An Introduction to $S(5, 8, 24)$

Maria E. Beane

Thesis submitted to the Faculty of the
Virginia Polytechnic Institute and State University
in partial fulfillment of the requirements for the degree of

Master of Science
in
Mathematics

Ezra A. Brown, Chair
John F. Rossi
Mark M. Shimozono

April 28, 2011
Blacksburg, Virginia

Keywords: Steiner Systems, Error-Correcting Codes, Mathieu Groups, Sphere Packings

An Introduction to $S(5, 8, 24)$

Maria E. Beane

(ABSTRACT)

$S(5, 8, 24)$ is one of the largest known Steiner systems and connects combinatorial designs, error-correcting codes, finite simple groups, and sphere packings in a truly remarkable way. This thesis discusses the underlying structure of $S(5, 8, 24)$, its construction via the $(24, 12)$ Golay code, as well its automorphism group, which is the Mathieu group M_{24}, a member of the sporadic simple groups. Particular attention is paid to the calculation of the size of automorphism groups of Steiner systems using the Orbit-Stabilizer Theorem. We conclude with a section on the sphere packing problem and elaborate on how the 8-sets of $S(5, 8, 24)$ can be used to form Leech's Lattice, which Leech used to create the densest known sphere packing in 24-dimensions. The appendix contains code written for Matlab which has the ability to construct the octads of $S(5, 8, 24)$, permute the elements to obtain isomorphic $S(5, 8, 24)$ systems, and search for certain subsets of elements within the octads.

Acknowledgments

First and foremost, I would like to thank Dr. Brown for directing me towards such an extraordinary area of study, and helping me to survive this past year. I am so grateful for his time, patience, and encouragement, the combination of which has given me the confidence to tackle a task I would have deemed impossible even a year ago. Without his dedication and support, the dreaded stabilizer may never have been conquered. A great deal of thanks is also due to my fellow researchers Jim Dickson and Andy Wills. Their support, feedback, and friendship have added an additional layer of comfort to this often overwhelming process.

In addition, I would like to thank Dr. Rossi and Dr. Shimozono for agreeing to be members of my thesis committee. As they have each served as my professors in the past, I would also like to thank them, as well as the entire Virginia Tech Math Department, for helping me to grow as a mathematician over the past five years. A special note is due to Dr. Haskell for encouraging this sometimes uncertain mathematician to attempt a thesis. The experience has been just as rewarding as he promised.

And lastly, I would like to thank James Duvall as well my unbelievably wonderful family. To Melissa, for keeping a watchful eye on her little sister over the years, and to my parents, for serving as constant sources of encouragement and inspiration. To dad, for blessing me with a bit of his mathematical prowess, and to mom, for giving me the eloquence to translate it into words. I am so proud to be the daughter of such remarkable people.

Though this was an attempt, there will never be enough words to truly express my gratitude to all those mentioned above.

Contents

List of Figures

Chapter 1

Introduction

One of the largest known Steiner systems, $S(5, 8, 24)$ is the set of 8-element subsets of a 24-element base set such that each 5-element subset is contained in only one of the 8-element subsets. As fascinating as it is mysterious, $S(5, 8, 24)$ yields an underlying connection between several seemingly unrelated fields of mathematics, such as combinatorial designs, error-correcting codes, finite simple groups, and sphere packings. The overall goal of this thesis is to acquaint the reader with this remarkable object and hopefully to spark an interest in the mysteries and complexities of discrete mathematics.

Steiner systems are part of an overarching area of mathematics called combinatorial designs, and so we begin our discussion in Chapter 1 with a few introductory definitions and results regarding these more general designs. We then make the transition to a quick overview of Steiner systems in Chapter 2, mainly focusing on issues of existence. From here, we move into Chapter 3, where we describe and dissect the structure of $S(5, 8, 24)$, including its 759 8-element subsets, each of which is called an octad. Interestingly enough, the results in this section are proved without even viewing an actual representation of the octads. To do this, we model the work of Anderson [1] and Todd [9] by combining observations about the system's structure with clever counting arguments. However, this is not to say that viewing the actual system is a waste of time. In fact, constructing the system is perhaps equally as fascinating as the system itself. Thus, in Chapter 4, we discuss the construction of $S(5, 8, 24)$ via the $(24, 12)$ Golay error-correcting code, and an implementation of this method in Matlab

is provided in Appendix A. We encourage the reader to utilize this program to generate the system at least once, in order to make their study more complete.

In Chapter 5, we discuss the automorphism group of $S(5, 8, 24)$, namely the set of permutations of the 24 elements in the base set that simultaneously permute the 8-element subsets amongst themselves. The automorphism group of $S(5, 8, 24)$ is the Mathieu group M_{24}, one of the first five sporadic groups to be discovered. To calculate the order of M_{24}, we enlist the Orbit-Stabilizer Theorem from abstract algebra, a technique that can used to calculate the order of any automorphism group of a Steiner system. Finally, in Chapter 6 we explore $S(5, 8, 24)$'s connection to the problem of sphere packing. Specifically, the system can be used to create the densest known sphere packing (on a lattice) in 24 dimensions.

1.1 Balanced Incomplete Block Designs

In mathematics, a *design* on a set V of v objects called *varieties* is a multiset of subsets of V. We refer to the subsets of V as *blocks*. Since this is an extremely vague definition, we may narrow our focus by placing certain restrictions on the blocks. Note that we have adopted the terminology of Bogart [2, Chapter 6].

