Upper and Lower Bounds on Permutation Codes of Distance Four

by

NATALIE SAWCHUCK
B.Sc. University of Alberta, 2005

A Dissertation Submitted in Partial Fulfillment of the
Requirements for the Degree of

MASTER OF SCIENCE

in the Department of Mathematics and Statistics

Upper and Lower Bounds on Permutation Codes of Distance Four

by

Natalie Sawchuck

B.Sc. University of Alberta, 2005

Supervisory Committee

Dr. Peter Dukes, Supervisor

(Department of Mathematics and Statistics)

Dr. Kieka Mynhardt, Departmental Member

(Department of Mathematics and Statistics)

Dr. Jing Huang, Departmental Member

(Department of Mathematics and Statistics)

Supervisory Committee

Dr. Peter Dukes, Supervisor
(Department of Mathematics and Statistics)

Dr. Kieka Mynhardt, Departmental Member
(Department of Mathematics and Statistics)

Dr. Jing Huang, Departmental Member
(Department of Mathematics and Statistics)

Abstract

A permutation array, represented by $PA(n, d)$, is a subset Γ of $\mathcal{S}_n$ such that any two distinct elements of Γ have a distance of at least d where d is the number of differing positions. We analyze the upper and lower bounds of permutation codes with distance equal to 4. An optimization problem on Young diagrams is used to improve the upper bound for almost all n while the lower bound is improved for small values of n by means of recursive construction methods.

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

Permutation codes have been present in coding theory for many years and their structure produces some interesting coding bounds. In coding theory the maximum size of a set of codewords and the minimum distance between codewords are constantly examined. To begin, some background definitions will be established.

The *length* of a codeword is the number of elements the codeword contains. If a given code C has length n, then a codeword in C has the form $(c_1, c_2, ..., c_n)$, where each c_i is an element in the alphabet of C. In coding theory, the Hamming distance is defined as the number of differing positions between two distinct codewords. The *minimum distance* d of a code can be defined as the least number of positions that any two codewords in C differ.

The symmetric group of degree n, denoted $\mathcal{S}_n$, is the group of all permutations on n symbols. The identity permutation is represented by ϵ. Two permutations $\sigma, \tau \in \mathcal{S}_n$ are at *distance* d if $\sigma\tau^{-1}$ has exactly $n - d$ fixed points.

A *permutation code* of distance d is a subset Γ of $\mathcal{S}_n$ such that the distance between members of Γ is at least d. As a result, permutation codes have alphabet size n, equal to the length, and $c_i \neq c_j$ for every element in a codeword. Also, permutation codes have minimum distance at least two since a transposition is the smallest change that can be made to a codeword.

A permutation code of size s can be represented by an $s \times n$ array whose rows represent the image of $(1, 2, ..., n)$ under the s permutations that satisfy the minimum distance, as defined in Chu et al. [2]. Such a permutation array is referred to as a $PA(n, d)$.

We will denote by $M(n, d)$ the maximum size of a $PA(n, d)$. Several $M(n, d)$ values have been determined for particular d as well as some useful upper bounds. The following are well-known consequences of the definitions from Deza and Vanstone [5].

Proposition 1.1. [5]

(a) $M(n, 2) = n!$.

(b) $M(n, 3) = n!/2$.

(c) $M(n, n) = n$.

(d) $M(n, d) \leq nM(n-1, d)$.

(e) $M(n, d) \leq n!/(d-1)!$.

Proof. (a) From the definition, the number of permutations of an alphabet of size n is $n!$. A permutation is a product of transpositions (exchange of any two elements) and any two distinct permutations differ by at least one transposition, thus having distance at least two. Therefore the maximum $PA(n, 2)$ will be the set of all possible permutations, $\mathcal{S}_n$.

(b) Consider the alternating group $\Gamma = \mathcal{A}_n$ having minimum distance three. The quotient of two permutations in $\mathcal{A}_n$ is also in $\mathcal{A}_n$ and therefore cannot be a single transposition.

(c) In order to have minimum distance between codewords equal to n all distinct codewords must differ in every single position. The lower bound for the desired permutation array is represented by taking Γ to be a cyclic subgroup of $\mathcal{S}_n$ order n. Finally, among any $n + 1$ permutations, two agree in at least one position.

(d) Consider a subarray of a $PA(n, d)$ consisting of all the rows whose first entry is k. Deleting the first column of this subarray creates a PA with elements $\{1, ..., n\} \setminus \{k\}$ and minimum distance d. Clearly it is possible to create at most n subarrays in this way.

(e) First observe that $n!/(d-1)! = n(n-1)(n-2)\cdots d$. Apply Proposition 1.1 (d) to the right side of itself exactly $(n-d)$ times to obtain $M(n, d) \leq n(n-1)(n-2)...(n-(n-(d+1)))M(n-(n-d), d)$. Now by applying Proposition 1.1 (b) we obtain the desired result. $\square$

The majority of investigations of $M(n, d)$ involve a large distance d but we consider $d = 4$ which, as demonstrated above, is the smallest undecided distance.

The Gilbert-Varshamov bound on $M(n, d)$ is an interesting lower bound to consider. A *derangement* of order k is an element of $\mathcal{S}_k$ having no fixed points. The number of derangements is denoted D_k. The set of all permutations having distance $\leq r$ from the element $\sigma \in \mathcal{S}_n$ creates a ball with radius r centered at σ. The volume of this ball is $V(n, r) = \displaystyle\sum_{k=0}^{r} \binom{n}{k} D_k$.

Proposition 1.2. [7] $M(n, d) \geq n!/V(n, d-1)$.

Proof. For this bound, consider the greedy algorithm construction. Pick any codeword $\sigma \in \mathcal{S}_n$. Add σ to Γ and throw away the contents of the ball centered at σ with radius $d-1$. Thus, $n! - V(n, d-1)$ codewords remain. Step by step add codewords to Γ by alternately picking codewords from $n! - |\Gamma| \cdot V(n, d-1)$ and throwing away the contents of the ball centered at the new codeword with radius $d-1$. Repeat until $n! - |\Gamma| \cdot V(n, d-1)$ is non-positive. Since $|\Gamma| \leq M(n, d)$ we have $n! - M(n, d) \cdot V(n, d-1) \leq 0$. $\square$

The Gilbert-Varshamov lower bound, specialized to $d = 4$, is

$$M(n, 4) \geq \frac{6n!}{2n^3 - 3n^2 + n + 6}. \tag{1.1}$$

Lower bounds on the size of permutation arrays using computational and recursive constructions have been researched by Chu, Colbourn and Dukes in [2]. It is possible to construct, through recursive methods in [2], permutation codes of minimum distance 4 which come close to or improve (1.1) for small values of n. Chapter 2 extends the work of Chu et al. to demonstrate a recursive construction and lower bound for a $PA(n, 4)$ presented in Theorem 2.13.

The sphere-packing bound is an upper bound for a $PA(n, d)$. If spheres are packed into a finite space, then the sum of the volume of the spheres cannot exceed the total volume of the entire space, creating an upper bound. The sphere-packing bound below considers balls of radius $\lfloor (d-1)/2 \rfloor$.

Proposition 1.3. [2] $M(n,d) \leq \frac{n!}{V(n,\lfloor \frac{d-1}{2} \rfloor)}$.

Unfortunately, the sphere-packing upper bound for $d = 4$ is simply $n!$. Although distance four has not been explicitly considered on its own, the following improvement for $d = 4$ was essentially known to Frankl and Deza in early investigations [7].

Proposition 1.4. $M(n,4) \leq (n-1)!$.

Proof. Consider for each $\sigma \in \mathcal{S}_n$ the set of all n words $A_\sigma = \{\sigma\} \cup \{(1i)\sigma : 2 \leq i \leq n\}$. We have $|A_\sigma| = n$ for any σ. Given a permutation code $\Gamma \subset \mathcal{S}_n$ of distance 4, it suffices to show that if $\sigma \neq \tau$ are both in Γ, then $A_\sigma \cap A_\tau = \emptyset$. Assume without loss of generality that the identity $\epsilon = 123 \cdots n \in A_\sigma \cap A_\tau$. If either σ or τ equals ϵ, then their distance is only two, a contradiction. So $\sigma = (1i)$ and $\tau = (1j)$ for some $1 < i < j \leq n$. But then $\sigma\tau^{-1} = (1ji)$ and σ, τ are at distance 3, another contradiction. $\square$

Tarnanen [13] used the theory of association schemes to establish an important upper bound on permutation codes by way of linear programming, (LP). For example, it was shown that $M(7,4) \leq 543$, an improvement on Proposition 1.4.

Chapters 3 and 4 set up necessary definitions and theory for the linear programming bound. In Chapter 5 an explicit LP upper bound is given for distance 4. The upper bound of Theorems 5.2 and 5.4 are an improvement of Proposition 1.4 for infinitely many n.

Chapter 2

Recursive Construction of $PA(n,4)$ for small n

A $PA(2m,4)$ (in fact, a collection of disjoint $PA(2m,4)$) can be constructed recursively from two sets of disjoint $PA(m,4)$. The disjoint $PA(m,4)$ are concatenated according to a constant weight binary code with length $2m$, weight m and distance 4. The basis cases are $n = 4, 5, 6$, where exact values of $M(n,4)$ for $n = 4, 5, 6$ are obtained by sharply k-transitive permutation groups for $k = 1, 2, 3$.

2.1 Sharply k-Transitive Groups

A permutation group G acting on n points is *k-transitive* if given any two lists of distinct points $u_1, \ldots, u_k$ and $v_1, \ldots, v_k$, there is a group element $g \in G$ which maps u_i to v_i for each i between 1 and k. If the element g is unique then the group G is said to be *sharply k-transitive*.

Proposition 2.1. [7] *Regarded as a permutation code, a sharply k-transitive permutation group of degree n has a minimum distance of $n-k+1$.*

In general there are $n(n-1)\ldots(n-k+1)$ elements of a sharply k-transitive group. If G is a sharply k-transitive group acting on $X = \{1, \ldots, n\}$ with $g, h \in G, (g \neq h)$, it follows that $g(1, 2, \ldots, n)$ and $h(1, 2, \ldots, n)$ agree in at most $k-1$ positions [2]. Since no two codewords can agree in k or more places the existence of a sharply k-transitive group is equivalent to a maximum cardinality $PA(n, n-k+1)$. This was first pointed out in Frankl and Deza [7]. The case $k = 2$ is relevant when n is a prime-power, denoted q.

