \{n\}) + 1 \leq \varpi(n,S)$. Let C be a code of length n with $W(C) \cap S = \emptyset$. Let C_2 be the subcode of C that does not contain $\mathbf{1}_n$. Now $\dim(C) - 1 \leq \dim(C_2)$ and $W(C_2) \cap (S \cup \{n\}) = \emptyset$. Suppose that C contains a word of odd weight. When n is even, removing the even weight vector of all ones does not change this. □

Let C be a $[n,k]$ binary code. Then we may choose a set of k generators for C. Any $k \times n$ matrix G whose row space equals, C is called a *generator matrix* for C. Conversely, given a $k \times n$ $(0,1)$-matrix G, its row space is called the code

generated by G. If G has rank k then the code generated is a $[n, k]$ code. A *parity check matrix* for C is a matrix H which is a generator matrix for the dual code of C. From the definition of the dual we know $HG^t = 0$. So

$$C = \{\mathbf{x} \in \mathsf{F}^n : H\mathbf{x}^t = 0\}.$$

From this it is evident that C conmtains a word of weight w if and only if there exist w columns of H summing to zero.

We can find information then about weight distributions by observing properties about parity check matrices. We wish to make use of binormal form as presented in Chapter 1. If M is a $k \times n$ binary matrix $2k \leq n$ that can be brought into binormal form by elementary row operations and columns permutations, then by Corollary 1.8 there exists k columns of M that sum to the vector of all zeros. In other words if C is the code whose parity check matrix is M, then C contains a word of weight k.

2. Forbidding Words of Weight about $\frac{1}{2}n$.

We are interested in determining ω or ϖ when our codes have length $2b$ and contain no words of weight b. The case b a positive even integer was investigated in [7]. There results are cited below as Theorem 2.6, Corollary 2.7 and the case k even in Theorem 2.10. We provide an alternative proof for Theorem 2.7. Theorem 2.8 considers the case where b is odd. We postpone the proofs of Theorem 2.6, Theorem 2.8 and Theorem 2.10 so that we may state some corollaries.

THEOREM 2.6. *If C is a $[4t, 2t]$ binary linear code, then C has a nonzero codeword $\mathbf{z}$ with $wt(\mathbf{z}) \equiv 0 \pmod{2t}$. In fact, $\omega(4t, \{2t, 4t\}) = 2t - 1$.*

COROLLARY 2.7.

$$\omega(4t, \{2t\}) = 2t;$$

$$\omega(n, \{2t\}) = 2t - 1 \qquad \text{for } 2t - 1 \leq n < 4t;$$

$$\omega(n, \{2t\}) \leq n - 2t \qquad \text{for } 4t \leq n.$$

PROOF: The first statement follows from Lemma 2.5. The lower bound for the second statement comes from Lemma 2.3, while the upper bound is a consequence of Lemma 2.2 where $S = \{2t\}$ and $T = \{4t\}$. Lemma 2.1 immediately implies the last statement. □

Now we have already noticed that $\omega(4t + 2, \{2t + 1\}) = 4t + 1$. So in the case where b is odd we should study ϖ instead of ω.

THEOREM 2.8. *If C is a $[4t + 2, 2t + 1]$ binary linear code that does not have $\mathbf{1}_{4t+2}$ in its dual, then C has a nonzero codeword $\mathbf{z}$ with $wt(\mathbf{z}) \equiv 0 \pmod{2t+1}$. In fact, $\varpi(4t + 2, \{2t + 1, 4t + 2\}) = 2t$.*

COROLLARY 2.9. *Let $t \geq 1$ then*

$$\varpi(4t + 2, \{2t + 1\}) = 2t + 1;$$

$$\varpi(n, \{2t + 1\}) = 2t \qquad \text{for } 2t \leq n < 4t + 2;$$

$$\varpi(n, \{2t + 1\}) \leq n - 2t - 1 \qquad \text{for } 4t + 2 \leq n.$$

PROOF: The proof follows the same lines as the proof of Corollary 2.7. □

THEOREM 2.10. *If $k \geq 2$ then*

$$\omega(2k, \{k, k - 1\}) = k - 1; \tag{2.3}$$

$$\omega(2k, \{k, k + 1\}) = k - 1. \tag{2.4}$$

Since for k even this was noted in [7], we will only include the proof here for k odd. As above by appealing to Lemmas 2.1, 2,2, and 2.3 we find:

COROLLARY 2.11. *If $k \geq 2$ then*

$$\omega(n, \{k, k+1\}) = k - 1 \qquad \text{for } k - 1 \leq n < 2k;$$

$$\omega(n, \{k, k+1\}) \leq n - k - 1 \qquad \text{for } 2k \leq n;$$

$$\omega(n, \{k-1, k\}) \leq n - k - 1 \qquad \text{for } 2k \leq n.$$

COROLLARY 2.12. *If $k \geq 2$ then*

$$\omega(2k-1, \{k-1, k\}) = k - 1;$$

$$\omega(2k-1, \{k-1, k, 2k-1\}) = k - 2;$$

$$\omega(n, \{k-1, k\}) = k - 2 \qquad \text{for } k - 1 \leq n \leq 2k - 2.$$

PROOF: Notice that Lemma 2.1 combined with Theorem 2.10 tells us $\omega(2k-1, \{k-1, k\}) \leq k - 1$. For the lower bound, let

$$C = \{\mathbf{v} = (v_i) \text{ such that } v_{k-1} = v_k = \cdots = v_{2k-1}\}.$$

This code has weight set $W(C) = \{1, 2, \ldots, k-2, k+1, \ldots, 2k-1\}$ and dimension $k - 1$. This proves the first part. Now this together with Lemma 2.5 shows

$$\omega(2k-1, \{k-1, k, 2k-1\}) = k - 2.$$

Now for the third part we know by Lemma 2.3 that there exists a code of dimension $k - 2$ with no words of weight $k - 1$ or k. From Lemma 2.2,

$$\omega(n, \{k-1, k\}) \leq \omega(2k-1, \{k-1, k, 2k-1\}).$$

□

LEMMA 2.13. *Let t be a positive odd integer, then*

$$\omega(2t, \{t-1\}) \leq t;$$
$$\omega(2t, \{t+1\}) = t.$$

PROOF: If t is an odd positive integer and C a $[2t, t+1]$ binary code, then there exists a $[2t, t]$ subcode D of C containing only even weight words. So D has no words of weight t. By Theorem 2.10 then D contains a word of weight $t-1$ and a word of weight $t+1$. The lower bound is trivial. □

COROLLARY 2.14. *Let t be a positive odd integer, $t \equiv 3 \pmod 4$ then*

$$\omega(2t, \{t-1\}) = t.$$

PROOF: By Lemma 2.13, it suffices to construct a lower bound. Let C be the code generated by the set $\{\mathbf{w}_i : 1 \leq i \leq t-2\} \cup \{\mathbf{z}\}$ where

$$\mathbf{w}_i = (v_j) \quad v_j = \begin{cases} 1 & \text{when } j \in i, t-2+i, 2t-3, 2t-2, \\ 0 & \text{otherwise,} \end{cases}$$

and

$$\mathbf{z}_i = (v_j) \quad v_j = \begin{cases} 0 & \text{when } j \in t-1, t, \ldots, 2t-3, \\ 1 & \text{otherwise.} \end{cases}$$

C is generated by

$$\begin{pmatrix} I_{t-2} & I_{t-2} & \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{0} \\ \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{1} \end{pmatrix}.$$

Now C is a $[2t, t-1]$ code with $W(C) = \{t+1\} \cup \{4u : 1 \leq u \leq \frac{t-1}{2}\}$. Since $t-1 \equiv 2 \pmod 4$ we conclude $W(C) \cap \{t-1\} = \emptyset$. The code C has only even weight words. Since t is odd $t-1$ is even. Adding any word with odd weight to C increases the dimension by one and does not add any new even weight words.

□

We conclude this section with the proofs of Theorems 2.6, 2.8, and 2.10.

PROOF OF THEOREM 2.6: The lower bound follows from Lemma 2.3. To prove the upper bound assume that C is a $[4t, 2t]$ binary linear code. If $\mathbf{1}_{4t} \in C$, we are done so assume not. The dual code is also a $[4t, 2t]$ code. We distinguish two cases.

CASE I: $\mathbf{1}_{4t} \notin C^{\perp}$.

By Corollary 1.5, the generating matrix of $C^{\perp}$ can be put into binormal form. Therefore by Corollary 1.8 there exists $2t$ columns of the parity check matrix of C summing to $\mathbf{0}_{2t}$. There exists a word of weight $2t$ in C.

CASE II: $\mathbf{1}_{4t} \in C^{\perp}$.

Let $\mathbf{y}_1, \ldots, \mathbf{y}_{2t}$ be a basis for C. Then as all codewords have even weight $\mathbf{e}_1 \notin C$. Let D be the code generated by $\mathbf{e}_1, \mathbf{y}_1, \ldots, \mathbf{y}_{2t-1}$. Now a codeword of D has even weight if it is in C; otherwise, it is of the form $\mathbf{e}_1 + \mathbf{c}$ for some codeword $\mathbf{c} \in C$. In which case it would have odd weight. Since $\mathbf{1}_{4t} \notin C$ clearly $\mathbf{1}_{4t} \notin D$. Also it is immediate that $\mathbf{1}_{4t} \notin D^{\perp}$. The code D then satisfies the conditions of Case I, so it contains a word of weight $2t$. Since $2t$ is even the word must actually lie in C. □

PROOF OF THEOREM 2.8: Let C be a $[4t+2, 2t+1]$ binary linear code with $\mathbf{1}_{4t+2} \notin C^{\perp}$. If $\mathbf{1}_{4t+2} \in C$, we are done so assume $\mathbf{1}_{4t+2} \notin C$. We can then apply Corollary 1.5 to the parity check matrix of C. Since the parity check matrix of C can be brought into binormal form, Corollary 1.8 implies there exists a word of weight $2t+1$ in C. Hence $\varpi(4t+2, \{2t+1, 4t+2\}) \leq 2t$. The lower bound follows from Lemma 2.3. □

PROOF OF THEOREM 2.10: To obtain the lower bounds consider the code C

where

$$C = \{(v_1, \ldots, v_{2k}) : v_{k-1} = v_k = \cdots = v_{2k}\}.$$

The code C is a $[2k, k-1]$ binary linear code with no words of weight $k, k-1$, or $k+1$. Naturally if we succeed in proving our assertion then by appealing to Lemma 2.2, we will have shown:

$$\omega(2k, \{k-1, k, k+1\}) = k-1.$$

When k is even the results have been shown in [7] so we will only consider the case where k is odd. To complete the proof of (2.3), it suffices to show that if C is a $[2k, k]$ binary linear code then C contains a word of weight k or $k-1$, while for (2.4) we need a word of weight k or $k+1$. Let C be a $[2k, k]$ binary linear code with k odd. It suffices to consider the following three cases.

CASE I: $\mathbf{1}_{2k} \notin C$ and $\mathbf{1}_{2k} \notin C^{\perp}$.

Theorem 2.8 implies C has a word of weight k.

Case II: $\mathbf{1}_{2k} \in C^{\perp}$.

Let $\mathbf{y}_1, \ldots, \mathbf{y}_k$ be a basis for $C^{\perp}$. Then as $\mathbf{1}_{2k} \in C^{\perp}$ we may assume that $\mathbf{y}_k = \mathbf{1}_{2k}$. Let D be the code generated by $\mathbf{y}_1, \ldots, \mathbf{y}_{k-1}$, and let M be a generating matrix of the code D. Now M is a $k-1$ by $2k$ binary matrix of rank $k-1$ that does not have $\mathbf{1}_{2k}$ in its row space. Therefore as M satisfies the hypothesis of Theorem 1.3, it may be brought into binormal form by elementary row operations and columns permutations.

Let $\mathbf{a}$ be the sum of the two columns of M "left over" after putting M into binormal form. Let A be the matrix formed after performing the elementary row operations needed to bring M into binormal form, and let $\mathbf{c}_i$ and $\mathbf{c}_j$ be the

above distinguished columns of A. Notice that A also generates D. By Lemma 1.7 there exists a set S_1 of $k-1$ columns of A summing to $\mathbf{0}_{k-1}$, and a set S_2 of $k-1$ columns of A summing to $\mathbf{a}$. Since we are dealing with binary vectors, the sum of columns in the set $S = S_2 \cup \{\mathbf{c}_i, \mathbf{c}_j\}$ is $\mathbf{0}_{k-1}$. Now the matrix M' formed by adjoining a row of all ones to the bottom of A is a generating matrix of $C^{\perp}$. As k is odd, observe that the columns of M' corresponding to the columns of A in the sets S_1 and S sum to 0_k in M'. Since M' is a parity check matrix of C, the code C contains a word of weight $k-1$ and a word of weight $k+1$.

CASE III: $\mathbf{1}_{2k} \in C$ and $\mathbf{1}_{2k} \notin C^{\perp}$.

Let $\mathbf{y}_1, \ldots, \mathbf{y}_k$ be a basis for C. Then as $\mathbf{1}_{2k} \in C$, we may assume that $\mathbf{y}_k = \mathbf{1}_{2k}$. Let D be the subcode of C generated by $\mathbf{y}_1, \ldots, \mathbf{y}_{k-1}$, and let M be the generating matrix of the dual code of D. Now M is a $(k+1) \times 2k$ binary matrix of rank $k+1$ with at least one row not orthogonal to $\mathbf{1}_{2k}$. Let M' be the matrix formed from M by adjoining two columns of zeros. Clearly there exists at least one row of M' not orthogonal to $\mathbf{1}_{2k}$. Since M' contains a column of zeros, M' does not have $\mathbf{1}_{2k+2}$ in its row space. As M' then satisfies the hypothesis of Corollary 1.5, it may be brought into binormal form by elementary row operations and columns permutations. By Corollary 1.8, there exists $k+1$ columns of M' summing to $\mathbf{0}_{k+1}$. So depending on whether or not the columns of zeros were used there exist $k, k-1$, or $k+1$ columns of M summing to $\mathbf{0}_{k+1}$. Thus, by the definition of M, there exists a word $\mathbf{z} \in D \subseteq C$ with $\mathrm{wt}(\mathbf{z}) \in \{k, k-1, k+1\}$. If $\mathrm{wt}(\mathbf{z}) = k \pm 1$, then $\mathrm{wt}(\mathbf{1}_{2k} + \mathbf{z}) = k \mp 1$. The word $\mathbf{1}_{2k} + \mathbf{z}$ is in C. $\square$

3. Bounds on $\omega(n, \{n-k, k, n\})$ for $n < 2k$.

In Section 2, we have investigated the case $n = 2k$ namely $\omega(2k, \{k, 2k\})$. We would like to use these results to consider what happens when $n < 2k$. The value of ω depended on among other things whether or not k was even or odd. So we will necessarily need to distinguish cases.

PROPOSITION 2.15. *Let t be a positive integer, and let n be an integer satisfying $2t+1 \leq n < 4t$.*

(1) *If n is odd,* $\omega(n, \{n-2t, 2t, n\}) = 2t-2$;

(2) *If n is even,* $n-2t-1 \leq \omega(n, \{n-2t, 2t, n\}) \leq 2t-2$.

PROOF: Let C be a $[n, 2t-1]$ binary linear code with no words of weight $n-2t, 2t$ or n. By adding zero coordinates, we may view $A = \langle C, \mathbf{1}_n \rangle$ as a code of length $4t$. Since it has dimension $2t$, Theorem 2.6 implies there is a word in A of weight $2t$ or $4t$. There is clearly no word of weight $4t$; thus, the code A contains a word of weight $2t$. This word cannot be in C so it must be of the form $\mathbf{c} + \mathbf{1}_n$ for some $\mathbf{c} \in C$. But then C contains a word of weight $n-2t$. The lower bound follows from Lemma 2.3. □

It is immediate then that by choosing $t = b$ and $n = 3b$ that

COROLLARY 2.16.

(1) *If b is an odd integer,* $\omega(3b, \{b, 2b, 3b\}) = 2b-2$;

(2) *If b is an even integer,* $b-1 \leq \omega(3b, \{b, 2b, 3b\}) \leq 2b-2$.

PROPOSITION 2.17. *Let t be a positive integer, and let n be an integer satisfying $2t+2 \leq n < 4t+2$. Then*

$$n-2t-2 \leq \varpi(n, \{n-2t-1, 2t+1, n\}) \leq 2t-1;$$

furthermore, when n is odd,

$$n - 2t - 2 \leq \omega(n, \{n - 2t - 1, 2t + 1, n\}) \leq 2t - 1.$$

PROOF: Let C be a $[n, 2t]$ binary linear code with no words of weight $n - 2t - 1, 2t + 1$ or n. Proceed as in the proof of Proposition 2.15. If n is even, assume C contains a word of odd weight. If n is odd, the word $\mathbf{1}_n$ has odd weight. The code A is a $[4t + 2, 2t + 1]$ code which contains a word of odd weight. By appealing to Theorem 2.8 we reach a contradiction. As before, the lower bound follows from Lemma 2.3. □

Using a result called Olson's Theorem [**17**] on elementary p-groups, it has been shown [**7**] that

LEMMA 2.18. *For a an odd integer and b a power of 2,*

$$\omega(ab, \{ib : 1 \leq i \leq a\}) = b - 1.$$

One can ask the question,"What happens if b is only required to be even?" The technique does not generalize if b is not a power of 2. In fact we can exhibit cases of dimension $\approx \frac{11b}{8}$ when $a = 3$. The first case of interest is $b = 6$. Let us first introduce an intermediate code. Consider the set

$$A_4 = \{f : GF(16) \to GF(2) : f \text{ a linear transformation}\}.$$

The coordinates of binary vectors of length 15 can be indexed by the nonzero elements of GF(16); therefore, by identifying f with the images under f of nonzero elements we may view A_4 as a binary code of length 15. Since GF(16) is a 4-dimensional vector space over Gf(2), we have that A_4 is a [15,4] code. All nonzero vectors in A_4 have weight 8. Let

$$C := \{(\mathbf{w}_1, \mathbf{w}_2) : \mathbf{w}_1 \in A_4, \mathbf{w}_2 \in \mathsf{F}^3\}.$$

If $\mathbf{z}_1, \mathbf{z}_2, \mathbf{z}_3$, and $\mathbf{z}_4$ are generators for A_4, then C is generated by

$$\mathbf{z}_1, \mathbf{z}_2, \mathbf{z}_3, \mathbf{z}_4, \mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3.$$

The weight set of C is $W(C) = \{1, 2, 3, 8, 9, 10, 11\}$. We have shown

$$7 \leq \omega(18, \{6, 12, 18\}).$$

This does not fit the pattern of Lemma 2.18.