Definition 1.1.1. *A design is called*

i) complete *if each block consists of all of V. Otherwise, the design is* incomplete.

ii) k-uniform *if each block has the same size k.*

iii) (pairwise) balanced of index λ *if each pair of distinct varieties appears together in exactly λ of the blocks.*

iv) linked *if any two blocks have exactly μ elements in common.*

v) regular *if each variety appears in exactly r blocks (r is called the* replication number *of the design).*

A design D with v varieties arranged into b blocks is called a *block design* if it is both k

uniform and regular with replication number r. If, in addition, D is balanced of index λ, then we call D a (b, v, r, k, λ) design. Furthermore, if $k < v$ then a (b, v, r, k, λ) design is called a *balanced incomplete block design* (often abbreviated as BIBD). Interestingly, these five parameters are not independent. In fact, b and r can be written in terms of the other three.

Theorem 1.1.2. *In a (b, v, r, k, λ) design,*

i) $r(k-1) = \lambda(v-1)$

ii) $bk = vr$

Proof. Based on [1, Theorem 6.1]

i) Consider $x \in V$. By definition, x is contained in r blocks, and each of these r blocks contains $k-1$ other varieties. So there are $r(k-1)$ pairs in the design which contain x. To obtain the right side of the equation, note that there are $v-1$ with which x can be paired. By definition, each of these pairs appears in exactly λ of the blocks. Since both sides of the equation count the same number, it follows that $r(k-1) = \lambda(v-1)$.

ii) Since each variety appears in exactly r blocks, there are vr appearances of elements altogether. But also each of the b blocks contains k varieties. Thus bk counts the number of appearances of elements altogether as well, and so $bk = vr$. □

1.2 Symmetric, Cyclic, and Isomorphic Designs

At this point, we are well overdue for an example of a block design, and so we begin with the following $(7, 7, 3, 3, 1)$ design:

$$123 \quad 145 \quad 167 \quad 246 \quad 257 \quad 347 \quad 356,$$

where abc denotes the set $\{a, b, c\}$.

Since there are only seven blocks and seven varieties, we can form the blocks by basic

trial and error. That is, we start by assuming that 123 is a block. By our rules, this means that $\{1,2\}$, $\{1,3\}$, and $\{2,3\}$ cannot appear in any of the other blocks. Therefore, we can pick 145 to be another block. Continuing this process will lead us to the above design.

In a $(7,7,3,3,1)$ design, the number of varieties is equal to the number of blocks. That is, $v = b$ rather than $v < b$, and we call this a *symmetric design*. Recall that $bk = vr$ by part (ii) of Theorem 1.1.2, and therefore, in a symmetric design, we have that $k = r$ as well. Because of the equality in parameters, we refer to these designs as (v,k,λ) designs, dropping the b and r. Thus, a $(7,7,3,3,1)$ design will often be referred to as a $(7,3,1)$ design. Another special property about symmetric designs is that they are linked. More specifically, each pair of blocks of a (v,k,λ) design intersects in exactly λ varieties. A proof of this fact can be found in Wallis [10, p. 26 (Corollary 2.10.2)].

There are several ways to group seven varieties into blocks of size three such that the resulting design is a BIBD. For example, another $(7,3,1)$ design is as follows:

$$124 \qquad 235 \qquad 346 \qquad 457 \qquad 561 \qquad 672 \qquad 713$$

How different are these designs? If we apply the permutation $(1)(2)(5)(3\ 4\ 6\ 7)$ to the varieties of the first $(7,3,1)$ design, we obtain the following bijective mapping between designs:

$$\begin{array}{llllllll} 123 & \mapsto & 124 & 167 & \mapsto & 173 & 257 \mapsto 253 & 356 \mapsto 457 \\ 145 & \mapsto & 165 & 246 & \mapsto & 267 & 347 \mapsto 463 & \end{array}$$

It turns out that we can find such an isomorphism between any two $(7,3,1)$ designs. That is, if we have two $(7,3,1)$ designs, say D_1 and D_2, then the varieties of D_1 can be permuted in such a way as to create D_2. In this thesis, all of our examples will have this property. However, just to be thorough, we list an example from Hall [6] in which this is not the case, namely the $(13,3,1)$ designs. There are exactly two nonisomorphic $(13,3,1)$ designs, each of which contains the following 22 triples:

1	2	3	1	12	13	2	11	13	4	10	13	7	8	13
1	4	5	2	4	6	3	4	8	4	11	12	7	10	12
1	6	7	2	5	7	3	5	12	5	8	11			
1	8	9	2	8	10	3	7	11	6	8	12			
1	10	11	2	9	12	4	7	9	6	9	11			

Then, one design contains the triples

$$3\ 6\ 10 \qquad 3\ 9\ 13 \qquad 5\ 6\ 13 \qquad 5\ 9\ 10,$$

while the other design contains the triples

$$3\ 6\ 13 \qquad 3\ 9\ 10 \qquad 5\ 6\ 10 \qquad 5\ 9\ 13.$$

By the placement of varieties 10 and 13, there is no way to transform one into the other.

Now, let's return our focus to the second of the above $(7, 3, 1)$ designs. Note that adding 1 to each entry of block 124 gives block 235, adding 1 to each entry of 235 gives 346, and so on. When we add 1 to each entry of 713, we obtain 124, thus forming a cycle of the blocks. Cleverly, we refer to this as a *cyclic design mod* 7 *with base block* 124. Note that this is equivalent to beginning with block 124 and repeatedly applying the permutation $T = (1\ 2\ 3\ 4\ 5\ 6\ 7)$ on each variety to obtain the subsequent blocks.