Proposition 2.2. [7] *If q is a prime-power, then*

$$M(q, q-1) = q(q-1).$$

Consider a finite field $\mathbb{F}_q$ of order q. The sharply 2-transitive group

$AGL(1,q)$ of linear transformations $x \mapsto ax+b, a \neq 0$ acting on $\mathbb{F}_q$ is a special case of Proposition 2.2. Therefore the permutations acting on the group are linear functions.

Proposition 2.3. [7] *If q is a prime-power, then*

$$M(q+1, q-1) = (q+1)q(q-1).$$

A special case of Proposition 2.3 arises from the sharply 3-transitive group $PGL(2,q)$ of fractional linear transformations $x \mapsto (ax+b)/(cx+d), ad-bc \neq 0$ acting on $X = \mathbb{F}_q \cup \{\infty\}$, where $\infty \mapsto a/c$ if $c \neq 0$ and $\infty \mapsto \infty$ if $c = 0$. Consider two cases:

If $c = 0$, $d = 1$ then $x \mapsto (ax+b)/(cx+d)$ simplifies to $x \mapsto ax+b$. This accounts for $q(q-1)$ permutations.

If $c \neq 0$, then $x \mapsto \frac{1}{c}(a'x+b')/(x+d')$ and $a'd' \neq b'$, which gives $q^2(q-1)$ permutations. Finally, $q(q-1) + q^2(q-1) = (q+1)q(q-1)$.

2.2 Small Disjoint $PA(n, 4)$

Lemma 2.4. [2] *For all* $n \geq 4$*, there are six disjoint* $PA(n, 4)$ *of size* $M(n, 4)$*.*

Proof. For a given a $PA(n, 4)$, 6 disjoint $PA(n, 4)$ of the same size can be created by applying all possible permutations to the last three columns. Any new codeword created will either differ because of the column permutations or from the first $n - 3$ positions and therefore all new codewords will be disjoint from the original $PA(n, 4)$. The same permutation is applied to every codeword of the $PA(n, 4)$; therefore distance 4 is preserved. □

We now consider various small values of n.

Example 2.5. From Proposition 2.1 a sharply 1-transitive group of size n has minimum distance n. A sharply 1-transitive group can be created by cyclic shifts of the identity codeword. From Proposition 1.1 (c) we have a $M(4, 4) = 4$.

1	2	3	4
2	3	4	1
3	4	1	2
4	1	2	3

Construction of the remaining five $PA(4,4)$ applies Lemma 2.4 to obtain 6 disjoint $PA(n,4)$, accounting for all $4! = 24$ permutations of length 4.

$$\begin{array}{|cccc|}\hline 1&2&3&4\\ 2&3&4&1\\ 3&4&1&2\\ 4&1&2&3\\ \hline\end{array}\quad
\begin{array}{|cccc|}\hline 1&2&4&3\\ 2&3&1&4\\ 3&4&2&1\\ 4&1&3&2\\ \hline\end{array}\quad
\begin{array}{|cccc|}\hline 1&3&2&4\\ 2&4&3&1\\ 3&1&4&2\\ 4&2&1&3\\ \hline\end{array}\quad
\begin{array}{|cccc|}\hline 1&3&4&2\\ 2&4&1&3\\ 3&1&2&4\\ 4&2&3&1\\ \hline\end{array}\quad
\begin{array}{|cccc|}\hline 1&4&2&3\\ 2&1&3&4\\ 3&2&4&1\\ 4&3&1&2\\ \hline\end{array}\quad
\begin{array}{|cccc|}\hline 1&4&3&2\\ 2&1&4&3\\ 3&2&1&4\\ 4&3&2&1\\ \hline\end{array}$$

The 6 disjoint $PA(4,4)$ consist of the symbols 1, 2, 3, 4. In order to obtain another 6 disjoint $PA(4,4)$ which will be used to concatenate to the original 6, a copy is made by adding 4 to each element.

$$\begin{array}{|cccc|}\hline 5&6&7&8\\ 6&7&8&5\\ 7&8&5&6\\ 8&5&6&7\\ \hline\end{array}\quad
\begin{array}{|cccc|}\hline 5&6&8&7\\ 6&7&5&8\\ 7&8&6&5\\ 8&5&7&6\\ \hline\end{array}\quad
\begin{array}{|cccc|}\hline 5&7&6&8\\ 6&8&7&5\\ 7&5&8&6\\ 8&6&5&7\\ \hline\end{array}\quad
\begin{array}{|cccc|}\hline 5&7&8&6\\ 6&8&5&7\\ 7&5&6&8\\ 8&6&7&5\\ \hline\end{array}\quad
\begin{array}{|cccc|}\hline 5&8&6&7\\ 6&5&7&8\\ 7&6&8&5\\ 8&7&5&6\\ \hline\end{array}\quad
\begin{array}{|cccc|}\hline 5&8&7&6\\ 6&5&8&7\\ 7&6&5&8\\ 8&7&6&5\\ \hline\end{array}$$

The 12 disjoint $PA(4,4)$ will be combined to construct a $PA(8,4)$, as demonstrated later in this chapter.

Example 2.6. A $PA(5,4)$ is generated by the sharply 2-transitive group $AGL(1,q)$ of linear transformations $x \mapsto ax+b$ acting on $\mathbb{F}_q$. For $q=5$, a is one of 1, 2, 3 or 4 (note: if $a=0$, $x \mapsto b$ which is not a permutation therefore $a \neq 0$) and b is one of 0, 1, 2, 3, 4. Thus there exist $4 \cdot 5 = 20$ codewords with minimum distance 4. This is an instance of Proposition 2.2.

$$\begin{array}{ccccc} 2 & 3 & 4 & 5 & 1 \\ 3 & 4 & 5 & 1 & 2 \\ 4 & 5 & 1 & 2 & 3 \\ 5 & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 & 5 \end{array} \qquad \begin{array}{ccccc} 3 & 5 & 2 & 4 & 1 \\ 4 & 1 & 3 & 5 & 2 \\ 5 & 2 & 4 & 1 & 3 \\ 1 & 3 & 5 & 2 & 4 \\ 2 & 4 & 1 & 3 & 5 \end{array} \qquad \begin{array}{ccccc} 4 & 2 & 5 & 3 & 1 \\ 5 & 3 & 1 & 4 & 2 \\ 1 & 4 & 2 & 5 & 3 \\ 2 & 5 & 3 & 1 & 4 \\ 3 & 1 & 4 & 2 & 5 \end{array} \qquad \begin{array}{ccccc} 5 & 4 & 3 & 2 & 1 \\ 1 & 5 & 4 & 3 & 2 \\ 2 & 1 & 5 & 4 & 3 \\ 3 & 2 & 1 & 5 & 4 \\ 4 & 3 & 2 & 1 & 5 \end{array}$$

Now apply Lemma 2.4 to obtain 5 more disjoint $PA(5,4)$. One of these is shown below, arising from the permutation (23) on the last three columns.

$$\begin{array}{ccccc} 2 & 3 & 4 & 1 & 5 \\ 3 & 4 & 5 & 2 & 1 \\ 4 & 5 & 1 & 3 & 2 \\ 5 & 1 & 2 & 4 & 3 \\ 1 & 2 & 3 & 5 & 4 \end{array} \qquad \begin{array}{ccccc} 3 & 5 & 2 & 1 & 4 \\ 4 & 1 & 3 & 2 & 5 \\ 5 & 2 & 4 & 3 & 1 \\ 1 & 3 & 5 & 4 & 2 \\ 2 & 4 & 1 & 5 & 3 \end{array} \qquad \begin{array}{ccccc} 4 & 2 & 5 & 1 & 3 \\ 5 & 3 & 1 & 2 & 4 \\ 1 & 4 & 2 & 3 & 5 \\ 2 & 5 & 3 & 4 & 1 \\ 3 & 1 & 4 & 5 & 2 \end{array} \qquad \begin{array}{ccccc} 5 & 4 & 3 & 1 & 2 \\ 1 & 5 & 4 & 2 & 3 \\ 2 & 1 & 5 & 3 & 4 \\ 3 & 2 & 1 & 4 & 5 \\ 4 & 3 & 2 & 5 & 1 \end{array}$$

As with Example 2.5, we will add 5 to each element in order to create another 6 disjoint $PA(5,4)$. The 12 disjoint $PA(5,4)$ will be combined to construct a $PA(10,4)$, mentioned later in this chapter.

Example 2.7. A $PA(6,4)$ is generated by the sharply 3-transitive group $PGL(2,q)$ of fractional linear transformations $x \mapsto (ax+b)/(cx+d), ad-bc \neq 0$ acting on $X = \mathbb{F}_q \cup \{\infty\}$. From Proposition 2.3 this gives $M(6,4) = 120$. Again, $\mathcal{S}_6$ is partitioned into 6 $PA(6,4)$ of this size.

2.3 Constant Weight Binary Codes

A binary word is a sequence of elements from the alphabet $\{0,1\}$. A *constant weight binary code* with length n, distance d and weight w has w occurrences of 1 and $n-w$ occurrences of 0 in each codeword and is written $A(n,d,w)$.