We have seen in Corollary 2.16, that

$$\text{If } b \text{ is odd, then } \omega(3b, \{b, 2b, 3b\}) = 2b - 2,$$

which is also nothing like the situation in Lemma 2.18. In fact when b is odd this is typical.

PROPOSITION 2.19. *If $a \geq 3$ and $b \geq 3$ are odd integers, then*

$$2b - 2 \leq \omega(ab, \{ib : 1 \leq i \leq a\}) \leq \frac{a+1}{2}b - 2.$$

PROOF: Let $k = \frac{a+1}{2}b$. By Lemma 2.2,

$$\omega(ab, \{ib : 1 \leq i \leq a\}) \leq \omega(ab, \{k, ab - k, ab\}).$$

If $a \equiv 1 \pmod 4$, then k is odd. The proof is completed by letting $k = 2t + 1$ in Propositon 2.17. If $a \equiv 3 \pmod 4$, then k is even in which case the proof is completed by letting $k = 2t$ in Proposition 2.15. The lower bound is the trivial lower bound we found in Lemma 2.3. □

The value of $\omega(ab, \{ib : 1 \leq i \leq a\})$ apparently depends on the exact value of a and on how b factors; the primary differences seem to concern b's factors of 2.

PROPOSITION 2.20. *Let b be a positive even integer and $a \geq 3$ an odd integer, then*

$$b - 1 \leq \omega(ab, \{ib : 1 \leq i \leq a\}) \leq \frac{a+1}{2}b - 2.$$

PROOF: The proof is identical to the proof of Proposition 2.19. We need only notice that since b is even, $k = \frac{a+1}{2}b$ is even. The lower bound is the trivial bound found in Lemma 2.3. □

When a and b are even it follows from Lemma 2.2 and Theorem 2.6 that

$$\omega(ab, \{ib : 1 \leq i \leq a\}) \leq \omega(ab, \{\frac{ab}{2}, ab\}) = \frac{ab}{2} - 1.$$

We would like an upper bound on $\omega(ab, \{ib : 1 \leq i \leq a\})$ that is essentially a multiple of b that improves the upper bound of Proposition 2.20.

In [**7**] it was shown:

LEMMA 2.21. *Suppose that $n = ab$ where b is a power of an odd prime and a is even. If C is a code of length n such that $D(C) \cap \{2ib : 1 \leq i \leq a/2\} = \emptyset$, then*

$$|C| \leq 2\sum_{i=0}^{b-1} \binom{n-1}{i}.$$

It is immediate then that

COROLLARY 2.22. *Let α and a be positive integers, and let p be an odd prime. Then for $b = 2p^\alpha$*

$$\omega(ab, \{ib : 1 \leq i \leq a\}) \leq \log_2 \left(2\sum_{i=0}^{p^\alpha - 1} \binom{ab-1}{i} \right). \tag{2.5}$$

The proof of Lemma 2.21 makes use of the following bound appearing in [**10**].

THEOREM (FRANKL). *Suppose $k = p^\alpha$, for p an odd prime, $\alpha \geq 1$. Let C be a code of length ℓ such that $k \nmid w$ for all $w \in D(C)$. Then*

$$|C| \leq \sum_{0 \leq i \leq k-1} \binom{\ell}{i}. \tag{2.6}$$

In his paper, the author conjectured that (2.6) holds for all positive integers k.

By taking the base two logarithm of this we would get a bound on the maximum dimension of a linear code which contains no codewords of weights congruent to 0 (mod p^α).

PROPOSITION 2.23. *Let p be an odd prime, α a positive integer, and a an odd integer. If $b = 2p^\alpha$, then*

$$\omega(ab, \{ib : 1 \le i \le a\}) < \left(\frac{1}{2}\log_2 \frac{(2a)^{2a}}{(2a-1)^{2a-1}} + \frac{\log_2 b - 1}{2b}\right) b.$$

In particular, for large b,

$$\omega(3b, \{b, 2b, 3b\}) \le 1.95008\, b.$$

PROOF: In Corollary 2.22 we found that

$$\omega(ab, \{ib : 1 \le i \le a\}) \le \log_2 \left(2 \sum_{i=0}^{p^\alpha - 1} \binom{ab-1}{i}\right) \le \log_2 \left(2p^\alpha \binom{ab-1}{p^\alpha - 1}\right).$$

It suffices to show that this last quantity is bounded above by

$$\left(\frac{1}{2}\log_2 \frac{(2a)^{2a}}{(2a-1)^{2a-1}} + \frac{1}{4}\frac{\log_2 p^\alpha}{p^\alpha}\right) 2p^\alpha.$$

Let d denote the difference:

$$d := \left(\frac{1}{2}\log_2 \frac{(2a)^{2a}}{(2a-1)^{2a-1}} + \frac{1}{4}\frac{\log_2 p^\alpha}{p^\alpha}\right) 2p^\alpha - \log_2 \left(2p^\alpha \binom{ab-1}{p^\alpha - 1}\right).$$

The binomial coefficient can be estimated using Stirling's formula for a positive integer k:

$$k! e^k = (k^k \sqrt{2\pi k})(1 + \epsilon_k)$$

where ϵ_k monotonically decreases to 0 as $k \to \infty$. Therefore:

$$\binom{m}{k} = \frac{m^m}{k^k (m-k)^{m-k}} \sqrt{\frac{m}{2\pi k(m-k)}} \frac{1+\epsilon_m}{(1+\epsilon_k)(1+\epsilon_{m-k})}.$$

We assume that $m > k$. Since ϵ_k is a decreasing function in k, we have

$$\frac{1+\epsilon_m}{(1+\epsilon_k)(1+\epsilon_{m-k})} \leq \frac{1+\epsilon_k}{(1+\epsilon_k)(1+\epsilon_{m-k})} = \frac{1}{1+\epsilon_{m-k}} < 1.$$

For ease of notation, let

$$\epsilon = \frac{1+\epsilon_{2at-1}}{(1+\epsilon_{t-1})(1+\epsilon_{2at-t})}.$$

Then since $\log x$ is an increasing function in x, we have

$$d > \log_2 \sqrt{a(2a-1)\pi} + p^\alpha \log_2(1 - \frac{1}{p^\alpha}) - \log_2 \epsilon.$$

Since $p^\alpha \geq 3$, the second term in the above expression is an increasing function in p^α. Thus

$$d > \log_2 \sqrt{15\pi} + \log_2 \frac{8}{27} > 1.$$

□

4. Lower Bounds on $\omega(ab, \{ib : 1 \leq i \leq a\})$.

The case b odd was handled by Corollary 2.16, the case b a power of 2 by Lemma 2.18. In this section we provide lower bounds on $\omega(ab, \{ib : 1 \leq i \leq a\})$ for even b. In particular we provide infinite families of even b which fail to satisfy Lemma 2.18. To prove lower bounds it suffices to exhibit a code of the desired dimension whose weight set does not intersect the particular set in question. Let us introduce some codes (see **[15, 16, 21]** that will be used to build codes of length $3b$.

(1) Let A_m be the code generated by the $m \times (2^m - 1)$ matrix whose columns are the nonzero binary vectors of length m. A_m is a $[2^m - 1, m]$ binary

linear code of constant nonzero weight 2^{m-1}. Its dual is the $[2^m - 1, 2^m - 1 - m]$ Hamming code.

(2) Let $G(24, 12)$ be the extended Golay code of length 24 and dimension 12 which we presented in Example 2.2. It is known that its weight set is $\{8, 12, 16, 24\}$. Let $G'(24, 12)$ be a subcode of $G(24, 12)$ of dimension 11 that does not contain the vector of all ones.

First of all, we would like to generalize our construction of the code of length 18 that did not meet the bound in Lemma 2.18.

PROPOSITION 2.24. *For* $2 \leq r \leq \frac{2^{m-1}+1}{3}$ *and* $m \geq 3$, *let* $b = 2^{m-1} - r$. *Then*

$$b + m - 2r + 1 \leq \omega(3b, \{b, 2b, 3b\}).$$

So if $m - 2r + 2$ is positive, we have exhibited an even b that fails to satisfy Lemma 2.18.

PROOF: Consider the code

$$C := \{(\mathbf{w}_1, \mathbf{w}_2) : \mathbf{w}_1 \in A_m, \mathbf{w}_2 \text{ any vector of length } 2^{m-1} - 3r + 1\}.$$

A nonzero word in A_m has weight 2^{m-1}. The weight set of C is then

$$W(C) = \{i, 2^{m-1} + i : 0 \leq i \leq 2^{m-1} - 3r + 1\}.$$

□

PROPOSITION 2.25.

$$13 \leq \omega(30, \{10, 20, 30\}).$$

Let $b \geq 18$ *be a positive integer such that* $b \equiv 2 \pmod 8$, *then*

$$\frac{11b - 14}{8} \leq \omega(3b, \{b, 2b, 3b\}).$$

PROOF: Write $b = 8r + 2$. Consider the code

$C := \{(\mathbf{w}_1, \ldots, \mathbf{w}_{r+1}) :$

$$\mathbf{w}_i \in G'(24, 12) \text{ for } 1 \leq i \leq r, \mathbf{w}_{r+1} \in \{\mathbf{0}_6, (1, 1, 1, 0, 0, 0)\}\}.$$

Its words have weight congruent to $0, 3 \pmod 4$ and are smaller than $16r+3 < 2b$. When $b = 10$ use $G(24, 12)$ in place of $G'(24, 12)$. □

PROPOSITION 2.26. *If $b \geq 14$ is a positive integer such that $b \equiv 6 \pmod 8$, then*

$$\frac{11b - 26}{8} \leq \omega(3b, \{b, 2b, 3b\}).$$

PROOF: Write $b = 8r + 6$. Consider the code

$$C := \{(\mathbf{w}_1, \ldots, \mathbf{w}_{r+2}) :$$

$$\mathbf{w}_i \in G'(24, 12) \text{ for } 1 \leq i \leq r, \mathbf{w}_{r+1} \in A_4, \mathbf{w}_{r+2} \in \{\mathbf{0}_3, (0, 0, 1)\}\}.$$

Nonzero codewords in C have weight congruent to $0, 1 \pmod 4$. The largest weight is $16r + 9 < 2b$. □

PROPOSITION 2.27. *Let b be a positive odd integer, $b \geq 3$. If $5b = 7t + m$ for $0 \leq m < 7$. Then*

$$\frac{15b - 3m}{7} \leq \omega(5b, \{b, 2b, 3b, 4b, 5b\}) \leq 3b - 2;$$

furthermore, if $b > 3, b \equiv 3 \pmod 4$ and $m \neq 0$ we have,

$$\frac{15b + 7 - 3m}{7} \leq \omega(5b, \{b, 2b, 3b, 4b, 5b\}) \leq 3b - 2.$$

PROOF: Let

$$C := \{(\mathbf{v}_1, \ldots, \mathbf{v}_t, \mathbf{0}_m) : \mathbf{v}_i \in A_3\}.$$

Now C is a $[7t+m, 3t]$ binary linear code whose weight set is

$$W(C) = \{4w : 1 \leq w \leq t\}.$$

Since $4b > 4t$, we have $4b \notin W(C)$. Since b is odd, this is sufficient to show $W(C) \cap \{b, 2b, 3b, 4b, 5b\} = \emptyset$. Now if $b \equiv 3 \pmod 4$ and $m \neq 0$, consider the code generated by C and $(\mathbf{0}_{7t}, \mathbf{v})$ where $\mathbf{v}$ is a word of length m and weight 1. All of our additional codewords have weight $w \equiv 1 \pmod 4$, the largest of which has weight $4t+1$. Now $4t+1 < 4t + \frac{7+3m}{5} \leq 3b$. The last inequality follows since $b \geq 11$ implies $t \geq 7$. Our new code then has no words of the undesired weights.

□

By using $G(24, 12)$ viewed as a code of length 25, we have

$$12 \leq \omega(25, \{5, 10, 15, 20, 25\}) \leq 13.$$

These lower bounds are all at least $2b$. From Lemma 2.2, we immediately find then

COROLLARY 2.28. *Let $a \geq 5$ and b be positive odd integers, then*

$$2b \leq \omega(ab, \{ib : 1 \leq i \leq a\}).$$

From our constructions in Proposition 2.25 and Proposition 2.26 we know we can construct codes of length $n = 3b$ where $b = 2p^\alpha$ for p an odd prime and $\alpha \geq 1$ for which the dimension is $\approx \frac{11b}{8}$. In view of Proposition 2.23, we see there is room for improvement.

We conclude with some questions.

(1) Is $\omega(18, \{6, 12, 18\}) = 8$ or 7?

(2) For $a = 3$ and $b = 2p^\alpha$, do we in fact have that $\omega(3b, \{b, 2b, 3b\}) < \frac{3b}{2}$ or possibly $\omega(3b, \{b, 2b, 3b\}) \approx \frac{ab}{2}$?

(3) For $a \geq 5$ and b as above, can we construct a code close to the upper bound?

(4) For a general odd a and a general even b is it true that $\omega(ab, \{ib : 1 \leq i \leq a\}) < \frac{ab}{2}$?

3

Colorings of Sets

Let $k, s,$ and n be positive integers. Let X be an n-set, and let $V = P_k(X)$ be the set of all k-subsets of X. For p a positive integer a *p-coloring* of V is a partition $C = \{C_i : i \leq p\}$ of the k-sets of X. A k-set A has color i if $A \in C_i$. Unless stated otherwise we will assume all elements of our partition are nonempty; thus, $p \leq \binom{n}{k}$. With respect to C an s-set S is *polychromatic* if no two k-subsets of S have the same color, i.e., $|S \cap C_i| \leq 1$ for all i. A coloring for which all s-sets are polychromatic is called a *strong* coloring on s-sets. Given an integer p, we wish to p-color the k-sets of X so as to maximize the number of polychromatic s-sets; let $m(p; k, s, n)$ be this maximum. Let $\gamma(k, s, n)$ be the minimum number of colors needed so that every s-set is polychromatic. We remark that we have just defined a vertex coloring of a hypergraph whose vertices are the k-sets of X and whose hyperedges are the s-sets of X.

Our primary interest is not in the study of $\gamma(k, s, n)$, but in the study of the function $m(\binom{s}{k}; k, s, n)$. We mention γ because $m(\binom{s}{k}; k, s, n) = \binom{n}{s}$ if and only if $\gamma(k, s, n) = \binom{s}{k}$, and because historically much time has been devoted to finding $\gamma(k, s, n)$ for specific choices of our parameters.

Strong $\gamma(k, k+2, n)$-colorings are useful in constructing codes of constant weight and minimum distance 4, cf. [**5, 8, 9**]. For the coding question, one wishes to have most of the color classes being as large as possible. The question

posed here differs slightly since we wish to minimize the number of colors with no restrictions imposed on the cardinality of the color classes. In this chapter, we develop some bounds on $\gamma(k,s,n)$. We also construct partitions to find exact values of $\gamma(k,s,n)$. Many of these bounds and constructions may be found in [5].

Notice that the study of $\gamma(k,s,n)$ is uninteresting if $k=s$ or $s=n$. Also since for $s \geq 2k$ every pair of distinct k-sets can be completed to an s-set, this case is also uninteresting. We have just seen:

PROPOSITION 3.1.

$$\binom{s}{k} \leq \gamma(k,s,n) \leq \binom{n}{k};$$

$$\gamma(k,s,n) = \begin{cases} 1 & \text{if } k=s, \\ \binom{n}{k} & \text{if } s=n, \\ \binom{n}{k} & \text{if } 2k \leq s. \end{cases}$$

We will assume that $2 \leq k < s < \min\{2k,n\}$. Define t to be the difference $2k-s$. Now for any two A and B we have $|A \cup B| = |A| + |B| - |A \cap B|$. This implies that $|A \cap B| \geq t$ if and only if $|A \cup B| \leq s$. It is evident then that a coloring of the k-subsets of X is a strong coloring of the s-sets if and only if no two k-sets of the same color intersect in t or more points.

Let G be the graph whose vertices are the k-subsets of X. Two vertices are adjacent if and only if their set intersection is at least t. We find then that our question is equivalent to the classical problem of finding the polychromatic number of the graph G; i.e., finding the minimum number of colors needed to color the vertices of G so no two vertices of the same color are adjacent. A *proper* coloring of G is a coloring of the vertices so that no edge has both ends the same color. Let $\chi(t,k,n)$ be the polychromatic number of G. We have then that for

$2 \leq k < s = 2k - t < \min\{2k, n\}$

$$\chi(t,k,n) := \gamma(k, 2k-t, n) \geq \binom{2k-t}{k}.$$

Assume C is a proper coloring of G. This imposes restrictions on the individual elements C_i of our partition. We will say that a t-set is *covered* by C_i if it is a subset of some element of C_i. In a proper coloring of G a t-set can be covered by at most one element of C_i for each i. Each t-set is contained in $\binom{n-t}{k-t}$ sets of size k; therefore, it is evident that

$$\chi(t,k,n) \geq \binom{n-t}{k-t}.$$

Let C be a proper coloring of G. The coloring C induces other colorings. The complement of the coloring C is the partition of $(n-k)$-sets of X formed by assigning a set A the color of its complement A^c. The external structure of C at x is the partition of k-sets of $X \setminus \{x\}$ obtained from C by removing from elements of C all blocks on x. Notice that C is a proper coloring of the graph whose vertices are the k-subsets of X where two vertices are adjacent if and only if their intersection is at least $t+1$. The contraction of C at a point $x \in X$ is a coloring of $(k-1)$-sets of the set $X \setminus \{x\}$. A block B is of color i if and only if $B \cup \{x\}$ is in C_i. Sets of the same color then intersect in no more than $t-1$ points.