More generally, a *cyclic design* is any design for which a permutation such as T exists. Since we have shown that all $(7, 3, 1)$ designs are isomorphic, our first $(7, 3, 1)$ design should be cyclic as well. Indeed this is the case, since applying $T_1 = (1\ 2\ 4\ 3\ 6\ 7\ 5)$ to the elements of the blocks in the first system gives the following mapping of blocks:

$$123 \ \mapsto\ 246 \ \mapsto\ 437 \ \mapsto\ 365 \ \mapsto\ 671 \ \mapsto\ 752 \ \mapsto\ 514 \ \mapsto\ 123.$$

Since constructing block designs is not always an easy task, cyclic designs are a welcome addition to our study. This becomes especially true when we add the fact that, for certain (b, v, r, k, λ) designs, the problem of constructing the design can be reduced to the problem of finding a difference set.

Definition 1.2.1. *A* (v, k, λ) difference set *is a* k*-element subset* D *of* $V = \{0, 1, \ldots, v-1\}$ *such that every nonzero integer mod* v *can be written in exactly* λ *ways as a difference of distinct elements from* D*.*

Theorem 1.2.2. *A* (v, k, λ) *difference set* D *is a base set for a* (v, k, λ) *symmetric design. That is, if* $D = \{v_1, v_2, \ldots, v_k\}$*, then the sets* $D_i = \{v_i + i, \ldots, v_k + i\}$ *are the blocks of the design, where addition is mod* v *and* $1 \leq i < v$*.*

A proof of Theorem 1.2.2 can be found in Hall [6, p. 148 (Theorem 11.1.1)]. Now, recall that in our first $(7, 3, 1)$ design, our base set was 124. Suppose we consider each of the differences of distinct elements from 124:

$$\begin{array}{llll} 1-2 = -1 = 6 \mod 7 & & 2-4 = -2 = 5 \mod 7 \\ 1-4 = -3 = 4 \mod 7 & & 4-1 = 3 \\ 2-1 = 1 & & 4-2 = 2 \end{array}$$

This gives us the set $\{1, 2, 3, 4, 5, 6\}$, where each nonzero integer mod 7 occurs exactly once. Thus, the above theorem says that our second $(7, 3, 1)$ design is cyclic, which we already know to be true. Unfortunately, not all designs are cyclic and so this theorem cannot always be used. For example, we will later investigate the $(9, 3, 1)$ designs which are not cyclic since there does not exist a $(9, 3, 1)$ difference set D. To see this, note that we can form differences from the elements of a size 3 difference set in $3 \cdot 2 = 6$ ways. However, since there are 8 nonzero varieties modulo 9, we cannot possibly have all 8 of these varieties appear even once in a set of size 6. Therefore, we cannot have a $(9, 3, 1)$ cyclic design.

1.3 Methods of Representation

Until now, our representations of designs have been purely numerical; that is, the blocks have been lists of positive integers. However, this is not the only way of representing a design, and we will discuss two alternative representations, keeping in the context of a $(7, 3, 1)$ design.

The first alternative representation of a $(7, 3, 1)$ design is a geometric one, and is displayed in Figure 1.1. The elements $1, \ldots, 7$ are represented by points, and the blocks are represented by lines (all but one being a straight line). Each line contains 3 of the 7 points, and these triples of points form a $(7, 3, 1)$ design. In fact, it is the second of the two $(7, 3, 1)$ designs we listed previously. Therefore, every pair of points lies in a unique line and two lines are either disjoint or intersect in one point. This geometric representation is known as the seven-point plane, and is the simplest example of a *finite projective plane*. More generally, we have the following definition.

Definition 1.3.1. [1, p. 84] *A* finite projective plane of order n *is a* $(v, k, 1)$ *design for which* $v = n^2 + n + 1$, $k = n + 1$ *for some positive integer* $n \geq 2$. *Therefore, there are* $n^2 + n + 1$ *points,* $n^2 + n + 1$ *lines, and the following statements hold:*

i) Any line contains $(n + 1)$ *points.*

ii) Any point lies on $(n + 1)$ *lines.*

iii) Each pair of points lies together in exactly one line.

iv) Each pair of lines intersects in exactly one point.

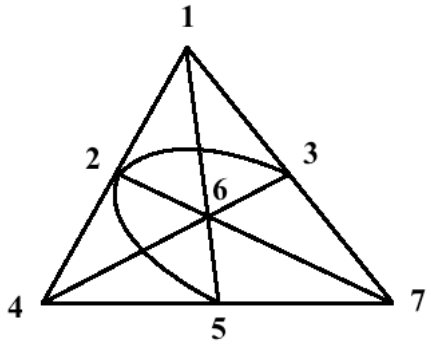


Figure 1.1: Geometric representation of a $(7, 3, 1)$ design.

Note that for a $(v, k, 2)$ design, every pair of varieties determines exactly two blocks and every pair of blocks intersects in exactly two varieties. These designs are called *biplanes*. As is the case with block designs, one of the major unsolved problems regarding projective planes is to find all values of n for which a plane of order n exists. Though we will not give a proof, it has been shown that no finite projective plane of order 6 exists. A thorough proof involving matrix algebra can be found in Anderson [1, p. 85 (Theorem 6.4)].

The next method of representation is called an *incidence matrix*. Suppose we have a (b, v, r, k, λ) design. Then the incidence matrix N has b rows which are indexed by the blocks and has v columns which are indexed by the varieties. More specifically, each entry N_{ij} is the number of times variety j appears in block i, which is either a 0 or a 1 since each block is a set. As an example, the incidence matrix of our second $(7, 3, 1)$ design from the previous section is as follows.