Lemma 2.8. [10] *The set $\mathbb{U}_w^n$ of all $\binom{n}{w}$ constant weight binary codewords can be partitioned into n disjoint constant weight binary codes, each with Hamming distance 4.*

Proof. Let $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ denote the residue classes modulo n. Consider the map

$$T : \mathbb{U}_w^n \to \mathbb{Z}_n$$

whose value at $\mathbf{a} = (a_0, \ldots, a_{n-1}) \in \mathbb{U}_w^n$ is

$$\begin{aligned} T(\mathbf{a}) &= \sum_{a_i=1} i \pmod n \\ &= \sum_{i=0}^{n-1} i a_i \pmod n. \end{aligned} \tag{2.1}$$

For $0 \le i \le n-1$ let C_i be the constant weight code $T^{-1}(i)$. We claim that the Hamming distance between any two distinct codewords of C_i, say $\mathbf{a}$ and $\mathbf{b}$, is at least four. For suppose it is two. Since $\mathbf{a}$ and $\mathbf{b}$ agree everywhere except for two positions, in one (say the rth) $\mathbf{a}$ is one and $\mathbf{b}$ is zero and in another (say the sth) $\mathbf{a}$ is zero and $\mathbf{b}$ is one. But $T(\mathbf{a}) = T(\mathbf{b}) = i$, so from 2.1

$$T(\mathbf{a}) = x + r = i \pmod{n},$$

$$T(\mathbf{b}) = x + s = i \pmod{n}$$

for some $x \in \mathbb{Z}_n$. This implies $r \equiv s (\text{mod } n)$, which is impossible. Thus C_i has a Hamming distance of at least four between its codewords. □

Corollary 2.9. [10] $A(n, 4, w) \geq \frac{1}{n}\binom{n}{w}$

Proof. From Lemma 2.8

$$|C_0| + |C_1| + \cdots + |C_{n-1}| = \binom{n}{w},$$

so for at least one j,

$$|C_j| \geq \frac{1}{n}\binom{n}{w}.$$

□

It is interesting to note that if n is of the form 2^k, $3{\cdot}2^k$ or $5{\cdot}2^k$, $(k \geq 2)$ and w is even then Brouwer et al. [1] proved that Corollary 2.9 can be replaced by

$$A(n,4,w) \geq \frac{1}{n-1}\binom{n}{w}.$$

Definition 2.10. Given a set of disjoint constant weight or permutation codes of sizes $c_1, c_2, \ldots, c_t$ we define their *norm* as

$$|c_1|^2 + |c_2|^2 + \cdots + |c_t|^2.$$

We require a basic inequality derived from the Cauchy-Schwarz inequality.

Lemma 2.11. *If* $x_1 + \cdots + x_n = N$, *then*

$$x_1^2 + \cdots + x_n^2 \geq \frac{N^2}{n},$$

with equality if and only if $x_i = \dfrac{N}{n}$ *for each* $i = 1, \ldots, n$.

Example 2.12. We will illustrate the construction of Lemma 2.8 to show $A(6,4,3) \geq 4 > \frac{20}{6}$. Take $n = 6$ and $w = 3$. All $\binom{6}{3} = 20$ constant weight codewords are partitioned into 6 disjoint constant weight binary codes with distance 4. Using the mapping T, we have for instance

$$110100 \mapsto 0 + 1 + 3 = 4.$$

Checking cases,

$$
\begin{aligned}
T^{-1}(0) &= \{000111, 011100, 101010, 110001\} \\
T^{-1}(1) &= \{011010, 100101, 101001\} \\
T^{-1}(2) &= \{010110, 011001, 100101\} \\
T^{-1}(3) &= \{001110, 010101, 100011, 111000\} \\
T^{-1}(4) &= \{001101, 010011, 110100\} \\
T^{-1}(5) &= \{001011, 101100, 110010\}.
\end{aligned}
$$

Therefore, $A(6, 4, 3) \geq 4$, with $T^{-1}(0)$ or $T^{-1}(3)$ being examples of the required codes.

2.4 Inductive Code Partitions and Bounds

Theorem 2.13. *For* $n = 2^k$,

$$M(n, 4) \geq \frac{n!}{6} \cdot \frac{8}{n^{\frac{\log_2 n+1}{2}}} = \frac{n!}{6 \cdot 2^{\frac{k(k+1)}{2}-3}}.$$

In fact, there is a partition of $\mathcal{S}_n$ *into* $6 \cdot 2^{\frac{k(k+1)}{2}-3}$ $PA(n, 4)$.

Proof. We prove the above by induction. Example 2.5 constructs 6 disjoint

$PA(4,4)$. Therefore take $n = 4$ as a base case.

$$\begin{aligned} M(4,4) &\geq \frac{4!}{6} \cdot \frac{8}{4^{\frac{\log_2 4+1}{2}}} \\ &= 4 \cdot \frac{8}{4^{\frac{3}{2}}} \\ &= 4. \end{aligned}$$

Assume the statement is true for some $n = 2^{k-1}$, $k \geq 3$. Then

$$\begin{aligned} M(2^{k-1},4) &\geq \frac{2^{k-1}!}{6} \cdot \frac{8}{(2^{k-1})^{\frac{\log_2 2^{k-1}+1}{2}}} \\ &= \frac{2^{(k-1)}!}{6} \cdot \frac{8}{(2^{k-1})^{\frac{k-1+1}{2}}} \\ &= \frac{2^{k-1}! \cdot 8}{6 \cdot 2^{\frac{k(k-1)}{2}}}. \end{aligned}$$

A $PA(2^k,4)$ can be constructed recursively from a $PA(2^{k-1},4)$ according to the following construction. Begin with two sets of disjoint $PA(2^{k-1},4)$, the first on the symbols $1,\ldots,2^{k-1}$ and the second on the symbols $(2^{k-1}+1),\ldots,2^k$. Next consider a constant weight binary code with length 2^k, weight 2^{k-1} and distance 4. Take all possible concatenations according to the constant weight binary code. This can be done by consecutively placing symbols $1,\ldots,2^{k-1}$ where zeros occur in the constant weight codewords, and placing symbols $(2^{k-1}+1),\ldots,2^k$ where ones occur. Distance 4 is preserved since each constant weight binary code has distance 4. $(M(2^{k-1},4))^2$ is the value for all possible concatenations and the size of a constant weight binary code with length 2^k, weight 2^{k-1} and distance 4 is at least $\binom{2^k}{2^{k-1}}/2^k$ (from Corollary 2.9). Finally, there are

$$6 \cdot 2^3 \cdots 2^{k-1} = \frac{2^{\frac{k(k-1)}{2}} \cdot 6}{8}$$

disjoint $PA(2^{k-1},4)$ from cyclic shifts of pairings of $PA(2^{k-1},4)$.

The recursive formula considers the sum of squares of disjoint $PA(2^{k-1},4)$ or the norm as defined earlier. The average size of a constant weight binary code with length 2^k, weight 2^{k-1} and distance 4 is $\binom{2^k}{2^{k-1}}/2^k$ when partitioned according to Lemma 2.8. From Lemma 2.11, a deviation from the average results in a greater value for the sum of squares therefore ensuring the lower bound of the recursive construction is maintained.

According to the recursive construction:

$$\begin{aligned}
M(2^k,4) &\geq (M(2^{k-1},4))^2 \cdot \frac{1}{2^k}\binom{2^k}{2^{k-1}} \cdot \frac{2^{\frac{k(k-1)}{2}} \cdot 6}{8} \\
&\geq (\frac{2^{k-1}! \cdot 8}{6 \cdot 2^{\frac{k(k-1)}{2}}})^2 \cdot \frac{1}{2^k}\frac{2^k!}{2^{k-1}! \cdot 2^{k-1}!} \cdot \frac{2^{\frac{k(k-1)}{2}} \cdot 6}{8} \\
&= \frac{(2^k)! \cdot 8}{6 \cdot 2^{\frac{k(k-1)}{2}} \cdot 2^k} \\
&= \frac{(2^k)! \cdot 8}{6 \cdot 2^{\frac{(k)(k+1)}{2}}}.
\end{aligned}$$

□

Theorem 2.14. *For* $n = 3 \cdot 2^k$, $k \geq 1$,

$$M(3 \cdot 2^k, 4) \geq \frac{(3 \cdot 2^k)!}{3^k \cdot 2^{\frac{k(k+1)}{2}}}$$

and there are $2^{\frac{k(k+1)}{2}-1} \cdot 3^{k-1} \cdot 6$ *such disjoint arrays.*

The recursive construction for a $PA(3 \cdot 2^k, 4)$ is similar to the method in Theorem 2.13 but instead uses the 6 disjoint $PA(6, 4)$ constructed in Example 2.6 as a base case.

Theorem 2.15. *For* $n = 5 \cdot 2^k$, $k \geq 0$,

$$M(5 \cdot 2^k, 4) \geq \frac{(5 \cdot 2^k)!}{6 \cdot 5^k \cdot 2^{\frac{k(k+1)}{2}}}$$

and there are $2^{\frac{k(k+1)}{2}} \cdot 5^k \cdot 6$ *such disjoint arrays.*

Again, the recursive construction for a $PA(5 \cdot 2^k, 4)$ is similar to the method in Theorem 2.13 but instead uses the 6 disjoint $PA(5, 4)$ constructed in Example 2.7 as a base case.

The recursive construction gives a lower bound for $M(n, 4)$ when $n = 2^k, 3 \cdot 2^k$ or $5 \cdot 2^k$. A nice consequence of the construction is not only the ability to recursively construct a $PA(n,4)$ but also, for example when $n = 2^k$, there is a method for obtaining exactly $2^{k(k+1)-3} \cdot 6$ disjoint $PA(2^k, 4)$. Although the Gilbert-Varshamov bound (1.1) is a stronger bound for higher values of n, the recursive bound provides an improvement for $n < 32$ as shown in Table 2.1. GV denotes the right side of (1.1). A more sophisticated use of the partitioning construction appears in [6].

Table 2.1: Lower bounds on $M(n,4)$

n	$\frac{n!}{M(n,4)}$	$n!/\mathrm{GV}$
4	6	15
5	6	31
6	6	56
8	48	141
10	60	286
12	72	507
16	768	1241
20	1200	2471
24	1728	4325
32	24576	10417

Chapter 3

Partitions and Characters of the Symmetric Group

A *partition* λ of n, denoted $\lambda \vdash n$, is an unordered list of positive integers which sum to n. Equivalently, we write $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_t)$ for a given partition consisting of t parts with $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_t$, and $n = \lambda_1 + \cdots + \lambda_t$.

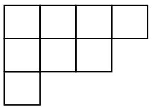
A partition is often identified with its corresponding *Young diagram*, defined below.

3.1 Young Diagrams

A *Young diagram* represents a partition λ by arranging n boxes in left-justified rows such that the ith row has the same number of boxes as the ith term in the partition [12].

Example 3.1. For example a possible partition for $n = 8$ is $\lambda = (4, 3, 1)$. The Young diagram is shown below.