By considering these partitions we have shown:

LEMMA 3.2.

$$\chi(t,k,n) = \chi(n-2k+t, n-k, n);$$

$$\chi(t,k,n) \geq \chi(t,k,n-1);$$

$$\chi(t-1,k,n) \geq \chi(t,k,n);$$

$$\chi(t+1, k+1, n+1) \geq \chi(t, k, n).$$

Given a coloring $F = \{F_i : i \leq p\}$ of $(k-1)$-sets of X we can naturally add a point ∞ to all the blocks and obtain a partition of the k-sets on ∞. If two blocks of the same color did not intersect in $(t-1)$ or more elements before, two blocks of the same color now do not intersect in t or more elements. Now if $D = \{D_i : i \leq m\}$ is a partition of the k-sets of X, the set

$$C = \{F_i \cup \{\infty\},\ D_i : i \leq p\} \cup \{D_i : p < i \leq m\}$$

is a partition of the k-sets of $X \cup \{\infty\}$. If we are fortunate we may choose D so that no two k-sets of the same color of C intersect in t or more elements. Of course we would like both p and m small. We always have

$$\chi(t, k, n+1) \leq \chi(t, k, n) + \chi(t-1, k-1, n).$$

This bound is not very good.

LEMMA 3.3.

$$\chi(k-1, k, n) \leq n.$$

PROOF: Let our set X be the set of integers mod n. For $1 \leq i \leq n$ let

$$C_i := \left\{ A \in P_k(X) : \sum_{j \in A} j \equiv i \pmod{n} \right\}.$$

We claim that $C = \{C_i : i \leq n\}$ is a partition of $P_k(X)$ into packings of $(k-1)$-sets. Let $B \in P_{k-1}(X)$. If $B \cup \{s\}, B \cup \{j\} \in C_i$, then $s \equiv j \pmod{n}$. This implies $s = j$. □

2. Packings.

The problem of finding the polychromatic number of G naturally leads us to ask:

What is the maximum number of k-sets of an n-set no two of which intersect in t or more points?

Let $D(t,k,n)$ represent this maximum. We are trying to find the maximum number of pairwise disjoint $P_t(Y)$ for $Y \in P_k(X)$. This is a packing problem. If P is a set of k-sets that satisfy this property, we say P is a *packing* of t-sets by k-sets. We will present a few of the properties of this function, for a more thorough survey see [**3**]. Since each of our colorings is a packing of t-sets by k-sets evidently $|C_i| \geq D(t,k,n)$; therefore,

$$\chi(t,k,n) \geq \frac{\binom{n}{k}}{D(t,k,n)}. \tag{3.1}$$

Let P be a packing of the t-sets of an n-set by k-sets. Elements of P are usually called *blocks*. Each t-set is in at most one block while each block contains exactly $\binom{k}{t}$ t-sets. We conclude then that

$$D(t,k,n) \leq \frac{\binom{n}{t}}{\binom{k}{t}}.$$

Equality is possible if and only if each t-set is contained in a unique k-set. A packing which achieves equality is an example of a Steiner system.

A t-(n,k,λ) design is a pair $(V,\mathcal{B})$ consisting of an n-set V of points, a collection $\mathcal{B} \subseteq P_k(V)$ of blocks so that every t-set is on exactly λ blocks. By arguing as above we see that there are exactly $\lambda\binom{n}{t}/\binom{k}{t}$ blocks. A symmetric design is a 2-(n,k,λ) design with $n > k$ and $k(k-1) = \lambda(n-1)$. In other words, a symmetric design is a 2-design with equal number of points and blocks. It is well known that in a symmetric design every two blocks intersect in exactly λ points.

A *Steiner system* $S(t,k,n)$ is a t-$(n,k,1)$ design. Existence of an $S(t,k,n)$ then gives a packing with $\binom{n}{t}/\binom{k}{t}$ blocks. Clearly any packing with this number of blocks is necessarily a Steiner system. If an $S(t,k,n)$ exists then by deleting a point and considering blocks on that point we have an $S(t-1,k-1,n-1)$.

It is known that

$$D(t,k,n) = D(n-2k+t, n-k, n); \tag{3.2}$$

$$D(t,k,n) \leq D(t,k,n-1) + D(t-1,k-1,n-1). \tag{3.3}$$

If a $S(t,k,n)$ exists, then (3.3) is actually an equality, cf. [**3**].

Notice that $D(2,k,n)$ is simply the maximum number of pairwise edge disjoint complete subgraphs of K_k in K_n. Each point is on at most $\left\lfloor \frac{n-1}{k-1} \right\rfloor$ k-sets of our packing. As there are k points per block and n points total we find the trivial upper bound:

$$D(2,k,n) \leq \left\lfloor \frac{n}{k} \left\lfloor \frac{n-1}{k-1} \right\rfloor \right\rfloor.$$

It has been shown by Kirkman and Schöheim [**3**] that

$$D(2,3,n) = \left\lfloor \frac{n}{3} \left\lfloor \frac{n-1}{2} \right\rfloor \right\rfloor - \epsilon,$$

where $\epsilon = 1$ for $n \equiv 5 \bmod 6$ and 0 otherwise.

We can easily argue that

$$D(2,k,3k-3) = \begin{cases} 4 & \text{when } k = 3, \\ 3 & \text{when } k \geq 4. \end{cases}$$

It is of course possible to have two disjoint blocks, but then there can be no others in our packing. So we assume all our blocks intersect. We can clearly have at least two blocks in our packing. There are $k-2$ points off these blocks. Every other block in our packing is on at most one element of these two blocks

so it is on at least $k-2$ points off these blocks. We realize immediately then if $k \geq 4$ it is possible to add a third block to our packing but no more, and if $k = 3$ it is possible to add two more blocks to our packing.

A hypergraph (X, E) is *almost regular* if the degrees of distinct vertices differ by at most one. So the configuration just described is then a hypergraph where the degrees are all one or two. Now suppose $3|\binom{3k-3}{k}$. Is it possible to partition the k-sets of a $(3k-3)$-set into $\binom{3k-3}{k}/3$ classes so that in each class elements intersect pairwise in at most one point?

Baranyai showed, cf. [3]:

LEMMA 3.4.. *Let $a_1, \ldots, a_u$ be natural numbers such that $\sum_{i=1}^{u} a_i = \binom{n}{k}$ then the edges of $(X, P_k(X))$ can be partitioned into almost regular hypergraphs (X, E_j) where $a_j = |E_j|$.*

A vertex in $(X, P_k(X))$ will have degree $\lceil \frac{ka_j}{n} \rceil$ or $\lfloor \frac{ka_j}{n} \rfloor$.

Specializing to the case $n = 3k-3 \geq 9$ and $a_i = 3$ for all i, this work shows that there exists a partition of the k-sets into classes of size three in which each element of X has degree one or two. It is unfortunate that this is not sufficient to show the existence of a strong coloring of order $\binom{3k-3}{k}/3$. This is apparent when one realizes that the hypergraph

$$(\{1,2,3,4,5,6,7,8,9\}, \{\{1,2,3,4\}, \{1,5,6,7\}, \{3,4,8,9\}\})$$

is an almost regular hypergraph with the appropriate parameters, but it is not a packing of 2-sets. In Section 5 we will exhibit strong colorings for $n = 9$ and $n = 12$ that do achieve this lower bound.

3. Lifting Packings.

Two Steiner systems $S(t,k,n)$ on the same n-set are disjoint if they have no k-sets in common. There can be at most $\binom{n-t}{k-t}$ disjoint Steiner systems $S(t,k,n)$. If such a set exists it is called a *large set* of disjoint $S(t,k,n)$. We have seen already that

LEMMA 3.5. *If* $1 \leq t < k < n$ *then*

$$\chi(t,k,n) \geq \binom{n-t}{k-t}$$

with equality if and only if a large set of disjoint Steiner systems $S(t,k,n)$ *exist.*

LEMMA 3.6. *Let* Y *be a* $(v-1)$*-set. Assume* $\lambda = \frac{v-k}{k-t+1} \in \mathbb{Z}$. *If* P *is a collection of* $\frac{\lambda\binom{v-1}{t-1}}{\binom{k}{t-1}}$ k*-subsets of* Y *that is a packing of* t*-sets, then* P *is a* $(t-1)$*-*$(v-1,k,\lambda)$ *design.*

PROOF: Assume we have such a collection. For $A \in P_{t-1}(Y)$, let r_A be the number of blocks in P containing A. We wish to show that $r_A = \lambda$. Let N_1 be the number of ordered pairs (A,B) such that $A \in P_{t-1}(Y)$ and $A \subseteq B \in P$. By definition then

$$N_1 = \sum_{A \in P_{t-1}(Y)} r_A.$$

Alternatively, if we fix $B \in P$, there are $\binom{k}{t-1}$ choices for A.

$$N_1 = |P|\binom{k}{t-1}.$$

So the average value of r_A is λ.

Fix A a $(t-1)$-subset of Y. Let N_2 be the number of ordered pairs (x,B) so that $x \notin A$, but $\{x\} \cup A \subseteq B \in P$. Trivially then

$$N_2 = (k-t+1)r_A.$$

Now for every $x \notin A$, $A \cup \{x\}$ is a t-set, so it is contained in at most one block of our packing;

$$r_A \leq \frac{v-t}{k-t+1} = \lambda + \frac{k-t}{k-t+1}.$$

Implying $r_A \leq \lambda$. □

We will establish next that the there are packings satisfying the hypothesis of Lemma 3.6.

PROPOSITION 3.7. *If an $S(t,k,v)$ exists then*

(1) $\chi(t,k,v) \geq \binom{v-t}{k-t}$;

(2) $D(t,k,v-1) = \frac{v-k}{k-t+1}\frac{\binom{v-1}{t-1}}{\binom{k}{t-1}}$;

(3) $\chi(t,k,v-1) \geq \binom{v-t}{k-t}$.

PROOF: The first inequality is a restatement of Lemma 3.5. Notice if an $S(t,k,v)$ exists, then $\lambda = \frac{v-k}{k-t+1}$ is the number of blocks on a $(t-1)$-set; thus, it is an integer. The contraction of an $S(t,k,v)$ at a point is an $S(t,k,v-1)$ so from (3.3) we find

$$D(t,k,v-1) = \frac{\lambda\binom{v-1}{t-1}}{\binom{k}{t-1}}.$$

Item (3) follows from statement (3.1). □

Now since $\chi(t,k,n)$ is an increasing function in n we have:

COROLLARY 3.8. *If a large set of disjoint $S(t,k,v)$ exists then*

$$\chi(t,k,v) = \chi(t,k,v-1) = \binom{v-t}{k-t}.$$

Sometimes it is possible to have the converse of Corollary 3.8.

THEOREM 3.9. *If an $S(k-1,k,v)$ exists then the following are equivalent.*

(1) *A large set of disjoint $S(k-1,k,v)$ exists;*

(2) $\chi(k-1,k,v) = v-k+1$;

(3) $\chi(k-1,k,v-1) = v-k+1$.

PROOF: By Lemma 3.5 and Corollary 3.8, it suffices to show (3) implies (1). To this end, let $C = \{C_i : i \leq v-k+1\}$ be a partition of the k-subsets of a $(v-1)$-set Y into packings of $(k-1)$-sets. We wish to extend this to a partition of the k-sets of $Y \cup \{\infty\}$ whose elements are packings of $(k-1)$-sets.

By Lemma 3.6 and Proposition 3.7 the packing C_i is a $(k-2)$-$(v-1,k,\frac{v-k}{2})$ design. It is natural then to extend our coloring to k-sets of $Y \cup \{\infty\}$ by defining $S = \{S_i : i \leq v-k+1\}$ by

$$S_i = C_i \cup \{T \cup \{\infty\} : T \in P_{k-1}(Y) \text{ and } T \not\subseteq B \text{ for all } B \in C_i\}.$$

By definition of our coloring C, each $(k-1)$-set of Y is covered by at most one block of each color. Our extension, therefore was chosen so that each $(k-1)$-set of Y is covered exactly once. Now if we are given a $(k-1)$ set $U \cup \{\infty\}$, then U is a $(k-2)$-subset of Y. There are then $\frac{v-k}{2}$ blocks of C_i containing U. So there are $v-k$ points in $Y \setminus U$ whose union with U is contained in a block of C_i. We conclude then that there is a unique point x of $Y \setminus U$ so that $U \cup \{x\}$ is not contained in a block of C_i. We have then that each S_i is an $S(k-1,k,v)$.

It remains to verify that these are actually disjoint $S(k-1,k,v)$. We started with a partition of $P_k(Y)$. For T a $(k-1)$-subset of Y, there are $v-k$ k-sets of Y containing T each of which must be in a different element of our partition. Therefore, there is a unique color i with $T \cup \{\infty\} \in S_i \setminus C_i$. □

We would like to know what other parameters guarantee that a packing can be lifted. We notice

PROPOSITION 3.10. *If P is a packing of 2-sets by $(n+1)$-subsets of a (n^2+n)-set with exactly n^2 blocks, then P is completable to a 2-$(n^2+n+1,n+1,1)$ design.*

PROOF: By Lemma 3.6, P is a 1-$(n^2+n, n+1, n)$ design. Let B be a block of P. Each point of P is on $n-1$ other blocks. Thus there are n^2-1 blocks intersecting B. Because P is a packing of 2-sets, no two blocks intersect in two or more points. This shows that every pair of blocks intersect in a unique point. The dual $P^{\perp}$ of P is the configuration whose points are the blocks of P and whose blocks are the points of P. We have shown $P^{\perp}$ is a 2-$(n^2, n, 1)$ design. Let us define an equivalence relation on the blocks of $P^{\perp}$. Two blocks A and B are equivalent if and only if $A = B$ or $A \cap B = \emptyset$. The equivalence classes then partition the blocks of $P^{\perp}$ into $n+1$ parallel classes each of size n. Now in P this means there is a partition $\{C_i : i \leq n+1\}$ of the points into sets of size n such that for each C_i, a block of P intersects C_i in exactly one point. We conclude that the collection

$$P \cup \{C_i \cup \{\infty\} : i \leq n+1\}$$

is a 2-$(n^2+n+1, n+1, 1)$ design. □

Notice however if we start with a set of packings of 2-sets of a (n^2+n)-set by $(n+1)$-sets although we can lift each color seperately to a packing of 2-sets by $(n+1)$-sets, there is no guarantee that this lifting will give disjoint packings.

4. Packings of Points and Pairs.

Now let us return to our study of $\chi(t, k, n)$. Proofs of existence of large sets of Steiner systems are not excessive. The special case $t = 1$ was handled by Baranyai. Notice for the existence of an S(1,k,n) it is necessary and sufficient that k divides n. When $t = 1$ we are asking for the minimum number of classes into which $P_k(X)$ can be split such that any two sets in any class are disjoint. In

such a coloring since there are at most $\lfloor \frac{n}{k} \rfloor$ k-sets of each color we need at least $\lceil \binom{n}{k} / \lfloor \frac{n}{k} \rfloor \rceil$ colors. As a consequence of Lemma 3.4 Baranyai showed [**3**]:

LEMMA 3.11 (BARANYAI). *One can partition the k-sets of an n-set into*

$$\left\lceil \binom{n}{k} / \lfloor \frac{n}{k} \rfloor \right\rceil$$

classes in which each element of our n-set occurs at most once. In our notation,

$$\chi(1,k,n) = \left\lceil \binom{n}{k} / \lfloor \frac{n}{k} \rfloor \right\rceil .$$

COROLLARY 3.12. *For $k \geq 4$,*

$$\chi(2,k,2k) = \binom{2k-1}{k}.$$

PROOF: With a little thought, one finds $D(2,k,2k) = 2$. The lower bound then follows from (3.1). But by Lemma 3.2, χ decreases as t increases so $\chi(2,k,2k) \leq \chi(1,k,2k)$. □

Let us consider now partitioning the triples of an n-set so that every 2-set is contained in at most one block of each color. Our first nontrivial case of study is then $n = 5$. By Lemma 3.2 $\chi(2,3,5) = \chi(1,2,5)$. The latter quantity is known to be 5 by Baranyai's result. A well-known result of Cayley [**3**] is that there are two disjoint S(2,3,7), but there are not three disjoint ones. By Theorem 3.5 then, $\chi(2,3,6) \geq 6$.

CONSTRUCTION: $\chi(2,3,6) = 6$.

Take as our 6 points $\{0,1,2,3,4,5\}$. Define $C = \{C_i\}$ by

$$C_1 = \begin{matrix}\{0,1,2\}\\ \{2,3,4\}\\ \{0,4,5\}\end{matrix} \qquad C_2 = \begin{matrix}\{0,1,5\}\\ \{1,2,3\}\\ \{3,4,5\}\end{matrix} \qquad C_3 = \begin{matrix}\{0,2,3\}\\ \{2,4,5\}\\ \{0,1,4\}\end{matrix}$$

$$C_4 = \begin{matrix}\{0,1,3\}\\ \{2,3,5\}\\ \{1,4,5\}\end{matrix} \qquad C_5 = \begin{matrix}\{0,2,4\}\\ \{1,3,4\}\\ \{0,3,5\}\\ \{1,2,5\}\end{matrix} \qquad C_6 = \begin{matrix}\{0,2,5\}\\ \{1,2,4\}\\ \{1,3,5\}\\ \{0,3,4\}.\end{matrix}$$

This construction shows that 6 colors is sufficient.

CONSTRUCTION: $\chi(2,3,7) = 6$.