Blocks of Design		Incidence Matrix						
	Indices :	1	2	3	4	5	6	7
124		1	1	0	1	0	0	0
235		0	1	1	0	1	0	0
346		0	0	1	1	0	1	0
457	$\mapsto$	0	0	0	1	1	0	1
156		1	0	0	0	1	1	0
267		0	1	0	0	0	1	1
137		1	0	1	0	0	0	1

Incidence matrices can sometimes reveal the underlying structure of a design more quickly than a numerical representation. For example, in the above matrix, we can see almost instantly that the design is cyclic. Furthermore, from the incidence matrix for a (b, v, r, k, λ) design, we can obtain a $(b, v, b-r, v-k, b-2r+\lambda)$ design. To do so, we first define the *complement* of a (b, v, r, k, λ) design D to be the design obtained by changing 0 to 1 and 1 to 0 throughout the incidence matrix of D.

Theorem 1.3.2. *The complement of a (b, v, r, k, λ) design D is a $(b, v, b-r, v-k, b-2r+\lambda)$ design D'.*

Proof. Let N denote the incidence matrix of D and N' denote the incidence matrix of D'. The complement of a design contains the same number of blocks and varieties as the original design, and thus the first two parameters of D and D' are identical. Since the rows of N denote the blocks of D, the number of 1's in a column i of N is equivalent to the number of blocks of D containing variety i, namely r. Thus, each column of N' contains $b-r$ 1's, and so each variety appears in $b-r$ blocks of D'. Furthermore, the number of times two columns i, j of D intersect in a 1 is equivalent to the number of blocks of D containing the pair i, j of varieties, namely λ, and the number of times they intersect in a 0 is equivalent to the number of blocks of D' containing the pair i, j of varieties, namely $b-2r+\lambda$, since each of the two columns contains r 1's and they intersect in λ 1's. Lastly, each row of D contains k 1's, and thus each row of D' contains $v-k$ 1's. That is, each block of D' has size $v-k$. Thus, D' is a $(b, v, b-r, v-k, b-2r+\lambda)$ design. □

The complement of the above $(7, 3, 1)$ design is as follows:

	Incidence Matrix								Blocks of Design
Indices :	1	2	3	4	5	6	7		
	0	0	1	0	1	1	1		3567
	1	0	0	1	0	1	1		1467
	1	1	0	0	1	0	1		1257
	1	1	1	0	0	1	0	$\mapsto$	1236
	0	1	1	1	0	0	1		2347
	1	0	1	1	1	0	0		1345
	0	1	0	1	1	1	0		2456

Note that this is indeed a $(7, 4, 2)$ design. Theorem 1.3.2 will prove to be extremely useful in our discussion of Golay codes when we discover that the generator matrix of the code contains the incidence matrix of an $(11, 6, 3)$ design as a submatrix.

Chapter 2

Steiner Systems

2.1 t-Designs and an Introductory Definition

Until now, we have only considered pairwise balanced designs, that is, designs in which each pair of distinct varieties appears together a certain number of times. What about designs where each triple or tetrad or quintuple of distinct varieties appear together a certain number of times? We will begin with the following definition.

Definition 2.1.1. *A $t-(v,k,\lambda)$ design consists of k-element subsets of a v-element set V such that each t-element subset of V is contained in exactly λ blocks of the design.*

Note that a $2-(v,k,\lambda)$ design is the same as the balanced incomplete block designs found in the previous sections. Now, at long last, we are ready to define the subject of this paper.

Definition 2.1.2. *A Steiner system, denoted $S(l,m,n)$, is a collection of m-element subsets of an n-element set B, called the* base set*, such that every l-element subset of B lies in exactly one of the m-element sets. That is, $S(l,m,n)$ is an $l-(n,m,1)$ design.*

The subset of these systems where $m=3$ and $l=2$ are called the Steiner triple systems, though they were first studied by a mathematician named Kirkman. As a side note, Kirkman

is quite well known in the field for posing the infamous school girl problem, which led to the question of which triple systems are resolvable. Note that a design is *resolvable* if the blocks may be grouped into s sets each of which is a partition of the set V of varieties. Further details on this subject can be found in Bogart [2, Chapter 6, Section 3].

So how different are Steiner systems from (b, v, r, k, λ) designs? Well, note that a $(7, 3, 1)$ design is actually the same as a $S(2, 3, 7)$ system. Therefore, much of what we have talked about in the previous sections applies to these systems as well.

2.2 Structure and Existence

For simplicity, we will refer to an m-element subset as an m-set. Now, given that a $S(l, m, n)$ exists, there is an exact formula for calculating the number of m-sets (blocks) in the system.

Theorem 2.2.1. *The number of m-sets in an $S(l, m, n)$ is*

$$\frac{\binom{n}{l}}{\binom{m}{l}}.$$

Proof. Let b denote the number of m-sets in $S(l, m, n)$. Note that $\binom{n}{l}$ is the number of distinct l-sets contained in the n-element base set B. Similarly, $\binom{m}{l}$ is the number of distinct l-sets contained in an m-set. By definition, we know that each l-set is contained in exactly one m-set of $S(l, m, n)$. Thus, it follows that

$$\binom{n}{l} = b \cdot \binom{m}{l}, \qquad \text{and so} \qquad b = \frac{\binom{n}{l}}{\binom{m}{l}}.$$

□

As with general block designs, the main open problems dealing with Steiner systems are those of existence. While there are no general existence theorems, there are several theorems which can guarantee existence given specific parameters l, m, and n.

Theorem 2.2.2. *If a system $S(l, m, n)$ exists, so does a system $S(l-k, m-k, n-k)$ for all $0 \leq k < l$.*

Proof. Suppose $k = 1$. Let v be a variety in the base set B, and consider the m-sets of $S(l, m, n)$ in which it is contained. Now, suppose we remove v from each of these m-sets. We have thus created a collection C of $(m-1)$-sets formed from an $(n-1)$-set. In order to conclude the result for $k = 1$, we must show that each of the $(l-1)$-sets is contained in exactly one of the $(m-1)$-sets. Suppose otherwise. That is, two of the $(m-1)$-sets, say P and Q contain the same $(l-1)$-set. But then $(P + v)$ and $(Q + v)$ both contain the same l-set, which is a contradiction to the definition of $S(l, m, n)$. Thus, an $S(l-1, m-1, n-1)$ system exists.