$\lambda = (4, 3, 1)$



The number of boxes in each column corresponds to the *conjugate* of the partition, denoted λ^*. The ith component of the conjugate is

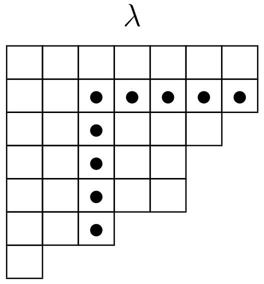
$$\lambda_i^* = |\{j : \lambda_j \geq i\}|.$$

The *main diagonal* of a Young diagram is comprised of all boxes in the ith row and ith column. The number of boxes included in the main diagonal is the *diagonal length*, which is denoted s.

The conjugate partition can also be obtained by reflecting along the main diagonal. The conjugate of the partition shown above is $(3, 2, 2, 1)$.

The value of $\lambda_1^* - \lambda_2^*$ corresponds to the number of ones in λ and is represented by $\varphi(\lambda)$.

A *hook* for a given box of a Young diagram includes that box itself, the boxes in the same row and to the right, as well as the same column and below. Therefore the *hook length* is one more than the number of boxes to the right and in the same row added to the number of boxes below and in the same column. An example of a hook for the partition $\lambda = (7, 7, 6, 5, 5, 3, 1)$ is given below.



3.2 Characters of $\mathcal{S}_n$

A *representation* of a group G is a homomorphism $h : G \to GL(N, \mathbb{C})$, mapping to the general linear group of complex numbers.

Definition 3.2. [12] Let $h(g)$, $g \in G$, be a matrix representation of the group and its operation. Then the *character* $\chi_h(g)$ of h at g is

$$\chi_h(g) = \mathrm{Tr} \circ h(g),$$

where Tr denotes the matrix trace. Thus χ_h maps G to $\mathbb{C}$. The *dimension* (or *degree*), written dim χ_h, is $N = \chi_h(1_G)$. As h is a homomorphism, a character χ_h is constant on any conjugacy class of G.

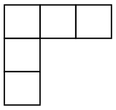
An *irreducible representation* of a group is a group representation that has no nonzero invariant subspaces [9].

Definition 3.3. [12] A *Young tableau* is obtained by filling in the boxes of the Young diagram with the symbols from 1 to n such that the numbers in each row and each column form an increasing sequence. We have dim $\lambda =$ the number of Young tableaux of shape λ.

The *hook length formula* states that if λ is a Young diagram with n boxes, then the number of Young tableaux with shape λ is $n!$ divided by the product of the hook lengths of the boxes [8].

Example 3.4. For $n = 5$, the number of Young tableaux with shape $(3, 1, 1)$ is $\frac{5!}{5 \cdot 2 \cdot 2} = 6$, by the hook length formula.

$\lambda = (3, 1, 1)$



Alternatively, the same value is obtained from directly counting the number of valid fillings. The corner box must have the value 1 while the other two boxes in the first row can be any of the remaining four values in increasing order. Once those two numbers are picked only one filling will create a valid Young tableau. Therefore the number of fillings is counted by $\binom{4}{2} = 6$.

The *character table* for a group G is an array with rows indexed by the inequivalent irreducible characters of G and columns indexed by the conjugacy classes. Both the irreducible characters of the symmetric group $\mathcal{S}_n$ and the conjugacy classes of $\mathcal{S}_n$ are in one-to-one correspondence with the set of all partitions of n. The character corresponding to partition λ is represented by χ^λ while μ is the conjugacy class corresponding to μ so the (λ, μ)-entry of the character table of $\mathcal{S}_n$ is $\chi^\lambda(\mu)$.

For $\mu = (1, 1, \ldots, 1)$, $\chi^\lambda(\mu) = \dim \chi^\lambda$ which is often written $\dim \lambda$. The explicit value of $\dim \lambda$ is obtained from the hook length formula.

The following example demonstrates the character table for $\mathcal{S}_3$.

Example 3.5. A conjugacy class in $G = \mathcal{S}_n$ consists of all permutations with a given cycle type. For $\mathcal{S}_3$ there are three conjugacy classes.

$$\begin{aligned} K_1 &= \{\epsilon\}, \\ K_2 &= \{(1,2),(1,3),(2,3)\}, \\ K_3 &= \{(1,2,3),(1,3,2)\}. \end{aligned}$$

The character table is shown below.

	K_1	K_2	K_3
$\chi^{(1,1,1)}$	1	1	1
$\chi^{(2,1)}$	1	-1	1
$\chi^{(3)}$	2	0	-1

3.3 The Frobenius Character Formulas

We write the conjugacy class corresponding to $(\overbrace{1,1,\ldots,1}^{n-t},t)$ by (t). Explicit values of $\chi^\lambda(t)/\dim\lambda$, for small values of t are found by the *Frobenius character formulas*, taken from Murnaghan [11]. We make later use of the equations

$$\frac{\chi^\lambda(2)}{\dim\lambda} = \frac{\sum_i \beta_i(\beta_i+1) - \sum_i \alpha_i(\alpha_i+1)}{n(n-1)}$$

$$\frac{\chi^\lambda(3)}{\dim\lambda} = \frac{\sum_i \alpha_i(\alpha_i+1)(2\alpha_i+1) + \sum_i \beta_i(\beta_i+1)(2\beta_i+1) - 3n(n-1)}{2n(n-1)(n-2)},$$

where $\lambda \vdash n$ has

- exactly s boxes on its main diagonal,
- $\alpha_1 > \alpha_2 > \cdots > \alpha_s$ boxes below the diagonal in columns 1 through s, and
- $\beta_1 > \beta_2 > \cdots > \beta_s$ boxes right of the diagonal in rows 1 through s.

Chapter 4

Association Schemes

4.1 Association Schemes

The definitions here are taken from Chapter 30 of [14]. An *association scheme* with k classes on a finite nonempty set X consists of $k+1$ nonempty symmetric binary relations $R_0, R_1, \ldots, R_k$ on X which partition $X \times X$ and satisfy the following conditions:

- $R_0 = \{(x, x) : x \in X\}$ is the identity relation

- For any triple of integers the cardinality

  $$p_{ij}^h = |\{z \in X : (x,z) \in R_i, (z,y) \in R_j\}|$$

  is independent of the choice of $(x,y) \in R_h$ where the numbers p_{ij}^h are called the *structure constants* of the scheme.

If $(x,y) \in R_i$, elements x and y are said to be i-associates in R.

Let $|X| = n$. We introduce the *adjacency matrices* $A_0, A_1, \ldots, A_k$ of an association scheme. For $h = 0, \ldots, k$, define the $n \times n$ matrix A_h, indexed by entries of X, as follows.

$$A_h(x,y) = \begin{cases} 1 & \text{if } (x,y) \in R_h, \\ 0 & \text{otherwise.} \end{cases}$$

By definition of the p_{ij}^h, the matrices A_h form a basis for the *Bose-Mesner algebra* with respect to entrywise multiplication. This algebra has a basis of orthogonal idempotents $E_0, \ldots, E_k$ with respect to ordinary matrix multiplication. By definition,

$$E_i E_j = \begin{cases} E_i & \text{if } i = j, \\ 0 & \text{otherwise.} \end{cases}$$

Also, we have $E_0 + \cdots + E_k = I$. The adjacency matrices obey similar identities with Schur (entrywise) multiplication. In other words,

$$A_i \circ A_j = \begin{cases} A_i & \text{if } i = j, \\ 0 & \text{otherwise,} \end{cases}$$

and $A_0 + \cdots + A_k = J$, where J is the all-one matrix of size $n \times n$.

The *first eigenmatrix* P is $(k+1) \times (k+1)$ with rows and columns indexed by $0, 1, \ldots, k$ such that $A_j = \sum_{i=0}^{k} P_{ij} E_i$.

The *second eigenmatrix* Q similarly has entries given by $nE_j = \sum_{i=0}^{k} Q_{ij} A_i$.

Given a set Y of points of an association scheme, the *distribution vector* of Y is defined to be $\boldsymbol{a} = (a_0, \ldots, a_k)$, where $a_i = |(Y \times Y) \cap R_i|$. Note that $a_0 = |Y|$.

For $J \subset \{1, \ldots, k\}$, a J-*clique* is a subset W of X such that for any $w_1, w_2 \in W$, $(w_1, w_2) \in R_j$ for some $j \in J$.

The following is Delsarte's linear programming bound for cliques in X.

Theorem 4.1. [4] *Subject to* $\boldsymbol{a} \geq \mathbf{0}$, $a_0 = 1$, $a_i = 0$ *for* $i \notin J$, *and*

$$\boldsymbol{a}Q \geq \mathbf{0}$$

put

$$M_{\mathrm{LP}} = \max \sum_{i=0}^{k} a_i.$$

Then M_{LP} *is an upper bound on the size of any* J*-clique.*

The following example presents the Johnson association scheme [14].

Example 4.2. The points of the *Johnson scheme* are the $\binom{v}{k}$ k-subsets of a v-set S. Two k-subsets A, B are declared to be i-th associates when $|A \cap B| = k - i$.

For $v = 8$, $k = 3$, this is a 3-class scheme with $\binom{8}{3} = 56$ points. Some of the intersection numbers of the scheme are listed below.

$$\begin{array}{llll}
p^0_{11} = 15, & p^1_{11} = 6, & p^1_{12} = 8, & p^1_{13} = 0, \\
p^0_{22} = 30, & p^2_{11} = 4, & p^2_{12} = 8, & p^2_{13} = 3, \\
p^0_{33} = 10, & p^3_{11} = 0, & p^3_{12} = 9, & p^3_{13} = 6.
\end{array}$$

The intersection number p^0_{11} is 15 since there are 15 triples one element away from any given triple. Similarly, the intersection number p^1_{11} is 6 since given triples with 1 differing element, there are 6 triples one element away from both.