Since $\chi(2,3,6)$ is a lower bound for $\chi(2,3,7)$, it suffices to give a coloring of the triples of 7 points using 6 colors. Take as our 7 points {0,1,2,3,4,5,6}. Define $C = \{C_i\}$ by

$$C_1 = \begin{matrix}\{1,2,4\}\\ \{2,3,5\}\\ \{3,4,6\}\\ \{0,4,5\}\\ \{0,2,6\}\\ \{0,1,3\}\\ \{1,5,6\}\end{matrix} \quad C_2 = \begin{matrix}\{3,5,6\}\\ \{0,4,6\}\\ \{0,1,5\}\\ \{1,2,6\}\\ \{0,2,3\}\\ \{1,3,4\}\\ \{2,4,5\}\end{matrix} \quad C_3 = \begin{matrix}\{0,2,5\}\\ \{0,3,4\}\\ \{0,1,6\}\\ \{1,2,3\}\\ \{2,4,6\}\\ \{1,4,5\}\end{matrix};$$

$$C_4 = \begin{matrix}\{1,3,6\}\\ \{0,1,4\}\\ \{1,2,5\}\\ \{2,3,4\}\\ \{0,3,5\}\\ \{4,5,6\}\end{matrix} \quad C_5 = \begin{matrix}\{0,2,4\}\\ \{1,4,6\}\\ \{3,4,5\}\\ \{2,3,6\}\\ \{0,5,6\}\end{matrix} \quad C_6 = \begin{matrix}\{1,3,5\}\\ \{2,5,6\}\\ \{0,3,6\}\\ \{0,1,2\}.\end{matrix}$$

Notice in this construction that two distinct blocks of the same color intersect in a unique point. Let us define a partitioning $E = \{E_i\}$ of the 4-sets of an 8-set $\{0,1,2,3,4,5,6,\infty\}$. A 4-set not on ∞ is in E_i if its complement is in C_i. A 4-set B on ∞ is in E_i if $B \setminus \{\infty\} \in C_i$. Blocks of the same color intersect in at most two points. So $\chi(3,4,8) \leq 6$. However by Lemma 3.2 $\chi(3,4,8) \geq \chi(3,4,7) = \chi(2,3,7)$.

$$\chi(3,4,8) = 6.$$

For many years the primary focus was in developing recursive constructions to show the existence of large sets of Steiner Triple Systems, STS(n)= $S(2,3,n)$. It is straightforward to show that a necessary condition for the existence of STS

is that $n \equiv 1,3 \bmod 6$. It is well known that these are also sufficient conditions [**11**]. In a series of papers J.X. Lu [**14**] gave constructions for large sets of disjoint STS(n) for $n \equiv 1,3 \pmod 6, n > 7$ for all but a finite number of admissable n. L. Teirlinck has constructed large sets of disjoint STS(n) for the finite number of cases which Lu was unable finish [**20**].

For other systems not much is known about existence although nonexistence has been demonstrated in numerous cases (see [**13**]). In 1982, however, Chouinard [**6**] constructed a large set of S(2,4,13). So by Corollary 3.8,

$$\chi(2,4,13) = \chi(2,4,12) = 55.$$

Now for $n \equiv 1,3 \pmod 6, n > 7$ there is a large set of S(2,3,n); therefore, by Theorem 3.9 if $n \equiv 0,1,2,3 \pmod 6, n > 7$ we know $\chi(2,3,n)$. If $n \equiv 4 \bmod 6$, then $D(2,3,n) = \frac{n(n-2)-2}{6}$. So $\chi(2,3,n) \geq n$, but by Lemma 3.3, n is also an upper bound.

For $n \equiv 5 \bmod 6$ we can again invoke Lemma 3.3 to conclude that n is an upper bound. Because χ is an increasing function in n, it is also immediate that $n-1$ is a lower bound. We exhibit a partition of the triples of an 11-set into 10 packings. That this is possible has been noted in [**5**].

CONSTRUCTION: $\chi(2,3,11) = 10$.

Let our set X be $\mathbb{Z}_{10} \cup \{\infty\}$. Let α be the cyclic permutation $(0\,1 \ldots 9)$. Since 3 and 10 are relatively prime the orbits of α on $P_3(\mathbb{Z}_{10})$ each have order 10. Furthermore, there is a unique representative of each orbit whose elements sum to zero mod 10.

Define

$$B := \{\{a,b,c\} \in P_3(\mathbb{Z}_{10}) : a+b+c \equiv 0 \bmod (10)\} \cup \{2,4,9\} \setminus \{4,7,9\}$$

and

$$M := \{\infty, 7, 9\} \cup \{\infty, 2, 6\} \cup \{\infty, 1, 8\} \cup \{\infty, 3, 4\}.$$

For $0 \leq i \leq 4$ let $C_i := \{\alpha^i B, \alpha^i M, \alpha^i\{\infty, 0, 5\}\}$. For $5 \leq i \leq 9$ let $C_i := \{\alpha^i B, \alpha^i M\}$. Our base sets were chosen so they contained one element out of each orbit. We assert that this is a partition of the triples of X such that no two triples of the same color intersect in two or more elements.

T. Etzion [**8, 9**] has constructed a family of $n \equiv 5 \pmod 6$ for which there exists a partition of the triples using $n-1$ packings. It is conjectured that for any $n \equiv 5 \pmod 6$ there exists a partition of the triples of an n-set into $n-1$ packings of pairs.

We summarize these results.

LEMMA 3.12.

$$\chi(2,3,n) = \begin{cases} 5 & \text{if } n = 5; \\ 6 & \text{if } n = 6; \\ 6 & \text{if } n = 7; \\ 10 & \text{if } n = 11; \\ n-2 & \text{if } n \equiv 1,3 \pmod 6, n \geq 9; \\ n-1 & \text{if } n \equiv 0,2 \pmod 6, n \geq 8; \\ n & \text{if } n \equiv 4 \pmod 6. \end{cases}$$

Now since $\chi(1,2,6) = 5$, it follows that $\chi(3,4,6) = 5$. Similiarly since $\chi(3,4,7) = \chi(2,3,7)$, we know $\chi(3,4,7) = 6$. In the last section we saw $\chi(3,4,8) = 6$. Let us now consider $n = 9$. Kramer and Mesner [**13**] have shown that there are at most five pairwise disjoint S(3,4,10). By Lemma 3.5 and Theorem 3.9, we conclude that $\chi(3,4,9) \geq 8$.

CONSTRUCTION: $\chi(3,4,9) = 8$.

Let our nine points be $\mathbb{Z}_7 \cup \{x, y\}$. Let α be the cyclic permutation taking i to

$i+1$ that fixes x and y. Since 7 is prime each orbit of α on the 4-sets, 3-sets, and 2-sets of $\mathbb{Z}_7$ has cardinality 7. Define C_0 by

$$\begin{array}{lllll} \{2,3,4,5\} & \{1,3,4,6\} & \{1,2,5,6\} & \{0,3,5,6\} & \{0,1,2,4\} \\ \{x,0,1,6\} & \{x,1,3,5\} & \{x,2,3,6\} & \{x,0,4,5\} & \\ \{y,1,2,3\} & \{y,0,2,5\} & \{y,1,4,5\} & \{y,0,4,6\} & \\ \{x,y,0,3\} & \{x,y,2,4\} & \{x,y,5,6\}. & & \end{array}$$

For $0 \leq i \leq 6$, let

$$C_i := \{\alpha^i T : T \in C_0\}.$$

Let

$$C_7 := \{\alpha^j\{x,3,5,6\}, \alpha^j\{y,1,2,4\} : 0 \leq j \leq 6\}.$$

The blocks in C_0 contain an orbit representative for all orbits except those containing $\{x,3,5,6\}$ and $\{y,1,2,4\}$. So we have partitioned the 4-sets. Since our blocks in C_0 and C_7 pairwise intersect in at most two points, $C = \{C_i : 0 \leq i \leq 7\}$ is a partition of the 4-sets into packings of 2-sets.

5. The Chromatic Number $\chi(2,k,3k-3)$.

We have already seen $\chi(2,3,6) = 6$ which is not $\binom{6}{3}/D(2,3,6)$. In this section we would like to give constructions for $k = 4$ and $k = 5$. We have shown that $D(2,k,3k-3) = 3$ for $k \geq 4$. We know then for $k \geq 4$, $\chi(2,k,3k-3) \geq \frac{\binom{3k-3}{k}}{3}$. When this number is an integer, is equality possible? We demonstrate that for the first two cases $k = 4$ and $k = 5$ it is.

We first describe our method. Choose p a large prime so that p is a divisor of $\frac{\binom{3k-3}{k}}{3}$. We also require that $k > n - p$. Let our n-set be

$$\mathbb{Z}_p \cup \{\infty_i : 1 \leq i \leq n-p\}.$$

We denote by α the permutation $(0\,1\,\ldots\,p-1)$ that cyclically shifts i to $i+1$ and fixes ∞_j for all j. Since p is prime, the orbits of α on the set $P_j(\mathbb{Z}_p)$ have cardinality p for each j, $k-n+p \leq j \leq k$. Each orbit will have a unique element whose sum over its elements will be 0 (mod p).

What we would like to do is to chose $\frac{\binom{3k-3}{k}}{3p}$ starter colors, so that we have exactly one representive out of each of these orbits. By applying our permutation α repeatedly, we will obtain a coloring of the k-sets each of which packs 2-sets. For $k=4$ and $k=5$ we describe the starter blocks. To the best of our knowledge this was not previously known.

CONSTRUCTION: $\chi(2,4,9) = 42$.

Use $p = 7$.

$$C_1 = \begin{matrix}\{\infty_1,\infty_2,0,3\}\\ \{\infty_1,1,2,4\}\\ \{3,4,5,6\}\end{matrix} \quad C_2 = \begin{matrix}\{\infty_1,3,5,6\}\\ \{\infty_1,0,1,2\}\\ \{\infty_2,2,4,6\}\end{matrix} \quad C_3 = \begin{matrix}\{\infty_1,\infty_2,0,2\}\\ \{\infty_2,1,5,6\}\\ \{2,3,4,6\}\end{matrix}$$

$$C_4 = \begin{matrix}\{\infty_2,0,2,3\}\\ \{\infty_2,4,5,6\}\\ \{\infty_1,0,1,4\}\end{matrix} \quad C_5 = \begin{matrix}\{\infty_1,\infty_2,0,1\}\\ \{0,2,3,4\}\\ \{1,3,5,6\}\end{matrix} \quad C_6 = \begin{matrix}\{\infty_1,2,4,6\}\\ \{\infty_2,0,3,6\}\\ \{0,1,4,5\}\end{matrix}$$

CONSTRUCTION: $\chi(2,5,12) = 264$.

Use $p = 11$.

$\{\infty_1 0,1,2,8\}$	$\{\infty_1,0,1,3,7\}$	$\{\infty_1,1,2,5,7\}$	$\{\infty_1,2,5,7,8\}$
$\{\infty_1,3,6,7,10\}$	$\{\infty_1,2,4,6,10\}$	$\{\infty_1,0,3,4,10\}$	$\{\infty_1,0,3,9,10\}$
$\{4,5,8,9,10\}$	$\{1,4,5,8,9\}$	$\{2,3,6,8,9\}$	$\{1,4,6,8,9\}$
$\{\infty_1,0,3,6,8\}$	$\{\infty_1,1,2,3,10\}$	$\{\infty_1,2,3,5,8\}$	$\{\infty_1,1,5,9,10\}$
$\{\infty_1,2,4,7,9\}$	$\{\infty_1,4,5,6,7\}$	$\{0,3,4,8,10\}$	$\{1,3,4,6,8\}$
$\{0,1,5,9,10\}$	$\{0,4,8,9,10\}$	$\{1,2,4,6,7\}$	$\{0,2,5,7,8\}$
$\{\infty_1,0,6,7,9\}$	$\{\infty_1,1,3,8,10\}$	$\{\infty_1,1,3,6,7\}$	$\{\infty_1,2,6,8,10\}$
$\{1,2,4,9,10\}$	$\{0,2,4,6,10\}$	$\{0,2,4,7,9\}$	$\{0,4,7,8,9\}$
$\{2,3,5,7,8\}$	$\{0,1,5,7,9\}$	$\{4,5,6,8,10\}$	$\{0,1,2,3,5\}$

$$\begin{array}{cccc}
\{\infty_1,0,3,4,6\} & \{\infty_1,1,3,4,7\} & \{\infty_1,3,8,9,10\} & \{\infty_1,0,6,8,9\} \\
\{3,5,7,8,10\} & \{2,5,7,8,9\} & \{2,4,5,7,10\} & \{1,2,4,5,6\} \\
\{0,1,2,9,10\} & \{0,1,5,6,10\} & \{0,1,6,7,8\} & \{0,2,3,7,10\}
\end{array}$$

$$\begin{array}{cccc}
\{\infty_1,4,5,8,10\} & \{\infty_1,1,4,7,8\} & \{\infty_1,3,5,6,10\} & \{\infty_1,4,6,8,9\} \\
\{1,3,7,8,9\} & \{0,3,7,9,10\} & \{1,2,4,6,9\} & \{0,4,5,7,10\} \\
\{0,2,5,6,9\} & \{0,2,4,5,6\} & \{0,4,5,7,8\} & \{1,2,3,7,9\}
\end{array}$$

$$\begin{array}{cccc}
\{\infty_1,3,4,8,9\} & \{\infty_1,2,5,9,10\} & \{\infty_1,0,1,5,7\} & \{\infty_1,1,8,9,10\} \\
\{0,1,4,7,10\} & \{2,3,4,6,7\} & \{0,6,8,9,10\} & \{2,5,6,7,8\} \\
\{1,2,5,6,8\} & \{0,1,3,8,10\} & \{2,3,4,5,8\} & \{0,3,4,6,9\}.
\end{array}$$

6. Some Values of $m(\binom{s}{k}; k, s, n)$.

We now shift our attention to the study of $m(p; k, s, n)$. If there are fewer than $\binom{s}{k}$ colors, then there can be no polychromatic s-sets. It is obvious that if $p \geq \gamma(k, s, n)$, we may have all s-sets polychromatic. If $2k \leq s < n$, and $p = \binom{s}{k}$, there will exist two k-sets of the same color; these will be contained in an s-set. Putting these together we find $m(\binom{s}{k}; k, s, n) = \binom{n}{s}$ if and only if $\chi(2k - s, k, n) = \binom{s}{k}$. Actually by Lemma 3.2, we have

$$m\left(\binom{s}{k}; k, s, n\right) = \binom{n}{s} \quad \text{if and only if} \quad \chi(n - s, n - k, n) = \binom{s}{k}.$$

We have seen that the latter is possible if and only if a large set of disjoint $S(n - s, n - k, n)$ exists. For example, Baranyai's Theorem gives us

$$m\left(\binom{lk-1}{lk-k}; lk - k, lk - 1, lk\right) = lk. \tag{3.4}$$

In general, we will not restate the results in this new terminology.

Let X be an n-set. Given a partition $C = \{C_i : i \leq \binom{s}{k}\}$ of the k-sets, we naturally obtain a partition $P = \{P_i : i \leq \binom{s}{k}\}$ of the $(n-k)$-sets of X. Let S be a polychromatic s-set, and let U be its complement in X. Every k-set in S is complement to an $(n-k)$-set containing U; conversely, every $(n-k)$-set containing U has its complement in S. So S is polychromatic with respect to C if and only if every $(n-k)$-set containing $X \setminus S$ is in a different element of P. We will say an $(n-s)$-set U has property CH if no two $(n-k)$-sets containing U have the same color in P. Then finding the maximum number of polychromatic s-sets if the k-sets are colored with $\binom{s}{k}$ colors is equivalent to coloring $(n-k)$-sets of X with $\binom{s}{k}$ colors so as to maximize the number of $(n-s)$-sets having property CH.

LEMMA 3.13.

$$m(n-1; n-2, n-1, n) = \begin{cases} n & \text{if } n \text{ is even;} \\ n-1 & \text{if } n \text{ is odd.} \end{cases}$$

PROOF: If n is even, this follows from Baranyai's Theorem; if n is odd this same theorem shows that $n-1$ is an upper bound on m. Assume n is odd; we will construct a coloring with $n-1$ polychromatic $(n-1)$-sets. By Baranyai's Theorem, we can partition the edges of K_{n-1} into $n-2$ perfect matchings, $\{P_i : i \leq n-2\}$. Define P_{n-1} to be the set of edges on our n^{th} point. We have then an $(n-1)$-coloring of the edges of K_n. This coloring contains exactly $n-1$ points with property CH. □

Let us find some lower bounds.