For $k = 2$, let $v_1 \in B$, and consider the $(m-1)$-sets of C (from the above paragraph for $k = 1$) which contain v_1. As before, we remove v_1 from each of the $(m-1)$-sets to obtain an $S(l-2, m-2, n-2)$ system. We can continue this process up to $l-1$ more times, and so the result follows. □

As a direct result of Theorems 2.2.1 and 2.2.2, we have the following corollary.

Corollary 2.2.3. *If $S(l, m, n)$ exists, then*

$$\frac{\binom{n-k}{l-k}}{\binom{m-k}{l-k}} \quad \textit{is an integer}$$

for all $0 \leq k < l$.

It is natural to wonder if the converse of the above corollary is true. Unfortunately, it is not. To see this, consider $l = 2$, $m = 7$, and $n = 43$. Note that

$$\frac{\binom{43}{2}}{\binom{7}{2}} = \frac{903}{21} = 43 \qquad \text{and} \qquad \frac{\binom{42}{1}}{\binom{6}{1}} = 7.$$

However, since $n = 43 = 6^2 + 6 + 1$ and $m = 6 + 1$, then the existence of a $S(2, 7, 43)$ system would imply the existence of a finite projective plane of order 6, which, as we discussed

in Section 1.3, does not exist. Thus, we have found a counterexample to the converse of Corollary 2.2.3.

In the 1970s, only four Steiner systems with $l > 3$ were known to exist, namely $S(5, 6, 12)$, $S(4, 5, 11)$, $S(5, 8, 24)$, and $S(4, 7, 23)$. Since then, a few more have been added such as $S(5, 6, 29)$, $S(5, 7, 28)$, $S(5, 6, 48)$, $S(5, 6, 76)$, $S(5, 6, 84)$, as well as the systems with $l = 4$ which are derived from these systems by the process described in the proof of Theorem 2.2.2. For the special cases of $l = 1$, 2, and 3, we know a bit more about existence of systems.

Theorem 2.2.4.

i) An $S(1, m, n)$ exists if and only if n is a multiple of m.

ii) An $S(2, 3, n)$ exists if and only if $n = 6s + 1$ or $n = 6s + 3$ for some $s \in \mathbb{Z}^+$.

iii) An $S(3, 4, n)$ exists if and only if $n = 6s + 2$ or $n = 6s + 4$ for some $s \in \mathbb{Z}^+$.

Proof.

i) By Corollary 2.2.3, if an $S(1, m, n)$ system exists, then $\frac{\binom{n}{1}}{\binom{m}{1}} = \frac{n}{m} \in \mathbb{Z}^+$. That is, m divides n. But note that an $S(1, m, n)$ system is simply a partition of an n-set into m-sets, which we can construct as long as n is a multiple of m.

ii) ($\Longrightarrow$) Suppose an $S(2, 3, n)$ exists. Then by Corollary 2.2.3,

$$\frac{\binom{n}{2}}{\binom{3}{2}} = \frac{n(n-1)}{6} \in \mathbb{Z}^+ \qquad \text{and} \qquad \frac{\binom{n-1}{1}}{\binom{2}{1}} \in \mathbb{Z}^+.$$

By the second equation, 2 divides $n - 1$ and therefore n is odd. That is, $n = 2a + 1$ for some $a \in \mathbb{Z}^+$. By the first equation, $\frac{n(n-1)}{6} = \frac{(2a+1)2a}{6} = \frac{a(2a+1)}{3} \in \mathbb{Z}^+$. Since 3 is a prime, then either 3 divides a or 3 divides $2a + 1$. So either $a = 3b$ or $2a + 1 = 3c$ for some $b, c \in \mathbb{Z}^+$. If $a = 3b$, then $n = 6b + 1$. Suppose $2a + 1 = 3c$. Since $n = 2a + 1$ and n is odd, it follows that c must be odd as well. So $n = 3(2d + 1) = 6d + 3$.

($\Longleftarrow$) Kirkman proved in 1847 that this condition on n is sufficient for an $S(2, 3, n)$ to exist. A complete proof can be found in Hall [6, p. 280 (Theorem 15.4.3)].

iii) The proof of the forward direction of (iii) relies heavily on Corollary 2.2.3 and thus is

very similar to that of the forward direction of (ii). H. Hanani proved the backward direction, a proof of which is outlined as part of Theorem 15.5.1 in [6]. □

Though we have barely scratched the surface of the field of general Steiner systems, the level of intricacy in these designs is already apparent. A great amount of research has been done on the subject, and we could easily use this chapter as a starting point for a different thesis. However, we have built enough machinery to properly begin our discussion of $S(5, 8, 24)$, and thus we will continue to the main subject of our paper. For the reader who has found his or her interest sparked by this chapter, the references of this paper serve as a wonderful place to discover more about the complexities of general Steiner systems. Specifically, Hall features an entire chapter devoted to the construction (and thus existence) of block designs for certain parameters [6, Chapter 15].

Chapter 3

Dissecting $S(5, 8, 24)$

3.1 The Basics of Octads

As stated in the introduction, the 8-sets of $S(5, 8, 24)$ are called *octads*. By definition, each quintuple of varieties is contained in exactly one octad. However, as can be seen from the following theorem, this is not the only restriction on subsets of the base set.