From the above intersection numbers we have:

$$A_1A_2 = 8A_1 + 8A_2 + 9A_3$$

and

$$A_1A_3 = 0A_1 + 3A_2 + 6A_3$$

which can be used to find:

$$\begin{array}{rcl} A_1^0 & = & A_0, \\ A_1^1 & = & \qquad A_1, \\ A_1^2 & = & 15A_0 + 6A_1 + 4A_2, \\ A_1^3 & = & 90A_0 + 83A_1 + 56A_2 + 36A_3 \\ A_1^4 & = & 1245A_0 + 1036A_1 + 888A_2 + 720A_3 \end{array}$$

From this table we can derive the minimal polynomial of A_1, after arithmetic:

$$x^4 - 20x^3 + 58x^2 + 276x - 315 = (x - 15)(x - 7)(x - 1)(x + 3) = 0.$$

Therefore the eigenvalues of A_1 are $15, 7, 1, \text{and} -3$. Using these values along with the eigenvalues for A_2 and A_3 we obtain the first eigenmatrix:

$$P = \begin{bmatrix} 1 & 15 & 30 & 10 \\ 1 & 7 & -2 & -6 \\ 1 & 1 & -5 & 3 \\ 1 & -3 & 3 & -1 \end{bmatrix}$$

To obtain the second eigenmatrix:

$$Q = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 15 & 0 & 0 \\ 0 & 0 & 30 & 0 \\ 0 & 0 & 0 & 10 \end{bmatrix}^{-1} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 15 & 7 & 1 & -3 \\ 30 & -2 & -5 & 3 \\ 10 & -6 & 3 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 7 & 0 & 0 \\ 0 & 0 & 20 & 0 \\ 0 & 0 & 0 & 28 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 7 & 20 & 28 \\ 1 & \frac{49}{15} & \frac{20}{15} & \frac{-84}{15} \\ 1 & \frac{-14}{30} & \frac{-100}{30} & \frac{84}{30} \\ 1 & \frac{-42}{10} & \frac{60}{10} & \frac{-28}{10} \end{bmatrix}$$

The columns of Q represent Delsarte's Inequalities and when fractions are cleared are:

$$\begin{aligned}
15 + 7a_1 - a_2 - 9a_3 &\geq 0, \\
30 + 2a_1 - 5a_2 + 9a_3 &\geq 0, \\
10 - 2a_1 + a_2 - a_3 &\geq 0.
\end{aligned}$$

The symmetric group defines an association scheme, called the *conjugacy scheme*, where $X = \mathcal{S}_n$ are the points, relations are indexed by partitions $\lambda \vdash n$, and $(\sigma, \tau) \in R_\mu$ if and only if $\sigma\tau^{-1}$ belongs to conjugacy class μ. Of course, σ and τ are at distance d if and only if $(\sigma, \tau) \in R_\mu$, where $\varphi(\mu) = n - d$.

Let $D \subseteq \{1, 2, \ldots, n\}$. A D-permutation code is a subset Γ of $\mathcal{S}_n$ such that any two distinct permutations in Γ are at some distance in D. For $D = \{d, d+1, \ldots, n\}$ we obtain $PA(n, d)$. The maximum size of such a set Γ is denoted $M(n, D)$. Frankl and Deza proved that

$$M(n, D)M(n, D^c) \leq n!,$$

where $D^c = \{1, \ldots, n\} \setminus D$.

4.2 The Linear Programming Bound

Tarnanen [13] considered the following specialization of Delsarte's Inequalities to cliques in the conjugacy scheme.

Theorem 4.3. [13] *Subject to* $a_\mu \geq 0$ *for all* $\mu \vdash n$, $a_{(1,\ldots,1)} = 1$, $a_\mu = 0$ *for all* $\mu \vdash n$ *having* $n - \varphi(\mu) \notin D$, *and*

$$\sum_{\mu \vdash n} a_\mu \chi^\lambda(\mu) \geq 0$$

for all $\lambda \vdash n$, *put*

$$M_{\mathrm{LP}}(n, D) = \max \sum_{\mu \vdash n} a_\mu.$$

Then

$$M(n, D) \leq M_{LP}(n, D). \tag{4.1}$$

Delsarte [4] in fact proved that (4.1) holds analogously for LP bounds. In our context,

$$M_{\mathrm{LP}}(n, D) M_{\mathrm{LP}}(n, D^c) \leq n!. \tag{4.2}$$

By (4.1) and (4.2), it follows that

$$M(n,4) = M(n,\{4,\ldots,n\}) \leq \frac{n!}{M_{\mathrm{LP}}(\{2,3\})} \tag{4.3}$$

So upper bounds on $M(n,4)$ follow from lower bounds on $M_{\mathrm{LP}}(\{2,3\})$. The convenient choice of $D = \{2,3\}$ above offers a nice simplification of Theorem 4.3.

Lemma 4.4. *Let $n \geq 4$. Then M_{LP} $=M_{\mathrm{LP}}(\{2,3\})$ is given by*

$$\max\{1+a+b : a,b \geq 0 \textit{ and } \forall\ \lambda \vdash n,\ \dim\,(\chi^\lambda) + a\chi^\lambda(2) + b\chi^\lambda(3) \geq 0\}.$$

For each feasible point (a,b), we obtain a bound $M_{\mathrm{LP}}\geq 1+a+b$. Our main result is proved by showing that $(a,b) = (3, n-2)$ is feasible in Lemma 4.4. A necessary and sufficient condition for this is, for all $\lambda \vdash n$,

$$\dim\,(\lambda) + 3\chi^\lambda(2) + (n-2)\chi^\lambda(3) \geq 0.$$

Applying the Frobenius character formulas (see Section 3.3) to Lemma 4.4

gives

$$\frac{1}{2n(n-1)}\Bigg[\sum_{j=1}^{s}(\beta_j(\beta_j+1)(2\beta_j+1)+6\beta_j(\beta_j+1))+ \\ \sum_{j=1}^{s}(\alpha_j(\alpha_j+1)(2\alpha_j+1)-6\alpha_j(\alpha_j+1))\Bigg]-\frac{3}{2}\geq -1.$$

This simplifies to the following:

$$\begin{aligned}\Phi(\lambda) &= \sum_{j=1}^{s}(\beta_j(\beta_j+1)(2\beta_j+7)+\alpha_j(\alpha_j+1)(2\alpha_j-5)) \qquad (4.4)\\ &\geq n(n-1).\end{aligned}$$

In the next chapter, we will prove the inequality in (4.4) for certain values of n.

Chapter 5

New LP Upper Bounds

In this chapter we will analyze partitions that minimize the value of $\Phi(\lambda)$ (4.4) as stated at the end of the previous chapter. This becomes an optimization problem on Young diagrams. We simplify $\Phi(\lambda)$ by defining the following polynomials:

$$\begin{aligned} f(x) &= x(x+1)(2x-5) \\ g(x) &= x(x+1)(2x+7). \end{aligned}$$

So,

$$\Phi(\lambda) = \sum_{j=1}^{s} [f(\alpha_j) + g(\beta_j)],$$

where as before λ has $\alpha_1 \geq \cdots \geq \alpha_s$ boxes below the diagonal and $\beta_1 \geq \cdots \geq \beta_s$ boxes right of the diagonal. Again, s is the number of boxes on the main diagonal.

5.1 Partition Operations to Minimize $\Phi(\lambda)$

We will show that applying the following partition operations result in a smaller value of $\Phi(\lambda)$, allowing us to make a conclusion about the shape of the partitions that will minimize the expression in (4.4). These partitions will be the constraining partitions of our inequality, resulting in fewer partitions to check in Theorem 4.3.

5.1.1 Flattening right of the diagonal

The following operation will move boxes right of the diagonal when one row of the partition is greater than some other row by at least two. The operation will move the last box of the larger row to the end of the smaller row, resulting in a smaller value of Φ. As a result of this operation we will have a new partition λ^R.

If these rows are $\lambda_j \geq \lambda_i + 2$ for $i > j$ then

$$\begin{aligned}
\beta_j^R &= \beta_j - 1. \\
\beta_i^R &= \beta_i + 1.
\end{aligned}$$

and otherwise $\beta_k = \beta_k^R$ and $g(\beta_k) = g(\beta_k^R)$. Therefore

$$\begin{aligned}
g(\beta_j) &= \beta_j(\beta_j + 1)(2\beta_j + 7) = 2\beta_j^3 + 9\beta_j^2 + 7\beta_j. \\
g(\beta_i) &= \beta_i(\beta_i + 1)(2\beta_i + 7) = 2\beta_i^3 + 9\beta_i^2 + 7\beta_i. \\
g(\beta_j^R) &= (\beta_j - 1)(\beta_j)(2\beta_j + 5) = 2\beta_j^3 + 3\beta_j^2 - 5\beta_j. \\
g(\beta_i^R) &= (\beta_i + 1)(\beta_i + 2)(2\beta_i + 9) = 2\beta_i^3 + 15\beta_i^2 + 31\beta_i + 18.
\end{aligned}$$

Now to verify the new value of (4.4) has decreased we add the new $g(\beta^R)$ values and subtract the old $g(\beta)$ values.

$$\begin{aligned}
[g(\beta_j^R) + g(\beta_i^R)] - [g(\beta_j) + g(\beta_i)] &= 6\beta_i^2 - 6\beta_j^2 + 24\beta_i - 12\beta_j + 18 \\
&= 6\beta_i(\beta_i + 4) - 6\beta_j(\beta_j + 2) + 18.
\end{aligned}$$

Since $(\beta_j + j) \geq (\beta_i + i) + 2$ and $i > j$:

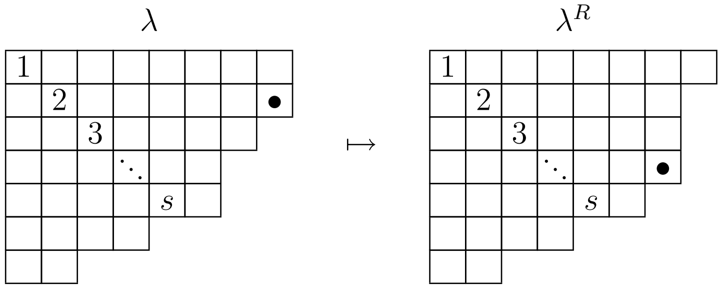
$$\beta_i - \beta_j \leq -3.$$

Therefore,

$$\begin{aligned} \Phi(\lambda^R) - \Phi(\lambda) &= [g(\beta_j^R) + g(\beta_i^R)] - [g(\beta_j) + g(\beta_i)] \\ &= 6\beta_i(\beta_i + 4) - 6\beta_j(\beta_j + 2) + 18 \\ &< 6\beta_i(\beta_j + 2) - 6\beta_j(\beta_j + 2) + 18 \\ &\leq -18(\beta_j + 2) + 18 \\ &\leq 0. \end{aligned}$$

Thus, provided $\lambda_j \geq \lambda_i + 2$, moving boxes according to the above operations will always result in a smaller value for Φ.