LEMMA 3.14. *For $s < n$,*

$$m\left(\binom{s}{k}; k, s, n\right) \geq \begin{cases} n-s+1 & \text{when } k = 2; \\ (n-s+1)\left\lfloor \frac{n}{s-1} \right\rfloor & \text{when } k \geq 3. \end{cases}$$

PROOF: Let X be an n-set. Suppose we have a partition the points

$$\{P_i : i \leq \left\lfloor \frac{n}{s-1} \right\rfloor + 1\}$$

such that $|P_i| = s-1$ if $i \neq \left\lfloor \frac{n}{s-1} \right\rfloor + 1$. We will define a map $f : \binom{X}{k} \to \{1, \ldots, \binom{s}{k}\}$ whose inverse image will be our coloring. Let S an s-set be a superset of P_1. There exists a point $x \notin P_1$ so that $\{x\} \cup P_1 = S$. Let $\{K_i : i \leq \binom{s}{k}\}$ be the collection of k-subsets of S. Define $f(K_i) = i$. For each $y \notin S$ and for each k-subset K_i on x, define $f(K_i \cup \{y\} \setminus \{x\}) = i$. The k-subsets of $S \cup \{y\} \setminus \{x\}$ have distinct images under the map f. So far we have $n - s + 1$ polychromatic s-sets. Many k-sets have not been colored. In fact, we have only colored k-sets which have at least $k-1$ points in P_1. When $3 \leq k$ we have not assigned colors to k-sets that have at least $k-1$ points in P_j for $2 \leq j \leq \left\lfloor \frac{n}{s-1} \right\rfloor$. By repeating the above argument and arbitrarily coloring any uncolored k-sets, we have a coloring with the asserted number of polychromatic s-sets. □

COROLLARY 3.15. *Assume* $4 \leq n$, *and* $2 \leq k < \frac{n}{2}$. *Then*

$$m\left(\binom{n-1}{k}; k, n-1, n\right) = 2.$$

PROOF: We need only show the upper bound. Assume we have been given a $\binom{n-1}{k}$-coloring of the k-sets of an n-set which supports three polychromatic $(n-1)$-sets. So there exists an $(n-3)$-set U and three distinguished points x_1, x_2, x_3 so that the sets $S_i = U \cup \{x_j : j \neq i\}$ are polychromatic. If any k-set in U had the same color as a k-set of $U \cup x_i$, then S_j would not be polychromatic for $j \neq i$. Let $T_i = \{K_\alpha : \alpha \in I\}$ be the collection of k-sets on x_i that are not on x_j for $j \neq i$. Elements in this collection being contained in S_j for $j \neq i$ must all have different colors. Moreover elements of T_1 and T_2 must have different colors

since they are contained in S_3. There are then at least $3\binom{n-3}{k-1} + \binom{n-3}{k}$ colors. That is

$$3\binom{n-3}{k-1} + \binom{n-3}{k} \leq \binom{n-1}{k}.$$

This implies $0 \leq k(2k-n)$. □

Let us momentarily continue to consider the special case of $s = n-1$. Statement (3.4) completely handles the case when $n-k$ divides n. Let us examine the case when $n-k$ does not divide n. Define d by

$$\left\lfloor \frac{n}{n-k} \right\rfloor = \frac{n-d}{n-k}.$$

Let X be an n-set and $P = \{P_i : i \leq \binom{n-1}{k}\}$ a coloring of the $(n-k)$-subsets of X. There are $\binom{n}{k}$ of these subsets being partitioned among $\binom{n-1}{k}$ sets. Since

$$\frac{\binom{n}{k}}{\binom{n-1}{k}} = \frac{n}{n-k},$$

there exists an i such that

$$|P_i| \leq \frac{n-d}{n-k}.$$

We may assume without loss that $i = 1$. Count the number of ordered pairs (x, U) where x is a point in $U \in P_1$. Let τ_j be the number of points contained in exactly j elements of P_1. We then have

$$(n-k)|P_1| = \sum_{j=0}^{|P_1|} \tau_j.$$

By our choice of P_1 we find that $\tau_1 \leq n-d$. Every point is on $\binom{n-1}{k}$ k-sets, but we are only using this many colors. A point satisfying property CH must be on exactly one element of P_1. There are at most τ_1 such points. We have shown

LEMMA 3.16. *If d is defined by*

$$\left\lfloor \frac{n}{n-k} \right\rfloor = \frac{n-d}{n-k},$$

then

$$m\left(\binom{n-1}{k}; k, n-1, n\right) \leq n-d.$$

COROLLARY 3.17. *Assume d is defined by*

$$\left\lfloor \frac{n}{n-k} \right\rfloor = \frac{n-d}{n-k}$$

and that for all t, $0 \leq t \leq d$ we have $(n-k-t) \mid (n-d)$. Then

$$m\left(\binom{n-1}{k}; k, n-1, n\right) = n-d.$$

PROOF: Let S be a d-subset of an $(n-1)$-set Y. Every $(n-1-k)$-subset of Y has between 0 and $n-1-k$ points in S; furthermore, given any t-subset of S with $t \leq n-1-k$, it can be completed to an $(n-1-k)$-subset of Y. This proves the Vandermonde convolution formula

$$\sum_{t=0}^{d} \binom{d}{t}\binom{n-1-d}{n-k-t-1} = \binom{n-1}{k}.$$

Let X be an n-set. Fix a d-set S of X. For each t, $0 \leq t \leq d$, since $(n-k-t) \mid (n-d)$ Baranyai's Theorem implies there exists a partition of the $(n-k-t)$-subsets of $X \setminus S$ into $\binom{n-d-1}{n-k-t-1}$ parallel classes. Say

$$P_t = \left\{ P_{i,t} : i \leq \binom{n-d-1}{n-k-t-1} \right\}.$$

For each t-subset $T \subseteq S$ and for $i \leq \binom{n-d-1}{n-1-k-t}$ define

$$C_{i,T} = \{T \cup A : A \in P_{i,t}\}.$$

The collection

$$C = \{C_{i,T} : T \in P_t(S), i \leq \binom{n-d-1}{n-1-k-t} \text{ for } 0 \leq t \leq d\}$$

defines a partial coloring of the $(n-k)$-subsets of X. By the Vandermonde convolution formula there are $\binom{n-1}{k}$ elements in C. Furthermore, C was defined so that each point in $X \setminus S$ satisfies property CH. □

What fraction of the s-sets can be polychromatic?

LEMMA 3.18. *For fixed integers k, s satisfying $1 \leq k \leq s$,*

$$(n-s)\, m(p; k, s, n) \leq n\, m(p; k, s, n-1).$$

PROOF: Assume $n \geq s$. Let $C = \{C_i : i \leq \binom{s}{k}\}$ be a coloring of the k-subsets of an n-set. Count the number of ordered pairs (S, U) where S is a polychromatic s-subset of the $(n-1)$-set U. For each choice of U, there are at most $m(p; k, s, n-1)$ choices for S. Alternatively, the number of $(n-1)$-sets containing a fixed s-set is exactly $\binom{n-s}{n-1-s}$. Equality is possible if and only if for every $(n-1)$-set U the coloring restricted to U supports $m(p; k, s, n-1)$ polychromatic sets. □

This is fact shows that the sequence

$$\left\{ \frac{m(\binom{s}{k}; k, s, n)}{\binom{n}{s}} \right\}_{n=s}^{\infty}$$

is a decreasing sequence of positive real numbers bounded above by 1.

COROLLARY 3.19. *If $m(\binom{s}{k}; k, s, n) = \binom{n}{s}$, then for all l, $s \leq l \leq n$*

$$m(\binom{s}{k}; k, s, l) = \binom{l}{s}.$$

Lemma 3.18 together with Corollary 3.15 implies:

$$\textit{If } 4 \leq n \textit{ and } 2k < n, \textit{ then } \quad m\left(\binom{n-1}{k}; k, n-1, n+1\right) \leq n+1.$$

PROPOSITION 3.20. *Let* $\binom{s}{k} = p \geq 2$ *and write* $\binom{n}{k} = pa + b$ *where* $0 \leq b < p$, *then*

$$m(p;k,s,n) \leq \sum_{i=0}^{\binom{s}{k}} \binom{b}{i}\binom{p-b}{\binom{s}{k}-i}(a+1)^i a^{\binom{s}{k}-i}.$$

This is an equality when $k = 1$.

PROOF: Let $C = \{C_i : i \leq p\}$ be a p-coloring of the k-sets of X. We define the support A of a set S to be the set of colors that S nontrivially intersects. The number of polychromatic s-sets in C is then at most

$$B(C) := \sum_{A \in P_{\binom{s}{k}}} \prod_{x \in A} |C_x|$$

If $k = 1$ this is the actual number of polychromatic s-sets. Our bound as stated in the lemma is achieved by evenly distributing the k-sets between the p colors. It remains to justify why no other distribution with exactly p nonempty colors would provide a larger upper bound.

By assumption there are at least two colors. Suppose there exists two colors with the difference in their cardinality being more than two. Without loss of generality assume that $|C_1| - |C_2| \geq 2$. Let $A \in C_1$, and let I be the set of integers from 3 to p. Create a new p-coloring F that differs from C only in that $A \in F_2$ instead of F_1. We then find that

$$B(F) - B(C) = (|C_1| - |C_2| - 1) \sum_{A \in P_{s-2}(I)} \prod_{j \in A} |C_j| > 0.$$

It should be remarked here that we have in no way shown that the best way to color the k-sets comes from an evenly distributed coloring. □

COROLLARY 3.21.

$$\lim_{n \to \infty} \frac{m(s;1,s,n)}{\binom{n}{s}} = \frac{s!}{s^s}.$$

7. Polychromatic Triangles.

In this section $k = 2$ and $s = 3$. We will view our 3-colorings as edge colorings of K_n. We want to find the maximum number of polychromatic triangles. Let C be a 3-coloring of the edges of K_n that supports $m(3; 2, 3, n)$ polychromatic triangles. Let M be the number of monochromatic triangles and N the number of triangles that are neither monochromatic or polychromatic. Let g_i, r_i, b_i respectively be the number of edges on vertex i of color green, red, blue respectively. Each triangle has associated to it a degree sequence (x_1, x_2, x_3) which is the sequence of numbers describing the number of red, green, and blue edges of the triangle. Consider the coloring obtained by merging the red and blue colors together to purple. We can count the number of triangles that have one purple edge and two green edges or two purple edges and one green edge. Each such triangle has exactly two vertices which lie on one purple edge and one green edge of the triangle. There are then

$$\frac{1}{2}\sum_{i=1}^{i=n} g_i(n-1-g_i)$$

such triangles. We find then

$$3m(3;2,3,n) + 2N = \frac{1}{2}\sum_{i=1}^{i=n}\left(g_i(n-1-g_i) + r_i(n-1-r_i) + b_i(n-1-b_i)\right).$$

This together with $M + N + m(3; 2, 3, n) = \binom{n}{3}$ implies

PROPOSITION 3.22.

$$m(3;2,3,n) = 2M + \binom{n+1}{3} - \frac{1}{2}\sum_{i=1}^{n}(g_i^2 + r_i^2 + b_i^2). \tag{3.5}$$

As a consequence we immediately find

$$m(3;2,3,n) \leq 2M + \frac{n(n-1)}{3}.$$

Notice that the number of polychromatic triangles on vertex i is at most $r_ib_i + r_ig_i + g_ib_i$. The remaining vertices form a $(n-1)$-set; thus,

$$m(3;2,3,n) \leq r_ib_i + r_ig_i + g_ib_i + m(3;2,3,n-1) \tag{3.6}$$

Now the sum $r_1(n-1-r_1) + b_1g_1$ is at most $r_1(n-1-r_1) + \frac{(b_1+g_1)^2}{4} = \frac{(n-1-r_1)(3r_1+n-1)}{4}$. So every vertex is on at most $\frac{(n-1)^2}{3}$ polychromatic triangles. Equality implying there are equal number of edges of each color on that vertex. If we count the number of ordered pairs (x,T) where x is a vertex on a polychromatic triangle T, we find

PROPOSITION 3.23.

$$m(3;2,3,n) \leq \frac{n}{3}\left\lfloor \frac{(n-1)^2}{3} \right\rfloor.$$

Suppose vertex i were on exactly $r_ib_i + r_ig_i + g_ib_i$ polychromatic triangles. Let R_i, B_i, G_i respectively be the set of other ends of red, blue, green edges on x. The color of edges from one of these sets to another is then determined. Polychromatic triangles are either on x, have one vertex in each of these three sets, or are contained in one of these sets. In which case the number of polychromatic triangles is at most

$$r_ib_i + r_ig_i + g_ib_i + r_ib_ig_i + m(3;2,3,r_i) + m(3;2,3,g_i) + m(3;2,3,b_i). \tag{3.7}$$

Let us consider a few small examples. We have seen already that

$$m(3;2,3,4) = 4. \tag{3.8}$$

We claim that

$$m(3;2,3,5) = 7.$$

By Proposition 3.23, $m(3;2,3,5) \leq 8$. Suppose C is a 3-coloring of the edges of K_5 that supports 8 polychromatic triangles. By (3.6) and (3.8) all vertices

must have degree sequence $2,2,0$ or $2,1,1$. Let i be a vertex of degree sequence $2,2,0$. Our inequality in (3.6) is then an equality. We may then use (3.7) which implies there are at most 4 polychromatic triangles. All vertices then have degree sequence $2,1,1$. By (3.5) we have $8 = 2M - 5$. It suffices then to construct a coloring with 7 polychromatic triangles. Let the red edges be $\{0,1\},\{2,4\},\{0,3\}$, the blue edges be $\{1,3\},\{1,4\},\{0,2\},\{3,4\}$, and the green edges be $\{1,2\},\{2,3\},\{0,4\}$.

By Lemma 3.18 we have

$$\text{For } n \geq 5, \qquad m(3;2,3,n) \leq 0.7\binom{n}{3}.$$

Of course to color an n-set with three colors, one could always divide up the points into three nearly equal sets S_i and view these as vertices of a triangle. All edges from S_1 to S_2 would be blue, all edges from S_1 to S_3 would be red, and all edges from S_2 to S_3 would be green. The sets themselves would have their edges colored best possible. By induction we find for $u \geq 2$

$$m(3;2,3,3^u) \geq \frac{3^{u-1}(9^u-1)}{8}.$$

By Lemma 3.18 we have for $n \leq 3^u$

$$\frac{m(3;2,3,n)}{\binom{n}{3}} \geq .25 + \frac{3}{3^u-2}.$$

This is not the best way. Instead divide the points into four sets S_i of about the same size. Since $m(3;2,3,4) = 4$ we can color the edges between sets in such a way that any triangle with each of its vertices in a different set S_i is polychromatic. Using this idea we find for $u \geq 2$

$$m(3;2,3,4^u) \geq \frac{4^u(16^u-1)}{15}.$$

This implies for $n \leq 4^u$ that

$$\frac{m(3;2,3,n)}{\binom{n}{3}} \geq .4 + \frac{3}{4^{u+1}-8}.$$

Being more careful we find

$$m(3;2,3,6) \geq 12,$$

$$m(3;2,3,7) \geq 20,$$

$$m(3;2,3,8) \geq 32.$$

By considering cases and using arguments similiar to the ones used for $n = 5$ we find these are all equalities. Thus for $n \geq 8$

$$\frac{m(3;2,3,n)}{\binom{n}{3}} \leq \frac{4}{7}.$$

We conjecture that asymptotically the best coloring comes about by dividing the points into 4 nearly equal sets as above.

CONJECTURE.

$$\lim_{n\to\infty} \frac{m(3;2,3,n)}{\binom{n}{3}} = 0.4.$$

4

Projective Geometry

Thus far we have restricted our attention to sets. It is natural to generalize to vector spaces. In this section we characterize specifically what type of vector spaces we wish to consider, and we give some basic results.

A projective geometry $\mathcal{P}$ is a triple (P, L, I) consisting of a set P of points, a set L of lines, and an incidence relation $I \subseteq P \times L$ that satisfy:

(P1) every pair of points are on a unique line;

(P2) every line contains at least three points;

(P3) $\mathcal{P}$ contains a set of three points which are not collinear;

(P4) for X_1, X_2, X_3 distinct points and ℓ_1, ℓ_2, ℓ_3 distinct lines with X_i on ℓ_j for all $i \neq j$, if ℓ is a line not incident with X_1 that intersects ℓ_2 and ℓ_3 then ℓ intersects ℓ_1.

Of special interest are projective planes which are projective geometries that satisfy:

(P5) every pair of distinct lines contain a common point.

Notice (P5) implies (P4) and that the point common to two distinct lines by (P1) is necessarily unique.

It is well known [**11**] that

LEMMA 4.1. *The class of projective planes is the same as the class of symmetric*

designs with $\lambda = 1$ *and* $k > 2$.

If we write $q + 1$ for k we say our projective plane has order q. Notice since each line contains at least three points we may assume $q \geq 2$. We will sometimes refer to lines of our projective planes as hyperplanes.

Projective geometries may be constructed fairly easily. For K a skewfield, let V be an $(n + 1)$-dimensional vector space over K. We define the incidence structure $\mathcal{P}(n, K)$ to be the collection of all subspaces of V with incidence being subspace inclusion. Let $\text{rank}(U)$ denote the rank of a subspace U in V, that is the cardinality of the largest independent set of vectors in U. The projective dimension of U in $\mathcal{P}(n, K)$ is one less than its rank in V. In particular $\mathcal{P}(n, K)$ has projective dimension n. Elements of $\mathcal{P}(n, K)$ of projective dimension $i - 1$ are called i-flats. Elements of projective dimension 0, 1, 2, and $n - 1$ are called respectively points, lines, planes, and hyperplanes. Let $\mathcal{P}_{n,1}(K)$ be the substructure of $\mathcal{P}(n, K)$ consisting of the points and lines of $\mathcal{P}(n, K)$.

LEMMA 4.2. *If* $n > 1$ *then* $\mathcal{P}_{n,1}(K)$ *is a projective geometry.*

PROOF: For U, W subspaces of V we define $U \cap W$ to be the largest subspace contained in U and W and $U + W$ to be the smallest subspace containing U and W. Since K is a skewfield subspaces of V satisfy the modular law:

$$\text{rank}(U + W) + \text{rank}(U \cap W) = \text{rank}(U) + \text{rank}(W).$$

Let U and W be distinct points then $U \cap W = 0$. By the modular law we then know that $U + W$ is a line which is necessarily unique. A line l having rank two contains two independent points U and W so it contains the distinct points $U, W, U + W$; ie. every line contains at least three distinct points. Since V is a $(n+1)$-dimensional vector space over K and $n+1 \geq 3$ there exists three collinear

points. Let X_1, X_2, X_3 be distinct points and l_1, l_2, l_3 distinct lines with X_i on l_j for all $i \neq j$. Let l be a line not incident with X_1 that intersects l_2 at Y and l_3 at Z. There exists $a, b, c, d \in K$ so that $Z = aX_1 + bX_2, Y = cX_1 + dX_3$; hence, $ac^{-1}Y - Z \in l_1 \cap l$. We have shown that (P1)–(P4) hold.

We have exhibited two ways to construct projective geometries. In [**11**] it is shown:

LEMMA 4.3. *If the number of points of a projective geometry $\mathcal{P}$ is finite, then either $\mathcal{P}$ is a projective plane or $\mathcal{P} \approx \mathcal{P}_{n,1}(K)$ for a unique n and a unique K.*

If K is a finite field, then K has q elements where q is a power of a prime; furthermore, it is unique up to isomorphism. We denote the unique field on q elements by $\mathrm{GF}(q)$. In view of Lemma 4.2 for $n \geq 3$ a projective geometry of dimension n and order q is $\mathcal{P}(n, q) := \mathcal{P}(n, \mathrm{GF}(q))$.