Theorem 3.1.1. *In* $S(5, 8, 24)$*,*

i) there are 759 *8-sets, called octads,*

ii) each variety is contained in 253 *octads,*

iii) each pair of varieties is contained in 77 *octads,*

iv) each triple of varieties is contained in 21 *octads,*

v) each tetrad of varieties is contained in 5 *octads,*

vi) each quintuple of varieties is contained in 1 *octad.*

Proof. Based on [1, Theorem 7.3]

i) By Theorem 2.2.1, the number of 8-sets in an $S(5, 8, 24)$ is

$$\frac{\binom{24}{5}}{\binom{8}{5}} = \frac{42504}{56} = 759.$$

ii) Let v be a variety in the base set. By the idea found in the proof of Theorem 2.2.2, consider the octads of $S(5,8,24)$ which contain v. If we remove v from each of these octads, we obtain an $S(4,7,23)$ system. So, the number of octads which contain v is the same as the number of 7-sets in $S(4,7,23)$. By Theorem 2.2.1, this is equal to

$$\frac{\binom{23}{4}}{\binom{7}{4}} = 253.$$

iii) Let v_1, v_2 be varieties in the base set. By the proof of part (ii) of this theorem, we can form an $S(4,7,23)$ system by collecting the octads of $S(5,8,24)$ which contain v_1 and then removing v_1 from each of them. Now, consider the 7-sets of this $S(4,7,23)$ system which contain v_2. If we remove v_2 from each of these 7-sets, we obtain an $S(3,6,22)$ system. Then the number of octads which contain v_1 and v_2 is the same as the number of 6-sets in $S(3,6,22)$. By Theorem 2.2.1, this is equal to

$$\frac{\binom{22}{3}}{\binom{6}{3}} = 77.$$

iv, v) Continuing the process used in parts (ii) and (iii), the number of octads which contain a given triple and the number of octads which contain a given tetrad is the same as the number of 5-sets in $S(2,5,21)$ and the number of 4-sets in $S(1,4,20)$, respectively. By Theorem 2.2.1, these two values are

$$\frac{\binom{21}{2}}{\binom{5}{2}} = 21 \quad \text{and} \quad \frac{\binom{20}{1}}{\binom{4}{1}} = 5.$$

vi) This is simply part of the definition of $S(5,8,24)$. □

As is the case with the $(7,3,1)$ designs, though there are several ways in which to write the octads of $S(5,8,24)$, all are isomorphic up to a permutation of the varieties. However, unlike $(7,3,1)$, $S(5,8,24)$ is not a cyclic design, though we will not prove this. Amazingly, we may examine the structure of the octads and their relationships to one another at quite a deep level without even looking at a copy of the actual design. To do so, we rely on clever observations and accompanying combinatorial arguments, both of which have been heavily influenced by Anderson [1] and Todd [9], and therefore most of the credit for the results in this section, as well as Section 3.2, should be given to these two authors.

Theorem 3.1.2. *Let E and F be distinct octads. Then $|E \cap F| < 5$ and $|E \cap F|$ is even.*

Proof. Suppose E and F are distinct octads and $|E \cap F| \geq 5$. By part (vi) of Theorem 3.1.1, each quintuple of varieties is contained in exactly one octad. Thus, it must be that $E = F$, which is a contradiction to our assumption that E and F are distinct.

Now, suppose $|E \cap F|$ is odd. Since $|E \cap F| < 5$, we must the consider the cases where $|E \cap F| = 1$ or 3. Let $E = \{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8\}$, and suppose $|E \cap F| = 3$. Consider $a_1, a_2, a_3 \in E$. Since E contains 5 other varieties, there are exactly 5 tetrads of E which contain $\{a_1, a_2, a_3\}$. By Theorem 3.1.1, each of these tetrads is contained in exactly 4 octads other than E. Thus, there are 20 octads other than E which contain $\{a_1, a_2, a_3, a_i\}$ for some $a_i \in E - \{a_1, a_2, a_3\}$.

But note that each of these 20 octads must be distinct. Suppose otherwise. Then there exists an octad G such that $\{a_1, a_2, a_3, a_i\}, \{a_1, a_2, a_3, a_j\} \in G$, and $a_i \neq a_j$. But this implies that $\{a_1, a_2, a_3, a_i, a_j\} \in G$, which is a contradiction to the fact that each 5-set lies in exactly one octad. Thus, it follows that each of the aforementioned 20 octads are distinct. But then there are 21 octads (counting A) which contain $\{a_1, a_2, a_3\}$ and another variety of E. By Theorem 3.1.1, no other octads can contain the triple $\{a_1, a_2, a_3\}$, and thus it cannot be that $|E \cap F| = 3$.

Let E be as before, but now suppose $|E \cap F| = 1$. Consider $a_1 \in E$. Since E contains 7 other varieties, there are $\binom{7}{3} = 35$ tetrads of E which contain a_1. By Theorem 3.1.1, each of these tetrads is contained in exactly 4 octads other than E. Thus, there are $35 \cdot 4 = 140$ octads other than E which contain $\{a_1, a_i, a_j, a_k\}$ for some $a_1, a_j, a_k \in E - \{a_1\}$. By an argument similar to that used when considering $|E \cap F| = 3$, each of these 140 octads must be distinct. Now, consider $a_2 \in E$. By Theorem 3.1.1, $\{a_1, a_2\}$ is contained in 76 octads other than E. However, note that $\binom{6}{2} \cdot 4 = 60$ of these octads contain a tetrad of the form $\{a_1, a_2, a_i, a_j\}$ for some $a_i, a_j \in E - \{a_1, a_2\}$.