We illustrate this operation with the following example. The diagonal cells are numbered and the box which will move is indicated with a bullet.



5.1.2 Flattening below the diagonal

This operation is similar to the previous one but instead considers length of the columns of the partitions (rows of the dual). This operation will move boxes below the diagonal when one column of the partition is greater than any other column by at least two. The operation will move the last box of the larger column to the end of the smaller column, resulting in a new partition λ^B and a smaller value of Φ. If these columns are $\lambda_j^* \geq \lambda_i^* + 2$ and $i > j$ then with

$$\begin{aligned} \alpha_j^B &= \alpha_j - 1, \\ \alpha_i^B &= \alpha_i + 1, \end{aligned}$$

we have

$$\begin{aligned}
f(\alpha_j) &= \alpha_j(\alpha_j+1)(2\alpha_j-5) = 2\alpha_j^3 - 3\alpha_j^2 - 5\alpha_j. \\
f(\alpha_i) &= \alpha_i(\alpha_i+1)(2\alpha_i-5) = 2\alpha_i^3 - 3\alpha_i^2 - 5\alpha_i. \\
f(\alpha_j^B) &= (\alpha_j-1)(\alpha_j)(2\alpha_j-7) = 2\alpha_j^3 - 9\alpha_j^2 + 7\alpha_j. \\
f(\alpha_i^B) &= (\alpha_i+1)(\alpha_i+2)(2\alpha_i-3) = 2\alpha_i^3 + 3\alpha_i^2 - 5\alpha_i - 6.
\end{aligned}$$

Therefore,

$$\begin{aligned}
\Phi(\lambda^B) - \Phi(\lambda) &= [f(\alpha_j^B) + f(\alpha_i^B)] - [f(\alpha_j) + f(\alpha_i)] \\
&= [2\alpha_j^3 - 9\alpha_j^2 + 7\alpha_j] + [2\alpha_i^3 + 3\alpha_i^2 - 5\alpha_i - 6] \\
&\quad -[2\alpha_j^3 - 3\alpha_j^2 - 5\alpha_j] - [2\alpha_i^3 - 3\alpha_i^2 - 5\alpha_i] \\
&= 6\alpha_i^2 - 6\alpha_j^2 + 12\alpha_j - 6.
\end{aligned}$$

Since $j - i \leq -1$ and $\alpha_i - \alpha_j \leq -3$:

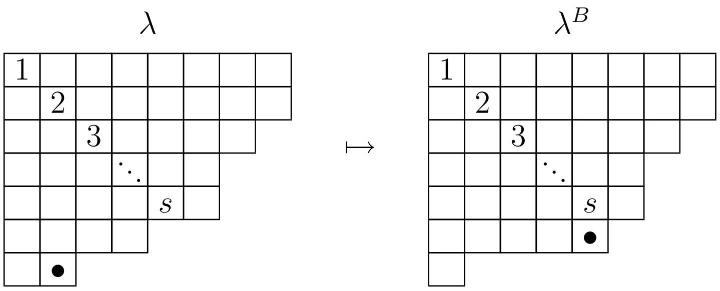
$$\begin{aligned}
\Phi(\lambda^B) - \Phi(\lambda) &= 6\alpha_i^2 - 6\alpha_j^2 + 12\alpha_j - 6 \\
&< 6\alpha_i(\alpha_j - 2) - 6\alpha_j(\alpha_j - 2) - 6 \\
&\leq -18(\alpha_j - 2) - 6.
\end{aligned}$$

Since $\alpha_j \geq 3$,

$$\Phi(\lambda^B) - \Phi(\lambda) \quad < \quad -18(\alpha_j - 2) - 6 < 0.$$

Therefore provided $\alpha_j \geq \alpha_i + 3$, moving boxes according to the above operations will always result in a smaller value for Φ.

The second operation is illustrated below.



5.1.3 Adding to the diagonal

The following operation will move a box into a hole on the diagonal when certain conditions are met. This will increase the length of the diagonal by one and create a new partition λ^D. As a result the value of Φ will either decrease or remain unchanged. First we will analyze moving boxes from below the diagonal to fill a diagonal hole.

If the previous two operations have been performed and both $\lambda_s, \lambda_s^* > s$ then for the largest j satisfying $\lambda_j^* \geq s + 2$:

$$\begin{aligned} \alpha_j^D &= \alpha_j - 1. \\ s^D &= s + 1. \\ \alpha_{s^D} &= 0. \end{aligned}$$

We have

$$\begin{aligned} f(\alpha_j) &= \alpha_j(\alpha_j + 1)(2\alpha_j - 5) = 2\alpha_j^3 - 3\alpha_j^2 - 5\alpha_j. \\ f(\alpha_j^D) &= (\alpha_j - 1)(\alpha_j)(2\alpha_j - 7) = 2\alpha_j^3 - 9\alpha_j^2 + 7\alpha_j. \\ f(\alpha_{s+1}) &= 0. \end{aligned}$$

Therefore,

$$\begin{aligned} \Phi(\lambda^D) - \Phi(\lambda) &= [2\alpha_j^3 - 9\alpha_j^2 + 7\alpha_j + 0] - [2\alpha_j^3 - 3\alpha_j^2 - 5\alpha_j] \\ &= -6\alpha_j^2 + 12\alpha_j \\ &\leq 0. \end{aligned}$$

Thus provided the moving boxes operations have been performed and $\lambda_j^* \geq s+2$, filling holes according to the above operations will result in a value of Φ that is either unchanged or smaller. The value of Φ remains unchanged when the value of α_j is exactly two.

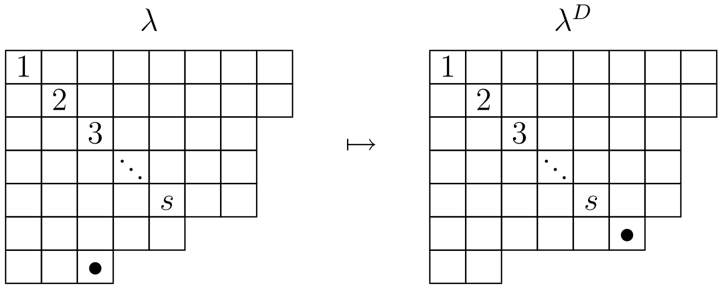
The operation for moving a box from the right of the diagonal to fill a hole on the diagonal is similar but results in strict inequality for the value of Φ due to the differing polynomial value. A box is moved from the right of the diagonal to fill a diagonal hole if the previous moving boxes operations have been performed and both $\lambda_s, \lambda_s^* > s$. Similarly, for the largest j satisfying $\lambda_j \geq s+2$:

$$\begin{aligned} \beta_j^D &= \beta_j - 1. \\ s^D &= s+1. \\ \beta_{s^D} &= 0. \end{aligned}$$

As a result:

$$[g(\beta_j^D) + g(\beta_{s+1})] - [g(\beta_j)] = -6\beta_j^2 - 12\beta_j < 0.$$

Therefore provided the moving boxes operations have been performed and $\lambda_j \geq s+2$, filling holes according to the above operations will always result in a smaller value for Φ. This operation is illustrated below:



As a consequence of the above Young diagram manipulations the resulting shape of the diagram will have a rectangular shape with the possible exception that the bottom row may contain one or more boxes and similarly the last column may contain one or more boxes. We call this a *near rectangle* since the shape is a rectangle with an inverse hook shape removed from the bottom right corner. In fact the shape that corresponds to a minimum value of Φ will be a near rectangle with a row/column difference of at most three. In order to force the mentioned near rectangle shape we need to apply the next two operations.

5.1.4 Transposing

The transposing operation will take the conjugate of λ if $\lambda_1 > \lambda_1^*$ for a near rectangle λ. If $\lambda_1 > \lambda_1^*$, then $\beta_i \geq \alpha_i$ for all $i = 1, \ldots, s$. Taking the conjugate of λ will interchange α_i with β_i and result in the new partition λ^*. If $\lambda_1 > \lambda_1^*$ then

$$\begin{aligned} \beta_j^* &= \alpha_j, \\ \alpha_j^* &= \beta_j. \end{aligned}$$

The new value of Φ will be smaller if

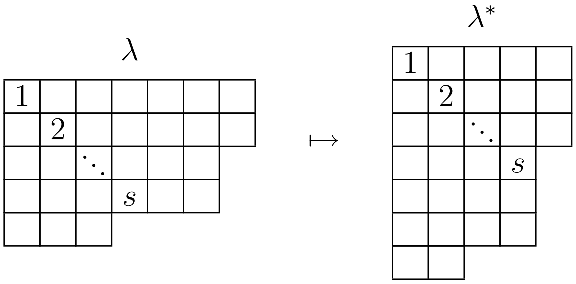
$$[g(\beta_j^*) + f(\alpha_j^*)] - [g(\beta_j) + f(\alpha_j)] \leq 0.$$

$$\begin{aligned} [g(\beta_j^*) + f(\alpha_j^*)] - [g(\beta_j) + f(\alpha_j)] &= [g(\alpha_j) - f(\alpha_j)] + [f(\beta_j) - g(\beta_j)] \\ &= [2\alpha_j^3 + 9\alpha_j^2 + 7\alpha_j] - [2\alpha_j^3 - 3\alpha_j^2 - 5\alpha_j] \\ &\quad +[2\beta_j^3 - 3\beta_j^2 - 5\beta_j] - [2\beta_j^3 + 9\beta_j^2 + 7\beta_j] \\ &= 12\alpha_j^2 + 12\alpha_j - 12\beta_j^2 - 12\beta_j. \end{aligned}$$

Since $\alpha_j \leq \beta_j$ for all j and $\alpha_1 < \beta_1$:

$$[g(\beta_j^*) + f(\alpha_j^*)] - [g(\beta_j) + f(\alpha_j)] \quad < \quad 0.$$

Therefore by transposing the partition according to the above operations, Φ will decrease.