It is natural to ask coloring questions on $\mathcal{P}$; we ask the same questions as we did on sets but replace the expression m-set by m-flat. To develop our trivial bounds we need to be able to determine the number of k-flats of an s-flat.

Let V be a rank m vector space over $\mathrm{GF}(q)$. The number of rank s subspaces of V is

$$\begin{bmatrix} m \\ s \end{bmatrix}_q = \frac{(q^m - 1)(q^{m-1} - 1) \cdots (q^{m-s+1} - 1)}{(q^s - 1)(q^{s-1} - 1) \cdots (q^1 - 1)}.$$

This is the Guassian number of m choose s over $\mathrm{GF}(q)$, cf. [**19**]. It is a polynomial in q of degree $s(m - s)$. The number of rank t subspaces of V containing a fixed rank s subspace of V is $\begin{bmatrix} m-s \\ t-s \end{bmatrix}_q$. It must be remembered when dealing with projective spaces that the projective dimension of a projective space is one less than its rank.

Let $\mathcal{P}$ be a projective geometry of dimension $n - 1$ and order q. Throughout this section this will mean that if $n = 3$ then $\mathcal{P}$ is a $2 - (q^2 + q + 1, q + 1, 1)$ design

otherwise $\mathcal{P} = \mathcal{P}(n-1, q)$. Let $C = \{C_i\}$ be a coloring of the k-flats of $\mathcal{P}$. An s-flat S is said to be *polychromatic* with respect to C if no two of its k-flats have the same color.

We are interested then in the following questions.

(1) What is the minimum number $\gamma_q(k, s, n)$ of colors needed to color the k-flats of a projective $(n-1)$-space of order q so that all s-flats are polychromatic?

(2) If p is fixed, what is the maximum number $m_q(p; k, s, n)$ of polychromatic s-flats possible?

As in the case of sets these questions are uninteresting when $k = s$ or $s = n$.

Now to have any polychromatic s-flat we need at least $\begin{bmatrix} s \\ k \end{bmatrix}_q$ colors. It is immediate that for $1 \leq k < s < n$

(4.1) $\begin{bmatrix} s \\ k \end{bmatrix}_q \leq \gamma_q(k, s, n) \leq \begin{bmatrix} n \\ k \end{bmatrix}_q$;

(4.2) if $p < \begin{bmatrix} s \\ k \end{bmatrix}_q$ then $m_q(p; k, s, n) = 0$.

If $n = 3$ then we may assume $k = 1$ and $s = 2$. Since $\mathcal{P}$ is a projective plane every two points determine a line so we need $q^2 + q + 1$ colors. For $n \geq 4$ let A, B be two k-flats of $\mathcal{P}$. We have

$$\operatorname{rank}(A + B) = \operatorname{rank}(A) + \operatorname{rank}(B) - \operatorname{rank}(A \cap B) \leq 2k$$

where equality holds only if $A \cap B = 0 \in V$. We conclude

$$\textit{If } 1 \leq k < 2k \leq s \leq n, \textit{ then } \gamma_q(k, s, n) = \begin{bmatrix} n \\ k \end{bmatrix}_q.$$

The study of $\gamma_q(k, s, n)$ is only interesting when $s < 2k$. If in a coloring of the k-flats there were two k-flats of the same color whose intersection was contained in a $(2k - s)$-flat, there are necessarily s-flats that are not polychromatic. This

is analogous to the situation on sets. Let us restrict our attention momentarily to $s = 2k-1$. We want then a partition of the k-flats into disjoint sets of k-flats. A $(k-1)$-*spread* is a set of k-flats such that each point is incident with exactly one element of our set. A $(k-1)$-*partial spread* is a set of k-flats such that each point is incident with at most one element of our set. To find $\gamma_q(k, 2k-1, n)$ we want to partition the k-flats into the fewest number of $(k-1)$-partial spreads. The cardinality of a $(k-1)$-spread then provides an upper bound on the number of disjoint k-flats.

$$\gamma_q(k, 2k-1, n) \geq \left\lceil \frac{\begin{bmatrix} n \\ k \end{bmatrix}_q}{\left\lfloor \frac{q^n-1}{q^k-1} \right\rfloor} \right\rceil .$$

A $(k-1)$-*parallelism* is a collection of $(k-1)$-spreads that partition the k-flats. So equality is possible above if and only if a $(k-1)$-parallelism exists. A. Beutelspacher [2] showed for $n = 2^{i+1}$, $i = 1, 2, \ldots$ that $\mathrm{PG}(n-1, q)$ admits a parallelism of lines. R. Baker [1] has shown if n is even, then $\mathrm{PG}(n-1, 2)$ admits a parallelism of lines.

2. Point Colorings.

Let C be a coloring of the points of $\mathcal{P}$ a projective $(n-1)$-space of order q. Evidently it is uninteresting to require all s-flats to be polychromatic. We wish then to consider the function $m_q(p; 1, s, n)$ where $2 \leq s < n$. There are no polychromatic s-flats unless there are at least $\begin{bmatrix} s \\ 1 \end{bmatrix}_q$ colors; as in our study of sets, we restrict our attention to this extreme case. In this discussion if $\mathcal{P}$ is a projective plane although we are not restricting our discussion to $\mathcal{P}(2, q)$ we will still refer to $\mathcal{P}$ as having dimension two as well as referring to points as 1-flats and lines as 2-flats. For $2 \leq s < n$ let $p = \frac{q^s-1}{q-1}$. Then p is the number of

points on a s-flat as well as the number of $(n-s+1)$-flats in $\mathcal{P}$ containing a fixed $(n-s)$-flat. Over all p-colorings of the points of $\mathcal{P}$, what is the maximum number of polychromatic s-flats supported by a coloring?

We first construct a lower bound by describing a color. We proceed recursively on the difference $n-s$. Let U be a $(n-s)$-flat. Color U recursively: if $n-s<s$ color U arbitrarily; otherwise, color U so as to obtain the maximum number of polychromatic s-flats. There are p $(n-s+1)$-flats in $\mathcal{P}$ containing U. Two points not in U have the same color if and only if they lie in the same $(n-s+1)$-flat on U. We call this coloring C_U. If $s>j$ define $m_q(p;1,s,j):=0$.

LEMMA 4.4. *For* $p=\frac{q^s-1}{q-1}$,

(1) $m_q(p;1,s,s)=1$;

(2) $m_q(p;1,s,n)\geq m_q(p;1,s,n-s)+q^{s(n-s)}$.

THEOREM 4.5. *If the points of a projective* $(n-1)$*-space* $\mathcal{P}$ *of order* q *are colored with* $p=\frac{q^{n-1}-1}{q-1}$ *colors, then there are at most* q^{n-1} *polychromatic hyperplanes. Equality is achieved only by those colorings* C_X *where* X *is a point.*

In our notation this becomes

$$m_q(\frac{q^{n-1}-1}{q-1};1,n-1,n)=q^{n-1}.$$

PROOF: Let $C=\{C_i : i\leq p\}$ be a p-coloring of the points of $\mathcal{P}$ which supports b polychromatic hyperplanes. If some color is not used then there are clearly no polychromatic hyperplanes; furthermore, if there exists a unique point of some color every polychromatic hyperplane must contain this point so there are at most p polychromatic hyperplanes. Now $p<q^{n-1}$ for $q\geq 2$ so we assume that there are at least two points of every color. There are $\frac{q^n-1}{q-1}=qp+1$ points in $\mathcal{P}$ which are being p-colored. Since $p\neq 1$ there are at most q points of some color.

Call this color red. We have seen there are at least two red points; let X be one of the red points. We distinguish two cases:

CASE 1: The red points are not collinear.

For $n = 3$ there are at least two lines on each red point that contain another red point. These lines are not polychromatic so there are at most $q-1$ polychromatic lines then on each red point. Assume $n \geq 4$. There are at least two lines ℓ, w on X each of which are incident with at least two red points. Any hyperplane on ℓ or w is not polychromatic. Each line is contained in exactly $\begin{bmatrix} n-2 \\ n-3 \end{bmatrix}_q$ hyperplanes. Since the lines ℓ and w span a rank 3 space, there are exactly $\begin{bmatrix} n-3 \\ n-4 \end{bmatrix}_q$ hyperplanes containing the span of ℓ and w. Now the number of polychromatic hyperplanes on X is at most the number of hyperplanes on X not containing ℓ or w which is

$$\frac{q^{n-1}-1}{q^{n-2}-1} - 2\frac{q^{n-2}-1}{q^{n-3}-1} + \frac{q^{n-3}-1}{q^{n-4}-1} = q^{n-2} - q^{n-3} < q^{n-2}.$$

CASE 2: The red points are collinear.

Let ℓ be the line containing all the red points. The number of polychromatic hyperplanes on X is at most the number of hyperplanes on X not containing ℓ which is

$$\frac{q^{n-1}-1}{q^{n-2}-1} - \frac{q^{n-2}-1}{q^{n-3}-1} = q^{n-2}.$$

Since a line either intersects a hyperplane in a unique point or is contained in the hyperplane, equality is possible only if every hyperplane on X not containing ℓ is polychromatic.

By counting ordered pairs (Y, w) where Y is a red point on a polychromatic line w we find there are at most q^{n-1} polychromatic hyperplanes with equality

if and only if there are exactly q red points, the red points lie on a line ℓ, and every hyperplane not containing ℓ is polychromatic.

Assume that C supports exactly q^{n-1} polychromatic hyperplanes. We wish to show that for some point X we have $C = C_X$. Our argument above then implies that some color class contains $q+1$ points while the others all contain q points. Relabeling if necessary we may assume that $|C_1| = q+1$. The points of C_1 lie in a line for if not there would be at most

$$|C_1|(q^{n-2} - q^{n-3}) = q^{n-1} - q^{n-3}$$

polychromatic hyperplanes. Therefore our supposition on C guarantees that for each $k \geq 1$ the points in C_k lie in a unique line. Denote by l_k the unique line covering the points of C_k. For $k > 1$ let $X_k := l_k \setminus C_k$. Any point in C_k for $k > 1$ lies on exactly q^{n-2} polychromatic hyperplanes.

We pause for a lemma:

LEMMA 4.6.

$$\ell_i \cap \ell_j \neq \emptyset \text{ for all } 1 \leq i, j \leq p.$$

PROOF: As all lines intersect in projective planes this is immediate if $n = 3$. Throughout the remainder of our argument we may assume that $n \geq 4$. Assume there exists a $j \in \{1, \ldots, p\}$ and $k \in \{2, \ldots, p\} \setminus \{j\}$ for which $\ell_j \cap \ell_k = \emptyset$. Let $Z \in C_k$. Then since $C_k \subset \ell_k$ we find that $Z \notin \ell_j$.

We conclude that the space Π spanned by Z and ℓ_j is a 3-flat. In a plane any two lines intersect; hence, because $\ell_j \cap \ell_k = \emptyset$ we have $\ell_k \not\subset \Pi$. Now $Z \in \ell_k$ implies the space spanned by Π and ℓ_k is a 4-flat. Any hyperplane containing Π respectively ℓ_k contains more than one point in C_j respectively C_k so it is not polychromatic. So on Z there are at most

$$\frac{q^{n-1}-1}{q-1} - \frac{q^{n-2}-1}{q-1} - \frac{q^{n-3}-1}{q-1} + \frac{q^{n-4}-1}{q-1} = q^{n-2} - q^{n-4} < q^{n-2}$$

polychromatic hyperplanes. □

We are now in a position to complete our proof of Theorem 4.5.

COMPLETION OF PROOF OF THEOREM 4.5: We assert that our coloring is simply C_{X_2}. In Lemma 4.6 letting $j = 1$ we find for all $k \in [2, p]$,

$$\emptyset \neq \ell_k \cap \ell_1 = \ell_k \cap C_1 = (\{X_k\} \cup C_k) \cap C_1 = \{X_k\} \cap C_1$$

which implies $X_k \in C_1$, for every $k \in [2, p]$. Applying Lemma 4.6 again this time with $j = 2$. We find for all $k \in [3, p]$

$$\emptyset \neq \ell_k \cap l_2 = (\{X_k\} \cup C_k) \cap (\{X_2\} \cup C_2) = \{X_k\} \cup \{X_2\}.$$

This last equation shows that $X_k = X_2$ for all $k \in [2, p]$ which is sufficient to prove our assertion. □

3. Balanced Lines.

We have shown then if we $(q + 1)$-color the points of a projective plane there are at most q^2 polychromatic lines; moreover, we have shown up to isomorphism what the coloring must be. In this section we wish to study the number of polychromatic lines in more detail. We will state our definitions for a general n, but our results will be concerned with $n = 3$ and $n = 4$. We actually solve a slightly different problem. Throughout this section $r \neq 1$ denotes a divisor of $q + 1$. If the points of a projective geometry $\mathcal{P}$ are r-colored, a line with equal number of points of each color is referred to as a *balanced* line. Polychromatic lines are simply balanced lines when $r = q+1$. Let $\varphi(n, q, r)$ denote the maximum number of balanced lines over all partitions $C = \{C_i : i \leq r\}$ of the points of $\mathcal{P}$.

So

$$\varphi(n,q,q+1) := m_q(q+1;1,2,n).$$

Let $\varphi^*(n,q,r)$ denote the maximum number of balanced lines over all partitions $C = \{C_i : i \leq r\}$ of the points of $\mathcal{P}$ where $|C_i| = \frac{1}{r}\begin{bmatrix} n \\ 1 \end{bmatrix}_q$ for all i. Notice if n is odd then trivially we have $\varphi^*(n,q,r) = 0$ since the cardinality of a set must be an integer. Evidently

$$\varphi^*(n,q,r) \leq \varphi(n,q,r).$$

Let d be a divisor of r. Given a r-coloring of the points of $\mathcal{P}$ we may partition our colors into d classes each of size r/d. We naturally then obtain a d-coloring. Any line that was balanced with respect to the r-coloring has remained balanced. We find then that

$$\varphi(n,q,r) \leq \varphi(n,q,d);$$

$$\varphi^*(n,q,r) \leq \varphi^*(n,q,d).$$

Throughout this section, $C = \{C_i : i \leq r\}$ will be a partition of the points of $\mathcal{P}$ a projective $(n-1)$-space of order q with c_i being the cardinality of C_i. For $\mathbf{x} = (x_i) \in \mathbb{Z}^r$ denote by $N(m,\mathbf{x})$ the number of m-flats of our geometry with exactly x_i points in class C_i.

LEMMA 4.7. *For* $2 \leq m \leq n-1$

(1) $\sum_{\mathbf{x}} N(m,\mathbf{x}) = \begin{bmatrix} n \\ m \end{bmatrix}_q$;

(2) $\sum_{\mathbf{x}} x_i N(m,\mathbf{x}) = c_i \begin{bmatrix} n-1 \\ m-1 \end{bmatrix}_q$;

(3) $\sum_{\mathbf{x}} x_i(x_i-1)N(m,\mathbf{x}) = c_i(c_i-1)\begin{bmatrix} n-2 \\ m-2 \end{bmatrix}_q$;

(4) *if* $i \neq j$ *then* $\sum_{\mathbf{x}} x_i x_j N(m,\mathbf{x}) = c_i c_j \begin{bmatrix} n-2 \\ m-2 \end{bmatrix}_q$;

(5) *if* $\sum_i x_i \neq \begin{bmatrix} m \\ 1 \end{bmatrix}_q$ *then* $N(m,\mathbf{x}) = 0$.

PROOF: The first equation simply counts the number of m-flats in $\mathcal{P}$. The second equation counts the number of ordered pairs (θ, S) where θ is a point in the intersection of an m-flat and the color class C_i. The third equation counts the number of ordered triples (θ, α, S) where θ and α are distinct points in C_i that lie in an m-flat S. The fourth equation is obtained similiarly but we require that α be in C_j instead of C_i. The result follows since every two distinct points determine a unique line and any flat containing these points necessarily contains this line. If $n = 3$ instead of saying m-flats we should technically say lines since our projective geometry may not be $\mathcal{P}(2, q)$, but regardless of this abuse of notation the result still holds. □

At this point let us provide some motivation. To acquire an upper bound on $\varphi(n, q, r)$ we wish to make use of the equations in Lemma 4.2. Let C be a coloring of the points that supports φ or φ^* balanced lines and assume that any m-flat with x_i points of color i has at most $f((x_i))$ balanced lines. Then since each balanced line is contained in exactly $\begin{bmatrix} n-2 \\ m-2 \end{bmatrix}_q$ m-flats we have

$$\begin{aligned} \begin{bmatrix} n-2 \\ m-2 \end{bmatrix}_q \varphi(n,q,r) &\leq \sum_{\mathbf{x}} f(\mathbf{x}) N(m, \mathbf{x}); \\ \begin{bmatrix} n-2 \\ m-2 \end{bmatrix}_q \varphi^*(n,q,r) &\leq \sum_{\mathbf{x}} f(\mathbf{x}) N(m, \mathbf{x}). \end{aligned} \tag{4.3}$$

To proceed then we need to obtain an upper bound $f(\mathbf{x})$ on the number of balanced lines in a m-flat with partition $\mathbf{x}$; moreover, our function $f(\mathbf{x})$ needs to be one for which we can evaluate or bound the righthand side of the above equations. Preferably in light of Lemma 4.7 we would like f to be a quadratic in the variables $x_1, \ldots, x_r$.

Given a coloring C of the points of a projective $(n-1)$-space we are naturally given a coloring of the points of any subset S of our points. The set S inherits

some structure from the geometry. A line in S will be a set of $q+1$ points in S which are collinear in $\mathcal{P}$.