Again, these 60 are distinct and so were counted in the 140 octads from the previous paragraph. We have already shown that two octads cannot intersect in exactly 3 elements. Therefore, the remaining $76 - 60 = 16$ octads which contain $\{a_1, a_2\}$ cannot contain any

more varieties of E. That is, there are 16 distinct octads whose intersection with E is precisely $\{a_1, a_2\}$. Similarly, for each $a_i \in E - \{a_1, a_2\}$, there are 16 distinct octads whose intersection with E is precisely $\{a_1, a_i\}$. This yields $7 \cdot 16 = 112$ distinct octads. Thus we have found $140 + 112 + 1 = 253$ octads (counting A) which contain a_1 and another variety of E. By Theorem 3.1.1, no other octads can contain a_1, and so it cannot be that $|E \cap F| = 1$. $\square$

We now define an operation called *symmetric difference* that can be used to "add" multiple octads together. A useful feature of this operation is that, if S is a set, then the set of subsets of S form a commutative group under symmetric difference.

Definition 3.1.3. *Let S be a set and $A, B \subseteq S$. The* symmetric difference *of A and B, denoted $A + B$, is the set of all elements of S which are in A or B but not both. That is, $A + B = (A \cup B) - (A \cap B)$.*

Though this notation can also refer to the sum of two sets, we will use " + " to denote symmetric difference unless otherwise stated. Now, as a result of the above theorem, we see that if E and F are octads, then either $|E \cap F| = 0$, $|E \cap F| = 2$, or $|E \cap F| = 4$. Since the symmetric difference of E and F is dependent on $E \cap F$, it follows that each of these cases yields a completely different structure of $E + F$. More specifically, $|E \cap F| = 0$ implies $|E + F| = 16$, $|E \cap F| = 2$ implies $|E + F| = 12$, and $|E \cap F| = 4$ implies $|E + F| = 8$.

Theorem 3.1.4. *If E and F are octads and $E \cap F = \emptyset$, then $(E + F)'$ is an octad.*

Proof. Since $E \cap F = \emptyset$, it follows that $|E + F| = 16$ and $|(E + F)'| = 8$. For contradiction, suppose that $(E + F)' = \{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8\}$ is not an octad. By Theorem 3.1.1, $\{a_1, a_2, a_3, a_4, a_5\}$ is contained in exactly one octad, call it G. Since $E \cap F = \emptyset$, then $G \cap (E + F) = G \cap (E \cup F) = (G \cap E) \cup (G \cap F)$. By Theorem 3.1.3, $|G \cap E|$ and $|G \cap F|$ are even, which implies that $|G \cap (E + F)|$ is even. Since $(E + F)$ and $(E + F)'$ are disjoint, it follows that $|G \cap (E + F)'|$ is even as well. That is, $|G \cap (E + F)'| = 6$ or 8. But if $|G \cap (E + F)'| = 8$, then $G = (E + F)'$, which is a contradiction to our assumption that $(E + F)'$ is not an octad. So $|G \cap (E + F)'| = 6$ and, without loss of generality, we may assume $a_6 \in G$ and $a_7, a_8 \notin G$. Now, by Theorem 3.1.1, $\{a_1, a_2, a_3, a_4, a_7\}$ is contained in

exactly one octad, call it H. Similar to before, $|H \cap (E+F)'| = 6$. But if $a_5 \in H$ or $a_6 \in H$, then $G = H$ by Theorem 3.1.1. Thus, it follows that $a_8 \in H$ and $a_5, a_6 \notin H$.

So $\{a_1, a_2, a_3, a_4, a_5, a_6\} \subset G$ and $\{a_1, a_2, a_3, a_4, a_7, a_8\} \subset H$. Again by Theorem 3.1.1, $\{a_1, a_2, a_3, a_5, a_7\}$ is contained in exactly one octad, call it K. As before, we must have $|K \cap (E+F)'| = 6$. However, this is impossible. To see this, first suppose a_4 or $a_6 \in K$. Then $|G \cap K| = 5$, and thus $G = K$, which is a contradiction since $a_7 \in K$ but $a_7 \notin G$. If $a_8 \in K$, then $|H \cap K| = 5$, and thus $H = K$, which is a contradiction since $a_5 \in K$ but $a_5 \notin H$. Therefore, we conclude that $(E+F)'$ is an octad. □

The above theorem is useless unless there actually exist pairs of disjoint octads. It is reasonable to think, even without proof, that these must exist. However, it may be surprising to learn that there are 30 octads which are disjoint from any given octad. Furthermore, each octad belongs to 15 *trios*, where a trio is defined to be a set of three pairwise disjoint octads.

Theorem 3.1.5. *Let E be an octad.*

i) E is disjoint from 30 *octads.*

ii) E belongs to 15 *trios.*

Proof.

i) By Theorem 3.1.3, if F is an octad, then $|E \cap F|$ is even and less than 5. Thus, we will count the number of octads which intersect with E in each of the possible nonzero orders. First, note that each tetrad of E is contained in exactly 4 other octads. So, there are $\binom{8}{4} \cdot 4 = 280$ octads that share a tetrad with E, and each of these octads must be distinct. Otherwise, there exists an octad F which contains two distinct tetrads of E, say T_1 and T_2. Since T_1 and T_2 are distinct, at least one element of T_2 must be different than those of T_1. But then F contains a 5-set of E, which is impossible.

   Each pair P of E is contained in exactly 76 other octads. Since there are 6 elements of E not contained in P, we can form a tetrad of E from P in $\binom{6}{2}$ ways. Therefore, $\binom{6}{2} \cdot 4 = 60$ of the 76 octads which contain P also contain a tetrad of E and so have already been counted among the 280 octads from the previous paragraph. Thus, there

are $76 - 60 = 16$ octads which intersect with E in exactly P and are distinct by the same reasoning as before. Since we can form pairs from E in $\binom{8}{2}$ ways, there are $16 \cdot \binom{8}{2} = 448$ octads that share exactly two elements with E.