5.1.5 Squaring

The squaring operation will be performed on a near rectangle when $\alpha_i \geq \beta_i + 3$ for all $i = 1, \ldots, s$. All lowermost boxes in columns 1 through s are moved onto the right of rows 1 through s, one per row. The resulting partition λ^S

has the following characteristics:

$$\begin{aligned} \beta_j^S &= \beta_j + 1. \\ \alpha_j^S &= \alpha_j - 1. \end{aligned}$$

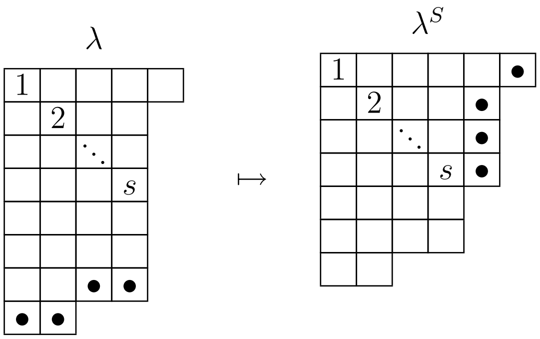
Therefore,

$$\begin{aligned} \Phi(\lambda^S) - \Phi(\lambda) &= [g(\beta_j^S) + f(\alpha_j^S)] - [g(\beta_j) + f(\alpha_j)] \\ &= [2\beta_j^3 + 15\beta_j^2 + 31\beta_j + 18] + [2\alpha_j^3 - 9\alpha_j^2 + 7\alpha_j] \\ &\quad -[2\beta_j^3 + 9\beta_j^2 + 7\beta_j] - [2\alpha_j^3 - 3\alpha_j^2 - 5\alpha_j] \\ &= 6\beta_j^2 + 24\beta_j + 18 - 6\alpha_j^2 + 12\alpha_j. \end{aligned}$$

Since $\beta_j \leq \alpha_j - 3$

$$\begin{aligned} \Phi(\lambda^S) - \Phi(\lambda) &\leq 6(\alpha_j - 3)^2 + 24(\alpha_j - 3) + 18 - 6\alpha_j^2 + 12\alpha_j \\ &= 6\alpha_j^2 - 36\alpha_j + 54 + 24\alpha_j - 72 + 18 - 6\alpha_j^2 + 12\alpha_j \\ &= 0. \end{aligned}$$

Therefore by moving sections of rows to columns according to the above operations, Φ will either decrease or remain unchanged.



When all of the possible partition operations have been performed, possibly several times, and there are no more valid moves remaining we are left with a limited number of rectangular shaped partitions. This gives the following lemma.

Lemma 5.1. *If* $\Phi(\lambda)$ *is minimized for Young diagram* λ*, then* λ *is a* $(t+i)\times t$ *rectangle for some* $i \in \{0, 1, 2, 3\}$*, with a hook of length* $t(t+i) - n$ *removed.*

5.2 $\Phi(\lambda)$ for $n = m^2$

Here, we use the structural results in Section 5.1 to prove an improved bound on $M(n, 4)$.

Theorem 5.2. *If* $n = m^2$ *where* $m \geq 2$ *is an integer, then* $(3, n-2)$ *is* *feasable for the LP in Lemma 4.4. Therefore* $M_{\mathrm{LP}}(\{2,3\}) \geq n+2$.

From (4.3) it follows that in this case

$$M(n,4) \leq \frac{n!}{(n+2)}.$$

Throughout, this subsection we assume $n = m^2$.

As a result of Lemma 5.1 there are four near rectangle shapes to consider. We define X to be the number of boxes in the last column of the partition.

5.2.1 $t \times t$ Square for $n = m^2$

For $i = 0$ dimensions are $t \times t$ and $t = m$ with no squares removed:

$$\begin{aligned}
\Phi(\lambda) &= \sum_{j=1}^{s}(\beta_j(\beta_j+1)(2\beta_j+7) + \alpha_j(\alpha_j+1)(2\alpha_j-5)) \\
&= \sum_{i=1}^{m-1} g(i) + \sum_{j=1}^{m-1} f(j) \\
&= \frac{1}{2}(m-4)(m-1)m(m+1) + \frac{1}{2}(m-1)m(m+1)(m+4) \\
&= m^2(m^2-1) \\
&= n(n-1).
\end{aligned}$$

This gives the following Lemma:

Lemma 5.3. $\sum_{i=1}^{m-1}[g(i) + f(i)] = m^2(m^2-1)$.

5.2.2 $(t+1)\times t$ Rectangle for $n=m^2$

For $i=1$ dimensions are $(t+1)\times t$ and $t=m$, $1\leq X\leq m-1$ with m squares removed:

$$\begin{aligned}
\Phi(\lambda) &= \sum_{i=1}^{m-1} g(i) - g(m-X-1) + \sum_{i=1}^{m} f(i) - f(X)\\
&= m^2(m^2-1) + f(m) - f(X) - g(m-X-1)\\
&= m^2(m^2-1) + m(m+1)(2m-5)\\
&\quad -X(X+1)(2X-5) - (m-X-1)(m-X)(2m-2X+5)\\
&= m^2(m^2-1) - 6m^2 + 6mX + 6m^2X - 6mX^2\\
&= m^2(m^2-1) + 6m(X-1)(m-X).
\end{aligned}$$

For $2\leq X\leq m-1$ we have that $\Phi(\lambda) > m^2(m^2-1)$ which is larger than for the square.

When $X=1$ we have a $(m+1)\times(m-1)$ rectangular shape with one extra square in the last column which corresponds to $\Phi(\lambda)=m^2(m^2-1)$, the same value as the square.

5.2.3 $(t+2) \times t$ Rectangle for $n = m^2$

Dimensions of $(t+2) \times t$ are not possible for $n = m^2$, since a rectangle with those dimensions bounds at most t^2+2t boxes and at least $t^2+2t-(2t-1) = t^2+1$ boxes. Therefore:

$$t^2 < m^2 < (t+1)^2.$$

Since there is no square integer between two consecutive squares we conclude that this shape is not possible for $n = m^2$.

5.2.4 $(t+3) \times t$ Rectangle for $n = m^2$

For $i = 3$ dimensions are $(t+3) \times t$. This forces $t = m-1$ with $m-2$ squares removed.

We have three cases depending on the size of X:

Case 1: If $5 \leq X \leq m-2$ and $m \geq 7$, then

$$\begin{aligned}
\Phi(\lambda) &= \sum_{i=1}^{m-2} g(i) - g(m-X-2) + \sum_{i=2}^{m+1} f(i) - f(X-1) \\
&= m^2(m^2-1) - g(m-1) - g(m-X-2) \\
&\quad + f(m) + f(m+1) - f(1) - f(X-1) \\
&= m^2(m^2-1) + 6m^2X - 6mX^2 - 6mX + 12X^2 - 12X - 6 \\
&= m^2(m^2-1) + 6mX(m-X-1) + 12X^2 - 12X - 6.
\end{aligned}$$

To determine if $6m^2X - 6mX^2 - 6mX + 12X^2 - 12X - 6 > 0$ for all feasible values of m and X, we find all local minima and calculate the value of $6m^2X - 6mX^2 - 6mX + 12X^2 - 12X - 6$ at each minimum and at the endpoints. Since $6mX(m-X-1) + 12X^2 - 12X - 6$ has a local maximum over the values $5 \leq X \leq m-2$ and both endpoints are positive for $m \geq 7$ we can conclude that $\Phi(\lambda) > m^2(m^2-1)$, larger than the square diagram.

Case 2: If $X = 4$, then

$$\begin{aligned}\Phi(\lambda) &= \sum_{i=1}^{m-2} g(i) - g(m-6) + \sum_{i=4}^{m+1} f(i)\\ &= m^2(m^2-1) - g(m-1) - g(m-6)\\ &\quad +f(m) + f(m+1) - f(1) - f(2) - f(3)\\ &= m^2(m^2-1) + 24m^2 - 12m + 144.\end{aligned}$$

For all values of m, $\Phi(\lambda) > m^2(m^2-1)$, larger than for the square.

Case 3: If $m-1 \leq X \leq m+1$, then

$$\begin{aligned}\Phi(\lambda) &= \sum_{i=1}^{m-2} g(i) + \sum_{i=2}^{m+1} f(i) - f(X-1)\\ &= m^2(m^2-1) - g(m-1) + f(m) + f(m+1) - f(1) - f(X-1)\\ &= m^2(m^2-1) + 2m^3 - 3m^2 - 5m - 2X^3 + 9X^2 - 7X\\ &= m^2(m^2-1) + m(m+1)(2m-5) - X(X-1)(2X-7).\end{aligned}$$

For $m-1 \leq X \leq m$, $\Phi(\lambda) > m^2(m^2-1)$, larger than for the square.

When $X = m+1$ we have a $(m+1) \times (m-1)$ rectangular shape with one extra square in the last row. This corresponds to $\Phi(\lambda) = m^2(m^2-1)$, the same value as the square.

To summarize, there are three shapes λ that minimize $\Phi(\lambda)$ for $n = m^2$: the $m \times m$ square and the $(m+1) \times (m-1)$ rectangles with one extra box added either to the first row or column.

5.3 $\Phi(\lambda)$ for $n = (m+2)(m-1)$

This subsection is devoted to the proof of the following result, similar to Theorem 5.2.

Theorem 5.4. *If* $n = (m+2)(m-1)$ *where* $m \geq 2$ *is an integer, then* $(3, n-2)$ *is feasable for the LP in Lemma 4.4. Therefore* $M_{\mathrm{LP}} \geq n+2$*.*

Again, from (4.3)

$$M(n,4) \leq \frac{n!}{(n+2)}.$$

Throughout, we assume $n = (m+2)(m-1) = m^2 + m - 2$.

As a result of Lemma 5.1 there are four near rectangle shapes to consider.