LEMMA 4.8. *Let S be a subset of our points whose intersection with color class C_i is s_i. The number of balanced lines in S is at most*

$$\frac{rs_i(q^{n-1}-1)}{q^2-1}.$$

If i and j are distinct the number of balanced lines in S is at most

$$\frac{rs_i}{q+1}\left\lfloor\frac{rs_j}{q+1}\right\rfloor$$

with equality if and only if each point of $S \cap C_i$ is on exactly $\frac{rs_j}{q+1}$ balanced lines. Moreover if $r \neq q+1$ then the number of balanced lines in S is at most

$$\frac{r^2 s_i(s_i-1)}{(q+1)^2 - r(q+1)}.$$

PROOF: Each point is on $\frac{q^{n-1}-1}{q-1}$ lines. Count the number of ordered pairs (X,ℓ) where X is a point in $S \cap C_i$ on a balanced line ℓ. Each balanced line on $X \in S \cap C_i$ is on exactly $\frac{q+1}{r}$ points of $S \cap C_j$. Since lines have at most one intersection there are at most

$$\left\lfloor\frac{s_j}{(q+1)/r}\right\rfloor$$

balanced lines on X. The result follows by counting the number of ordered pairs (X,ℓ) where $X \in S \cap C_i \cap l$ and l is a balanced line in S. Now assume $r \neq q+1$ then each balanced line contains at least two points of each color. We count the number of ordered triples (X,Y,ℓ) where X and Y are distinct points in $S \cap C_i$ on the balanced line ℓ. For each balanced line there are $\frac{q+1}{r}(\frac{q+1}{r}-1)$ choices for the ordered pair (X,Y). Alternatively each of the $s_i(s_i-1)$ ordered pairs are covered by at most one line. □

COROLLARY 4.9. *For n even*

$$\varphi(n,q,r) \leq \frac{(q^n-1)^2}{(q^2-1)^2}.$$

For n odd

$$\varphi(n,q,r) \leq q^2\frac{(q^{n-1}-1)^2}{(q^2-1)^2}.$$

PROOF: Now assume we have been given an arbitrary coloring C of the points of our projective $(n-1)$-space with c_i points of color i. Let n be even then since there are $\frac{q^n+1}{q-1}$ points there exists distinct i and j so that $c_i + c_j \leq \frac{2(q^n-1)}{(q-1)r}$. By Lemma 4.8 then there are at most

$$\frac{r^2c_ic_j}{(q+1)^2} \leq \frac{r^2(c_i+c_j)^2}{4(q+1)^2} \leq \frac{(q^n-1)^2}{(q^2-1)^2}$$

balanced lines supported by C. The proof if $r = 2$ and $n = 3$ will be postponed until Corollary 4.13. Assume then $r \geq 3$ and n is odd. If for all distinct i and j

$$c_i + c_j \geq \frac{2q(q^{n-1}-1)}{(q-1)r} + 1,$$

then

$$2\frac{q^n-1}{q-1} = \frac{2q(q^{n-1}-1)}{q-1} + 2 = \sum_1^{r-1}(c_i + c_{i+1}) + (c_r + c_1) \geq \frac{2q(q^{n-1}-1)}{q-1} + r.$$

So we may assume then that there exists distinct colors i and j so that

$$c_i + c_j \leq \frac{2q(q^{n-1}-1)}{(q-1)r}.$$

By Lemma 4.8 then there are at most

$$\frac{r^2c_ic_j}{(q+1)^2} \leq \frac{r^2(c_i+c_j)^2}{4(q+1)^2} \leq q^2\frac{(q^{n-1}-1)^2}{(q^2-1)^2}$$

balanced lines supported by C. □

If we know $\varphi(n,q,r)$, we may actually improve the above bounds slightly. Assume for $m \geq n$ we are given an r-coloring of the points of $\mathcal{P}(m-1,q)$. By counting the number of ordered pairs (ℓ, S) where ℓ is a balanced line on a n-flat S, we find

$$\varphi(m,q,r) \leq \frac{\begin{bmatrix} m \\ n \end{bmatrix}_q \varphi(n,q,r)}{\begin{bmatrix} m-2 \\ n-2 \end{bmatrix}_q}.$$

Before we proceed any further let us modify our construction of C_U to obtain constructions of r-colorings. We proceed recursively to define a coloring of the points of our $(n-1)$-space. Let U be a $(n-2)$-flat. Color U recursively: if $n=3$, color U arbitrarily; otherwise, color U so as to obtain the maximum number of polychromatic lines. Let $\{H_i : i \leq q+1\}$ be the set of hyperplanes on U. A point off U is in some plane H_j. If j satisfies

$$1 + \frac{(i-1)(q+1)}{r} \leq j \leq \frac{i(q+1)}{r},$$

then the point is given color i. Compare this coloring with C_U in Section 2. To distinguish this from C_U, denote this coloring by C_U^*. Every line whose intersection with U is trivial is a balanced line. If we define $\varphi(1,q,r) := 0$ and $\varphi(2,q,r) := 1$, we have shown:

$$\begin{aligned} &\text{for } n \geq 3 \qquad \varphi(n-2,q,r) + q^{2n-4} \leq \varphi(n,q,r); \\ &\text{for } n \text{ even} \qquad \varphi^*(n-2,q,r) + q^{2n-4} \leq \varphi^*(n,q,r). \end{aligned} \tag{4.4}$$

For $n=3$ our lower bound and our upper bounds are equivalent. We will show that our construction above yields the unique example of a coloring with the maximum number of polychromatic lines in this case. Notice that this is basically the same result as Theorem 4.5. We will postpone the proof of uniqueness until the end of this section. Precisely we have:

THEOREM 4.10. *For $r \neq 1$ a divisor of $q+1$*

$$\varphi(3,q,r) = q^2.$$

Equality is achieved only by those colorings we denoted C_X^* where X is a point.

Notice our recursion for n odd implies

$$\varphi(n,q,r) \geq q^2 \frac{q^{2n-2}-1}{q^4-1}, \tag{4.5}$$

while for n even it implies

$$\varphi(n,q,r) \geq \frac{q^{2n}-1}{q^4-1}. \tag{4.6}$$

The dominant term in both cases is q^{2n-4}. Our upper bounds also have dominant term being q^{2n-4}, which of course is the dominant term in the expression for the number of lines contained in $\mathcal{P}$.

THEOREM 4.11.

$$\varphi^*(4,q,r) = q^4+1.$$

Equality is achieved only by C_ℓ^* where ℓ is a line.

THEOREM 4.12.

$$m_q(q+1;1,2,4) = q^4+1.$$

Equality is achieved only by C_ℓ where ℓ is a line.

We will postpone the proof of these theorems until Section 4. For each $\mathbf{x} = (x_i : i \leq r)$ an ordered partition of q^2+q+1, define

$$g(\mathbf{x}) := \frac{2r}{(r-1)(q^2+1)} \sum_{1 \leq i < j \leq r} x_i x_j - \frac{2q(q^2+q+1)}{q^2+1}.$$

Now by Lemma 4.7, we know

$$\sum_{\mathbf{x}} g(\mathbf{x})N(3,\mathbf{x}) = \frac{q^{n-2}-1}{q-1}\frac{2r}{(r-1)(q^2+1)}\sum_{1\le i<j\le r} c_ic_j - \frac{2q(q^2+q+1)}{q^2+1}\begin{bmatrix} n \\ 3 \end{bmatrix}_q.$$

The maximum of such a function occurs when all the c_i are all about equal subject to the fact that they are integers and must sum to $\frac{q^n-1}{q-1}$. Suppose instead that $c_1 - c_2 \geq 2$. Take a point from C_1 and put it into C_2 to create the coloring $C' = \{C_i'\}$. I claim the sum increases.

$$\sum_{1\le i<j\le r} c_i'c_j' = \sum_{1\le i<j\le r} c_ic_j + c_1 - c_2 - 1 > \sum_{1\le i<j\le r} c_ic_j.$$

Thus

$$\sum_{\mathbf{x}} g(\mathbf{x})N(3,\mathbf{x}) \leq \begin{cases} q^2 & \text{if } n=3 \\ (q^4+1)(q+1) & \text{if } n=4. \end{cases} \tag{4.7}$$

Equality is possible only if all the C_i's are as equal as possible.

Suppose we can find f so that

$$\sum_{\mathbf{x}} f(\mathbf{x})N(3,\mathbf{x}) \leq \sum_{\mathbf{x}} g(\mathbf{x})N(3,\mathbf{x}).$$

Using this together with (4.5) and (4.6) will show the numeric bounds in Theorem 4.10, Theorem 4.11 and Theorem 4.12. Uniqueness will necessarily be handled separately.

COROLLARY 4.13. *Assume $2|(q+1)$ and that the points of a projective $(n-1)$-space have been 2-colored red and blue. Let H be a projective plane with x_1 red points, and x_2 blue points. Assume $x_i \leq \frac{q^2+q}{2}$. Define f by*

$$f(\mathbf{x}) = \begin{cases} 0 & \text{if } x_i < \frac{q+1}{2}, \\ \frac{4x_i(x_i-1)}{q^2-1} & \text{if } \frac{q+1}{2} \leq x_i \leq \frac{q^2-1}{2}, \\ q^2-1 & \text{if } \frac{q^2+1}{2} \leq x_i \leq \frac{q^2+q}{2}-1, \\ q^2 & \text{if } \frac{q^2+q}{2} = x_i. \end{cases} \tag{4.8}$$

Then the number of balanced lines in H is at most $f(\mathbf{x}) \leq q^2$. Equality is possible only if $x_i = \frac{q^2+q}{2}$ for some i and each point in $H \cap C_i$ is on exactly q balanced lines.

PROOF: We remark that q must be odd and that necessarily $x_1 + x_2 = q^2 + q + 1$. There are also at least two points of each color on a balanced line. By symmetry we may assume that $x_2 \leq \frac{q^2+q}{2}$. In view of Lemma 4.8 we need only concern ourselves with $x_2 \geq \frac{q^2+1}{2}$. In Lemma 4.8 we found that the number of balanced lines in H was at most

$$\frac{2x_1 \left\lfloor \frac{2x_2}{q+1} \right\rfloor}{q+1}.$$

For $x_1 = \frac{q^2+q}{2}$ the claim is evident since $\frac{2}{q+1} < 1$. Notice the bound $f(\mathbf{x}) = q^2$ can be attained only when each red point is on exactly q balanced lines. Now if $x_2 = \frac{q^2+1}{2} + m$ where $0 \leq m \leq \frac{q-3}{2}$ then

$$\left\lfloor \frac{x_2}{(q+1)/2} \right\rfloor = \lfloor q - 1 + \frac{2m+2}{q+1} \rfloor = q - 1$$

which implies there are at most

$$\frac{2(q-1)x_1}{q+1} = q^2 - 1 - \frac{2m(q-1)}{q+1}$$

balanced hyperplanes. □

COROLLARY 4.14. *Assume $3 \leq r \leq q+1$ is a divisor of $q+1$ and that the points of a projective $(n-1)$-space have been r-colored by C. Let H be a projective m-flat with x_i points in color class C_i. Choose t so that $x_t \geq x_i$ for all i. Let $T := \{1, 2, \ldots, r\} \setminus \{t\}$ and define*

$$f(\mathbf{x}) := \begin{cases} 0 & \text{if } x_i < \frac{q+1}{r} \text{ for some } i, \\ \frac{2r^2}{(r-1)(r-2)(q+1)^2} \sum_{i,j \in T,\, i<j} x_i x_j & \text{otherwise.} \end{cases} \tag{4.9}$$

Then the number of balanced lines in H is at most $f(\mathbf{x})$. Furthermore if $x_i \geq \frac{q+1}{r}$ for all $i \neq t$ and H supports exactly $f(\mathbf{x})$ balanced lines, then there exists an integer d such that for $i \neq t$ $x_i = d\frac{q+1}{r}$ and each point in $H \cap C_i$ is on exactly d balanced lines in H.

PROOF: For $r \geq 3$ there are $\binom{r-1}{2} \geq 1$ choices for i and j. Applying Lemma 4.8 to each pair and adding the resulting equations yields the appropriate upper bound. As each term is nonnegative equality is possible only if we have equality term by term. □

In the following $f(\mathbf{x})$ is to be taken as in Corollary 4.13 or Corollary 4.14.

LEMMA 4.15. *Let $\mathbf{x} = (x_i : i \leq r)$ be a partition of q^2+q+1 satisfying $x_i \geq \frac{q+1}{r}$ for all i. Then*

$$f(\mathbf{x}) \leq g(\mathbf{x}).$$

Equality is possible only if

$$\{x_i\} = \{q^2 + \frac{q+1}{r}, \frac{q+1}{r}\} \text{ or } \{q\frac{q+1}{r} + 1, q\frac{q+1}{r}\}.$$

PROOF: Assume we have been given a plane whose points are partitioned into $\mathbf{x}$ and $x_i \geq \frac{q+1}{r}$ for all i. Let $x_t \geq x_i$ for all i. Since the number of points in a plane is q^2+q+1 which we are coloring with r colors, we have $x_t \geq \frac{q(q+1)}{r}+1$. Without loss of generality $t = 1$. Define $s := q^2+q+1-x_1$ then $s = \sum_2^r x_i \leq \frac{q(r-1)(q+1)}{r}$. We distinguish two cases.

CASE 1: $r = 2$.

$$g(\mathbf{x}) = \frac{4x_2(q^2+q+1-x_2) - 2q(q^2+q+1)}{q^2+1}.$$

For $\frac{q+1}{2} \leq x_2 \leq \frac{q^2-1}{2}$ since $r = 2$ is a divisor of $q+1$ we necessarily have $q \geq 3$ which implies

$$x_2 \leq \frac{q^2-1}{2} < \frac{q^3-1}{2q}.$$

Now

$$f(\mathbf{x}) - g(\mathbf{x}) = \frac{8q^2(\frac{q+1}{2} - x_2)(\frac{q^3-1}{2q} - x_2)}{q^4 - 1} \leq 0.$$

Equality is possible only if $x_2 = \frac{q+1}{2}$. Now if $\frac{q^2+1}{2} \leq x_2 \leq \frac{q^2+q}{2} - 1$ then

$$g(\mathbf{x}) \geq g((\frac{q^2+1}{2} + q, \frac{q^2+1}{2})) = \frac{q^4+1}{q^2+1} > q^2 - 1 = f(\mathbf{x}).$$

If $x_2 = \frac{q^2+q}{2}$ then

$$f(\mathbf{x}) = g(\mathbf{x}) = q^2.$$

CASE 2: $r \geq 3$. By the Cauchy-Schwartz inequality

$$\left(\sum_{2 \leq i \leq r} x_i\right)^2 \leq (r-1) \sum_{2 \leq i \leq r} x_i^2.$$

Therefore

$$\sum_{2 \leq i < j \leq r} x_i x_j = \frac{\left(\sum_{2 \leq i \leq r} x_i\right)^2 - \sum_{2 \leq i \leq r} x_i^2}{2} \leq \frac{(r-2)s^2}{2(r-1)}.$$

We should also note that

$$\sum_{1 \leq i < j \leq r} x_i x_j = x_1 \sum_{2}^{r} x_j + \sum_{2 \leq i < j \leq r} x_i x_j.$$

Now

$$\begin{aligned} f(\mathbf{x}) - g(\mathbf{x}) &= \frac{4((q+1)^2 - qr)}{(r-1)(r-2)(q+1)^2(q^2+1)} \sum_{2 \leq i < j \leq r} x_i x_j - \\ &\frac{2}{(q^2+1)(r-1)} \left(-rs^2 + rs(q^2+q+1) - (r-1)q(q^2+q+1)\right) \\ &\leq \frac{2r^2(q^2+q+1)}{(r-1)^2(q^2+1)(q+1)^2} \left[s - \frac{(r-1)(q+1)}{r}\right] \left[s - \frac{(r-1)(q+1)q}{r}\right]. \end{aligned}$$

By supposition, $\frac{(r-1)(q+1)}{r} \leq s \leq \frac{(r-1)(q+1)q}{r}$. Equality is possible only if x_i is constant for all $i \geq 2$ and $s = \frac{(r-1)(q+1)}{r}$ or $s = \frac{(r-1)(q+1)q}{r}$. □

We complete this section by showing that C_X^* where X is a point is the unique optimal coloring of points in a projective plane, optimal being defined with respect to balanced lines.

PROOF OF THEOREM 4.10: If $r = q+1$ we have already shown this in Theorem 4.5; hence, we assume that $r < q+1$. Let H be a plane whose points have been r-colored by $C = \{C_i\}$. By (4.5) we may assume C supports q^2 balanced lines. Each color must contain at least $\frac{q+1}{r}$ points or else there would not be any balanced lines. Let $x_i = |C_i|$. Now by (4.7) and Lemma 4.15 we may conclude

$$q^2 \leq f(\mathbf{x}) \leq g(\mathbf{x}) \leq q^2.$$

Our inequality being an equality implies that for $2 \leq r < q+1$ without loss of generality, H has been colored with $C = \{C_i\}$ where

$$|C_i| = \begin{cases} q\frac{q+1}{r} + 1 & \text{for } i = r, \\ q\frac{q+1}{r} & \text{for } i \neq r. \end{cases}$$

Fix $j \neq r$. There are $q\frac{q+1}{r} + 1$ points in C_r so each point in C_j is on at most q balanced lines. Since there are exactly q^2 balanced lines in our plane, each point in C_j is on exactly q balanced lines and one line having q points in C_j and one point in C_r.

Let X and Y be distinct points in C_j and let m be the unique line on X having one point in C_r. Let Z be this unique point on m in C_r. Assume Y is not on m. The line on Y and any point of $m \cap C_j \setminus X$ is then necessarily balanced. Consider now the line on Y having a unique point in C_r. This line must intersect m since H is a plane. We've just argued that it cannot be on a point of $m \cap C_j$;

therefore, it must be on Z. So far we have shown each point in C_j lies on line on Z having q points in C_j. If $r = 2$ we are then done, otherwise choose $t \neq j, r$. Now j was arbitrary so each point in C_t lies on exactly q balanced lines and one line having q points in C_t and one in C_r. Let T be a point in C_t. All lines on T must intersect the line m. We have shown that if they intersect m in C_j they are necessarily balanced. So a line on Z and a point of C_t must have q points in C_t. We conclude that $C = C_Z^*$. □

4. Projective 3-space, PG$(3, q)$.

In this section we prove Theorem 4.11 and Theorem 4.12. We are considering then r-colorings on the points of PG$(3, q)$ so as to maximize the number of balanced lines.