5.3.1 $(t+3)\times t$ Rectangle for $n=(m+2)(m-1)$

For $i=3$ the shape is $(t+3)\times t$, where $t=m-1$, with no squares removed.

$$\begin{aligned}\Phi(\lambda) &= \sum_{i=1}^{m-2} g(i)+\sum_{i=3}^{m+1} f(i)\\ &= (m+2)(m-1)(m^2+m-3)\\ &= n(n-1).\end{aligned}$$

5.3.2 $t\times t$ Square for $n=(m+2)(m-1)$

For $i=0$ the shape is a $t\times t$ square, where $t=m+1$, with $m+3$ squares removed. Easy calculations give

$$\begin{aligned}\Phi(\lambda) &= \sum_{i=1}^{m} g(i)-g(m-X)+\sum_{i=1}^{m} f(i)-f(X+2)\\ &= (m+2)(m-1)(m^2+m-3)+g(m-1)+g(m)-g(m-X)\\ &\quad +f(1)+f(2)-f(m+1)-f(X+2)\\ &= (m+2)(m-1)(m^2+m-3)+6mX(m-X)+18X(m-X).\end{aligned}$$

Since $m \geq 4$ and $1 \leq X \leq m-3$ we have that

$$\Phi(\lambda) > (m+2)(m-1)(m^2+m-3),$$

which is larger than for the $(t+3) \times t$ rectangle.

5.3.3 $(t+1) \times t$ Rectangle for $n = (m+2)(m-1)$

For a $(t+1) \times t$ rectangle, we have $t = m$ with two squares removed.

Case 1: Two squares removed from last column of the rectangle.

$$\begin{aligned}
\Phi(\lambda) &= \sum_{i=1}^{m-1} g(i) + \sum_{i=2}^{m} f(i) \\
&= (m+2)(m-1)(m^2+m-3) + g(m-1) + f(2) - f(m+1) \\
&= (m+2)(m-1)(m^2+m-3) + 0.
\end{aligned}$$

We have that $\Phi(\lambda) = (m+2)(m-1)(m^2+m-3)$, the same value as for the $(t+3) \times t$ rectangle.

Case 2: Two squares removed from the last row of the rectangle.

$$\begin{aligned}\Phi(\lambda) &= \sum_{i=1}^{m-1} g(i) + \sum_{i=1}^{m} f(i) - f(2)\\ &= (m+2)(m-1)(m^2+m-3) + g(m-1) + f(1) - f(m+1)\\ &= (m+2)(m-1)(m^2+m-3) + 0.\end{aligned}$$

We have that $\Phi(\lambda) = (m+2)(m-1)(m^2+m-3)$, the same value as for the $(t+3) \times t$ rectangle.

5.3.4 $(t+2) \times t$ Rectangle for $n = (m+2)(m-1)$

For the $(t+2) \times t$ rectangle, $t = m$, with $m+2$ squares removed:

$$\begin{aligned}\Phi(\lambda) &= \sum_{i=1}^{m-1} g(i) - g(m-X-1) + \sum_{i=2}^{m+1} f(i) - f(X+2)\\ &= (m+2)(m-1)(m^2+m-3)\\ &\quad + g(m-1) - g(m-X-1) + f(2) - f(X+2)\\ &= (m+2)(m-1)(m^2+m-3)\\ &\quad + 6m^2X - 6mX^2 + 6mX - 12X^2 - 12X.\end{aligned}$$

Since $6m^2X - 6mX^2 + 6mX - 12X^2 - 12X$ has a local maximum over the values $1 \leq X \leq m-2$ and both endpoints are positive for $m \geq 3$ we have that $\Phi(\lambda) > (m+2)(m-1)(m^2+m-3)$, which is larger than the $(t+3)\times t$ rectangle.

Therefore there are three shapes that minimize $\Phi(\lambda)$: the $(m+3)\times m$ rectangle and both of the $(m+1)\times m$ rectangles with two squares removed.

5.4 Other values of n

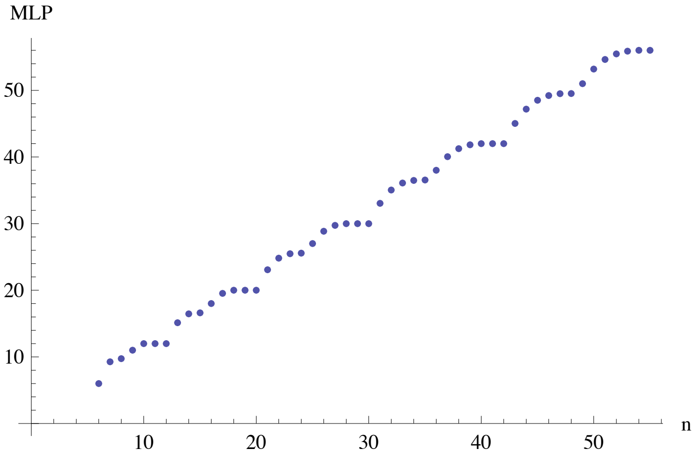
A lower bound on M_{LP} is obtained for each feasible point of the LP in Lemma 4.4. We have considered $n = m^2$ and $n = (m+2)(m-1)$ but we are also able to run the LP for other values of n. The LP for $M(n, D)$ requires exhausting all characters and even with a computer can be tedious and slow. However, to run the LP using D^c, we are able to use a restricted character table and obtain values far more efficiently.

The following table provides some M_{LP} values for small n.

Table 5.1: M_{LP} for small values of n

n	M_{LP}	a	b	n	M_{LP}	a	b
6	6	3	2	29	30	4.1429	24.8571
7	9.2727	1.9091	6.3636	30	30	4.5789	24.4211
8	9.75	1.75	7	31	33.0508	1.5763	30.4746
9	11	3	7	32	35.0392	1.6209	32.4183
10	12	3	8	33	36.0920	1.6196	33.4724
11	12	3.6667	7.3333	34	36.4929	1.5892	33.9037
12	12	3.6667	7.3333	35	36.5455	1.5455	34
13	15.1304	1.6957	12.4348	36	38	3	34
14	16.4528	1.7170	13.7358	37	40.0556	3.0833	35.9722
15	16.6154	1.6154	14	38	41.2599	3.0969	37.1630
16	18	3	14	39	41.8264	3.0620	37.7645
17	19.5455	3.0909	15.4545	40	42	3	38
18	20	3	16	41	42	4.2414	36.7586
19	20	3.9767	15.0233	42	42	4.8235	36.1765
20	20	4.2222	14.7778	43	45.0361	1.5542	42.4819
21	23.0769	1.6154	20.4615	44	47.1852	1.5926	44.5926
22	24.8201	1.6619	22.1583	45	48.5243	1.6019	45.9223
23	25.4839	1.6323	22.8516	46	49.2258	1.5899	46.6359
24	25.5682	1.5682	23	47	49.4964	1.5644	46.9320
25	27	3	23	48	49.5326	1.5326	47
26	28.8571	3.0952	24.7619	49	51	3	47
27	29.7368	3.0789	25.6579	50	53.1930	3.0702	49.1228
28	30	3	26				

Figure 5.1: M_{LP} for small values of n



Chapter 6

Conclusions

We have obtained a recursive construction for a $PA(n,4)$ when $n = 2^k, 3 \cdot 2^k$ or $5 \cdot 2^k$ and an improvement on the Gilbert-Varshamov bound for small n. A nice consequence of the construction is not only the ability to recursively construct a $PA(n,4)$ but also, for example when $n = 2^k$, there is a method for obtaining exactly $2^{k(k+1)-3} \cdot 6$ disjoint $PA(2^k,4)$. The partitioning construction can be improved upon to provide stronger lower bounds on $M(n,4)$ as stated in [6].

Our main upper bound on $M(n,4)$ is an improvement on existing bounds. In order to determine $M_{\mathrm{LP}}(n,D)$ we must exhaust all character constraints but using D^c allows us to use a restricted character table and obtain values for $M_{\mathrm{LP}}(n, D)$ more efficiently. It is interesting to note that as a result of (4.3), obtaining a poor upper bound with $M_{\mathrm{LP}}(n, D^c)$ is actually advantageous for bounding $M(n, 4)$. The values of $n = m^2$ and $n = (m+2)(m-1)$ have been closely considered. We can also run the linear programming bound using the restricted character table to obtain other values of n, as listed in Table 5.1.

Bibliography

[1] A.E. Brouwer, J.B. Shearer, N.J.A. Sloane and W.D. Smith, A new table of constant weight codes, *IEEE Trans. Inform. Theory* **36** (1990), 1334–1380.

[2] W. Chu, C.J. Colbourn and P.J. Dukes, Constructions for permutation codes in powerline communications, *Des. Codes and Cryptography* **32** (2004), 51–64.

[3] C.J. Colburn, T. Kløve and A.C.H. Ling, Permutation arrays for powerline communication and mutually orthogonal Latin squares, *IEEE Trans. Inform. Theory* **50** (2004), 1289–1291.

[4] P. Delsarte, An algebraic approach to the association schemes of coding theory, *Philips Res. Rep. Suppl.* No. 10 (1973).

[5] M. Deza and S.A. Vanstone, Bounds for permutation arrays, *J. Statist. Plann. Inference* **2** (1978), 197–209.

[6] P. Dukes and N. Sawchuck, Permutation codes of distance four, preprint.

[7] P. Frankl and M. Deza, On the maximum number of permutations within given maximal or minimal distance, *J. Combin. Theory Ser. A* **22** (1977), 352–360.

[8] W. Fulton, *Young Tableaux*, London Mathematical Society Student Texts 35, Cambridge University Press, New York, 1997.

[9] W. Fulton and J. Harris, *Representation Theory*, Springer-Verlag, New York, 1991.

[10] R.L. Graham and N.J.A. Sloane, Lower bounds for constant weight codes, *IEEE Trans. Inform. Theory* **26** (1980), 37–43.

[11] F.D. Murnaghan, *The Theory of Group Representations*, Johns Hopkins Press, Baltimore, 1938.

[12] B. Sagan, *The Symmetric Group*, Brooks/Cole, California, 1991.

[13] H. Tarnanen, Upper bounds on permutation codes via linear programming, *European J. Combin.* **20** (1999), 101–114.

[14] J.H. van Lint and R.M. Wilson, *A Course in Combinatorics*, Cambridge University Press, Cambridge, 1992.