To prove the upper bounds, it suffices to prove that for $f(\mathbf{x})$ and $g(\mathbf{x})$ as defined in the previous sections we have

$$\sum_{\mathbf{x}} f(\mathbf{x})N(3,\mathbf{x}) \leq \sum_{\mathbf{x}} g(\mathbf{x})N(3,\mathbf{x}) \leq (q+1)(q^4+1).$$

By (4.5) we know the last inequality is true and that it is attainable only if each color class contains an equal number of points. We will need the following observation.

LEMMA 4.16. *Let $C = \{C_i : i \leq r\}$ be a partition of the points of PG$(3, q)$ so that for some i we have $|C_i| = \frac{(q^2+1)(q+1)}{r}$. Then C supports at most $q^4 - 1$ balanced lines or each plane contains at least $\frac{q+1}{r}$ points of C_i. If $r = q + 1$ and $|C_i| = q^2$, then C supports at most q^4 balanced lines or each plane contains at least 1 point of C_i.*

PROOF: Assume that points in C_i are colored red, and assume H is a plane with $j < \frac{q+1}{r}$ red points. Let C support β balanced lines. There are no balanced lines in H. Let $u = \frac{q+1}{r}$. Let A be the set of points that are neither red or in H. Then A satisfies

$$|A| = q^3 + j - (q^2+1)u \leq q^3 - 1 - q^2 u \leq (q+1-u)(q^2-q+1) - q(u-1) - 2.$$

Each balanced line on a red point of H lies on $q+1-u$ points in A. Thus there are at most $q^2 - q$ balanced lines on each red point of H. In $\mathrm{PG}(3,q)$ lines are either contained in a plane or intersect it uniquely; consequently, each red point not in H lies on at least $q-u$ points in A. There are at most q^2-1 balanced lines on each red point not in H. Let N be the number of ordered pairs (X,ℓ) where X is a red point on a balanced line ℓ. We have shown

$$\frac{q+1}{r}\beta \leq |C_i \setminus H|(q^2-1) + |C_i \cap H|(q^2-q) = \frac{q+1}{r}(q^4-1) - j(q-1).$$

For $r = q+1, |C_i| = q^2$, and $j = 0$, a similar argument shows that C supports at most q^4 balanced lines. □

PROOF OF THEOREM 4.11: The lower bound follows from (4.6). Assume we have been given a coloring $C = \{C_i\}$ of the points of $\mathrm{PG}(3,q)$ with

$$|C_i| = \frac{(q^2+1)(q+1)}{r}$$

for all i. We may assume that C supports $\beta \geq \varphi^*(4,q,r) \geq q^4+1$ balanced lines. Now if $\mathbf{x} = (x_i : i \leq r)$ is an ordered partition of q^2+q+1 then by Lemma 4.16 $N(3,\mathbf{x}) = 0$ unless $x_i \geq \frac{q+1}{r}$ for all i. So by (4.3), (4.7), and Lemma 4.15 we have

$$(q+1)(q^4+1) \leq (q+1)\beta \leq \sum_{\mathbf{x}} f(\mathbf{x})N(3,\mathbf{x})$$
$$\leq \sum_{\mathbf{x}} g(\mathbf{x})N(3,\mathbf{x}) \leq (q+1)(q^4+1).$$

We have established that $\varphi^*(n,q,r) = q^4+1$. Assume we have a coloring that achieves this bound. So if $N(3,\mathbf{x}) \neq 0$, then $f(\mathbf{x}) = g(\mathbf{x})$ and any plane with partition $\mathbf{x}$ contains exactly $f(\mathbf{x})$ balanced lines. From Lemma 4.15 it follows that we have planes of only two types. A plane is said to be of type I_j if it has partition $\mathbf{x} = (x_i)$ with

$$x_i = \begin{cases} q\frac{q+1}{r}+1 & \text{for } i = j, \\ q\frac{q+1}{r} & \text{for } i \neq j, \end{cases}$$

and it supports exactly q^2 balanced lines. A plane is said to be of type II_j if it has partition $\mathbf{x} = (x_i)$ with

$$x_i = \begin{cases} \frac{q+1}{r}+q^2 & \text{for } i = j, \\ \frac{q+1}{r} & \text{for } i \neq j, \end{cases}$$

and it supports exactly 1 balanced line.

So C supports exactly q^4+1 balanced lines only if all planes are of type I_j or II_j for some j. Assume this is the case, we wish to distinguish some line ℓ and prove C is the coloring C^*_ℓ.

Let α_j be the number of planes of type I_j, and β_j be the number of planes of type II_j. Every plane is of one of these types so

$$\sum_1^r(\alpha_j+\beta_j) = q^3+q^2+q+1.$$

By counting the number of ordered pairs (ℓ, H) where ℓ is a balanced line on a plane H we also know

$$\sum_1^r(q^2\alpha_j+\beta_j) = (q^4+1)(q+1).$$

Combining these equations yields

$$\sum_1^r \alpha_j = q^3+q^2,$$

$$\sum_1^r \beta_j = q+1.$$

Thus there exists j_0 and a plane of type II_{j_0}. Let ℓ be the balanced line on this plane. We assert $C = C^*_\ell$.

Let α^ℓ_j be the number of planes on ℓ of type I_j and β^ℓ_j be the number of planes on ℓ of type II_j. Every plane on ℓ is of one of these two types so

$$\sum_1^r (\alpha^\ell_j + \beta^\ell_j) = q + 1.$$

Fix $s, 1 \leq s \leq r$ and count the number of ordered pairs (X, H) where X is a point in $H \cap C_s$ and H is a plane on ℓ. If X is on ℓ, then it is in every plane on ℓ; if it is not on ℓ, then it is on a unique plane on ℓ. So we have

$$\begin{aligned}\frac{q+1}{r}(q+1) + \frac{q^2(q+1)}{r}1 \\ = (\frac{q(q+1)}{r} + 1)\alpha^\ell_s + (\frac{q+1}{r} + q^2)\beta^\ell_s + \sum_{j \neq s}(\frac{q(q+1)}{r}\alpha^\ell_j + \frac{q+1}{r}\beta^\ell_j).\end{aligned}$$

Combining these two relationships we have:

$$\alpha^\ell_s + q^2\beta^\ell_s + \sum_{j=1}^r \frac{q^2-1}{r}\alpha^\ell_j = q^2\frac{q+1}{r}. \tag{4.10}$$

For every $s, 1 \leq s \leq r$ we have then that

$$r\alpha^\ell_s \equiv k \pmod{q^2}$$

where $k = \sum_1^r \alpha^\ell_j$ is constant. The integer r is invertible mod q^2 since $r \neq 1$ is a divisor of $q+1$ implies r and q^2 are relatively prime. Therefore, α^ℓ_s is constant mod q^2. As α^ℓ_s is a nonnegative integer bounded above by $q+1$ we actually have that α^ℓ_s is constant. By (4.10) then we find β^ℓ_s is also constant and these constants satisfy:

$$\alpha^\ell_s + \beta^\ell_s = \frac{q+1}{r}. \tag{4.11}$$

By our choice of ℓ we know that $\beta_{j_0}^{\ell} \neq 0$. So for each j, $1 \leq j \leq r$ we have at least one plane of type II_j. If $r = q+1$, then we immediately see that our coloring C is C_{ℓ}^{*}. Otherwise $r \leq q-1$. In this case label our planes on ℓ H_i where for $1 \leq i \leq r$ we assume the plane H_i is of type II_i. Now recall by our definition of planes of type II_i that if X is a point off ℓ on a plane of type II_i, then X is in C_i. Consider a line in $\mathrm{PG}(3,q)$ that intersects ℓ trivially. It necessarily then contains $\beta_s^{\ell} \geq 1$ points of each color. We need the following claim whose proof will be given later.

CLAIM 4.17: Each line in $\mathrm{PG}(3,q)$ is either balanced, monochromatic, or is two colored with a unique point of one color. Furthermore, each plane of type I_j contains $\frac{q+1}{2}$ monochromatic lines while planes of type II_j contain $\frac{q(q+1)}{2}$ monochromatic lines.

Assuming our claim then our line is two colored or it is balanced. We distinguish two cases:

CASE 1. $r \geq 3$:

As we have at least three colors on this line. That is to say every line that intersects ℓ trivially is a balanced line. There are q^4 such lines. Since ℓ is chosen as a balanced line and our coloring supports exactly q^4+1 balanced lines any line other than ℓ that intersects ℓ nontrivially is not balanced. Our planes on ℓ then all must be of type II_j for some j. There are then by (4.11) exactly $\frac{q+1}{r}$ planes of type II_j for each $1 \leq j \leq r$. We have then that $C = C_{\ell}^{*}$.

CASE 2. $r = 2$.

Let ν be the number of lines in C_1, τ the number of lines in C_2, μ the number of lines that have q points in C_1, and σ the number of lines that have q points

in C_2. The number of unbalanced lines is then

$$\nu + \mu + \sigma + \tau = q^3 + 2q^2 + q.$$

An edge in C_i is an ordered pair (X, Y) of distinct points $X, Y \in C_i$. Count the number of edges in C_i.

$$\binom{q+1}{2}\nu + \binom{q}{2}\mu + \binom{\frac{q+1}{2}}{2}(q^4+1) = \binom{\frac{(q^2+1)(q+1)}{2}}{2};$$

$$\binom{q+1}{2}\tau + \binom{q}{2}\sigma + \binom{\frac{q+1}{2}}{2}(q^4+1) = \binom{\frac{(q^2+1)(q+1)}{2}}{2}.$$

Solving these equations we have

$$\nu + \tau = \mu + \sigma = \frac{q(q+1)^2}{2}.$$

Every monochromatic line is in a unique plane H_i for some i. Let us count the number of monochromatic lines. Each plane of type I_j contains $\frac{q+1}{2}$ monochromatic lines while planes of type II_j contain $\frac{q(q+1)}{2}$ monochromatic lines. The number of monochromatic lines is $\nu + \tau$.

$$\sum_{j=1}^{2}\left(\frac{q+1}{2}\alpha_j^\ell + \frac{q(q+1)}{2}\beta_j^\ell\right) = \frac{q(q+1)^2}{2}.$$

Since α_j^ℓ and β_j^ℓ are constant and by (4.11) their sum is $\frac{q+1}{2}$ we conclude

$$\beta_j^\ell = \frac{q+1}{2} \qquad \text{for } j = 1, 2.$$

As before this implies $C = C_\ell^*$. □

PROOF OF CLAIM 4.17: Let H be a plane of type II_r. Since we have a unique balance line which covers exactly $\frac{q+1}{r} = x_i$ points of $C_i \cap H$ for $1 \le i \le r-1$, we have that the points of C_i for $1 \le i \le r-1$ are collinear. Since lines intersect

uniquely all of our line must be two colored or contained in C_r. There are then exactly $\frac{q(q+1)}{r}$ monochromatic lines.

Let H be a plane of type I_r then by Lemma 4.10 $C|_H = C_X^*$ for some point X. There are then exactly $\frac{q+1}{r}$ balanced lines, and all lines are two colored, balanced, or monochromatic. □

Let us now consider $m_q(q+1;1,2,4)$.

PROOF OF THEOREM 4.12: By (4.6) it suffices to consider the upper bound. Let $C = \{C_i : i \leq q+1\}$ be a coloring of the points of $\mathrm{PG}(3,q)$ that supports $\beta \geq q^4+1$ polychromatic lines. If for some distinct i,j we had $|C_i| + |C_j| \leq 2q^2$, then by Lemma 4.8

$$q^4 + 1 \leq \beta \leq |C_i||C_j| \leq q^4.$$

So we may assume that for all distinct i,j we have

$$|C_i| + |C_j| \geq 2q^2 + 1.$$

Now fix j; since

$$\sum_{i=1}^{q+1} |C_i| \geq 2q^3 + q - |C_j|(q-1)$$

we find

$$(q-1)|C_j| \geq q^2(q-1) - 1.$$

Equality is possible only if $|C_i| = 2q^2 + 1 - |C_j|$ for all $i \neq j$. Thus

$$|C_j| \geq \begin{cases} q^2 & \text{if } q \neq 2, \\ 3 & \text{if } q = 2. \end{cases}$$

Our choice of j was arbitrary so relabeling if necessary we conclude that one of the following occur

(1) $q = 2$ and $|C_1| = 3, |C_2| = |C_3| = 6$;

(2) $|C_1| = q^2, |C_2| = q^2 + 2$, and $|C_i| = q^2 + 1$ for $i \notin \{1,2\}$;

(3) $|C_i| = q^2 + 1$ for $1 \leq i \leq q+1$.

Assume we have the situation of (1). Each point is on seven lines. If the points in C_1 are not collinear, then each point in C_1 is on at most five polychromatic lines. This gives a total of at most fifteen polychromatic lines. Assume the points in C_1 are collinear. There are four planes on this line each of which by Theorem 4.5 contain at most four polychromatic lines. Every polychromatic line must contain a point in C_1, thus there are at most sixteen polychromatic lines in this situation.

So we either have the case where all colors classes contain equal number of points, or we have the slightly skew case. As in the proof of Theorem 4.11, if all planes have at least one point of each color

$$(q+1)(q^4+1) \leq (q+1)\beta \leq \sum_{\mathbf{x}} f(\mathbf{x})N(3,\mathbf{x}) \leq \sum_{\mathbf{x}} g(\mathbf{x})N(3,\mathbf{x}) \leq (q+1)(q^4+1).$$

We therefore have equality; the last inequality being equality implies that all color classes contain equal number of points. By appealing to Theorem 4.11 we are done.

So assume there exists a plane H with no points of some color. By Lemma 4.16, we necessarily have $H \cup C_1 = \emptyset$ and $H \cup C_i \neq \emptyset$ otherwise. Let $|H \cup C_j| = x_j$. Now since $1 \leq x_j \leq |C_j| \leq q^2+1$ for $j \neq 1$ and the sum $\sum_{j=2}^{q+1} x_j = q^2+q+1$, we may conclude that the most unevenly distributed partition has one element equal to q^2+1, one element equal to 2, and $q-2$ elements equal to 1. We have seen in the proof of (4.7) that a sum of the form $\sum x_i x_j$ increases as the x_i's approach their average. We have then that

$$\sum_{1 \leq i < j \leq q+1} x_i x_j \geq g((0, q^2+1, 2, 1, \ldots, 1)) = \frac{2q^3+q^2+q-2}{2},$$

which implies $g(\mathbf{x}) > 0 = f(\mathbf{x})$. In this case we find

$$(q+1)(q^4+1) \leq (q+1)\beta \leq \sum_{\mathbf{x}} f(\mathbf{x})N(3,\mathbf{x}) < \sum_{\mathbf{x}} g(\mathbf{x})N(3,\mathbf{x}) \leq (q+1)(q^4+1).$$

We conclude if some plane contains no points of one color, C supports fewer than $q^4 + 1$ polychromatic lines. $\square$

BIBLIOGRAPHY

[1] R. D. Baker, Partitioning the planes of $AG_{2m}(2)$ into 2-designs, *Discrete Math.* **15** (1976), 205–211.

[2] A. Beutelspacher, On parallelisms in finite projective spaces, *Geometriae Dedicata* **3** (1974), 35–40.

[3] A. E. Brouwer, Packing and covering of $\binom{k}{t}$-sets, *Packing and Covering in Combinatorics* (ed. A. Schrijver), Mathematical Centre Tracts **106**, 1979.

[4] A. E. Brouwer and A. Schrijver, Uniform hypergraphs, *Packing and Covering in Combinatorics* (ed. A. Schrijver), Mathematical Centre Tracts **106**, 1979.

[5] A. E. Brouwer, J. B. Shearer, N. J. A. Sloane, W. D. Smith, A new table of constant weight codes, *I.E.E.E. Information Theory* **36** (1990), 1334–1380.

[6] L. Chouinard II, Partitions of the 4-subsets of a 13-set into disjoint projective planes, *Discrete Mathematics* **45** (1983), 297–300.

[7] H. Enomoto, P. Frankl, N. Ito, and K. Nomura, Codes with given distance, *Graphs and Combinatorics* **3** (1987), 25–38.

[8] T. Etzion, Optimal partitions for triples, to appear.

[9] T. Etzion, Partitions of triples into optimal packings, to appear.

[10] P. Frankl, Orthogonal vectors in the n-dimensional cube and codes with missing distances, *Combinatorica* **6** (1986), 279–285.

[11] M. Hall Jr., *Combinatorial Theory 2nd ed.*, John Wiley and Sons, New York, 1986.

[12] J. Hirschfeld, *Projective Geometries over Finite Fields*, Oxford University Press, Oxford, 1979.

[13] E. Kramer, D. Mesner, Intersections among steiner systems, *J. Combinatorial Theory (A)* **16** (1974), 273–285.

[14] J. X. Lu, On large sets of disjoint steiner triple systems, I–III *J. Combinatorial Theory (A)* **34** (1983), 140–183; IV–VI **37** (1984), 136–192.

[15] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Mathematical Library **16**, Elsevier Science Publishers, New York, 1977.

[16] R. J. McEliece, *The Theory of Information and Coding*, Cambridge University Press, Cambridge, 1977.

[17] J. E. Olson, A combinatorial problem on finite abelian groups, *J. Number Theory* **1** (1969), 8–10.

[18] B. Rothschild and P. Frankl, Personal correspondence.

[19] R. P. Stanley, *Enumerative Combinatorics, Volume I*, Wadsworth, Monterey, California, 1986.

[20] L. Teirlinck, A completion of Lu's determination of the spectrum for large sets of disjoint Steiner systems, to appear in *J. Combinatorial Theory (A)*.

[21] J. van Lint, *Introduction to Coding Theory*, Graduate Texts in Mathematics **86**, Springer Verlag, New York, 1982.