Since there are 758 octads other than E in $S(5, 8, 24)$, it follows that $758-280-448 = 30$ of them are disjoint from E.

ii) By part (i), E is disjoint from 30 octads, and let F be one of them. Then by Theorem 3.1.4, $G = (E + F)'$ is an octad. Since G is disjoint from E, G is a member of the 30 octads. But G is disjoint from F as well, so we can form a pair of disjoint octads within the 30. Continuing this process, we can create 14 more pairs of disjoint octads, and so E belongs to 15 trios. □

Continuing our discussion of the relationships between octads, we now focus on the case where $|E \cap F| = 4$.

Theorem 3.1.6. *If E and F are octads and $|E + F| = 8$, then $(E + F)$ is an octad.*

Proof. For contradiction, suppose $E + F = \{a_1, \ldots, a_8\}$ is not an octad. We begin by taking the unique octad G which contains $\{a_1, a_2, a_3, a_4, a_5\}$, and then mimic the proof of Theorem 3.1.4. □

Since an octad contains 8 varieties, we can think of an octad as being the union of two tetrads, which we call *complementary* tetrads. By construction, complementary tetrads are disjoint. Now, using this concept, we provide the following restatement of Theorem 3.1.6.

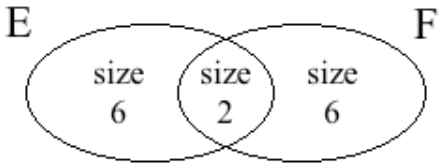
Corollary 3.1.7. *Let T_1, T_2, and T_3 be tetrads. If T_1 and T_2 are both complementary to T_3, then T_1 and T_2 are themselves complementary.*

Proof. By definition, since T_1 and T_2 are both complementary to T_3, then $E = T_1 + T_3$ and $F = T_2 + T_3$ are octads. Since $|E \cap F| = 4$, it follows that $|E + F| = 8$, and therefore, by Theorem 3.1.6, $E + F = T_1 + T_2$ is an octad. That is, T_1 and T_2 are complementary. □

Since each tetrad T is contained in exactly 5 octads, each tetrad determines 5 complementary tetrads, $T_1, \ldots, T_5$. By the above corollary, these 5 complementary tetrads are themselves complementary in pairs. Therefore, T, T_1, $\ldots$, T_5 is a set of 6 mutually complementary tetrads. Since there are $\binom{24}{4} = 10626$ possible tetrads, then there are $\frac{10626}{6} = 1771$ such sets.

3.2 Dodecads

In the previous section, we discussed the cases where the intersection of two octads E and F was either size 0 or 4. We now wish to discuss what happens when the intersection contains two elements, as shown in the picture below. Again, much of our work models that of Anderson and Todd.



In this case, the symmetric difference of E and F forms a special 12-element set called a *dodecad*. This does not imply that every 12-set of the base set is a dodecad. In fact, a 12-set D is a dodecad if and only if we can write it as the symmetric difference of two octads. Therefore, a dodecad can also be thought of as the union of two hexads, where each hexad is contained in an octad of $S(5, 8, 24)$. We refer to these as *special hexads*. Each dodecad only contains one such pair of special hexads since each quintuple of the base set (and thus hexad) is contained in exactly one octad. Now, since a dodecad contains twelve varieties, it seems possible that an 8-set of a dodecad could be an octad of $S(5, 8, 24)$. However, this is not the case.

Theorem 3.2.1. *Let D be a dodecad. Then D contains no octads.*

Proof. Since D is a dodecad, then $D = E + F$ for some octads E and F with $|E \cap F| = 2$. For contradiction, suppose G is an octad and $G \subset D$. Note that E and F both intersect with D in exactly 6 varieties. Thus, $E \not\subset D$ and $F \not\subset D$, and so $E \neq G$ and $F \neq G$. Since $|E \cap G|$ and $|F \cap G|$ are even and less than 5 and $|(E \cap G) + (F \cap G)| = |(E + F) \cap G| =$

$|D \cap G| = 8$, it follows that $|E \cap G| = |F \cap G| = 4$ and $(E \cap G) \cap (F \cap G) = \emptyset$. Let $T_1 = E \cap G$ and $T_2 = F \cap G$. Then T_1 and T_2 are complementary (since $T_1 + T_2 = G$). But recall that $|E \cap F| = 2$, so let $E \cap F = \{a_1, a_2\}$. Then $E = \{T_1, e_1, e_2, a_1, a_2\}$ and $F = \{T_2, f_1, f_2, a_1, a_2\}$ for some e_1, e_2, f_1, f_2. Therefore, T_1 and $\{e_1, e_2, a_1, a_2\}$ are complementary and T_2 and $\{f_1, f_2, a_1, a_2\}$ are complementary. By Corollary 3.1.7, T_2 and $\{e_1, e_2, a_1, a_2\}$ are complementary, and $\{e_1, e_2, a_1, a_2\}$ and $\{f_1, f_2, a_1, a_2\}$ are complementary. But this is a contradiction to our claim that complementary tetrads must be disjoint. Thus, we conclude that D does not contain an octad. □

Thus, since a dodecad contains no octads, the intersection of a dodecad and an octad must contain fewer than 8 elements. Recall from Theorem 3.1.3, that the size of the intersection between two octads must be even and less than 5. It turns out that the intersection of a dodecad and an octad also has 3 possible sizes, namely 2, 4, and 6. Before we prove this, we will prove a seemingly unrelated lemma about the special hexads of a dodecad.

Lemma 3.2.2. *Let D be a dodecad. Any quintuple of D uniquely determines a special hexad. Furthermore, D contains* 132 *special hexads.*

Proof. Let $D = E + F$ be a dodecad, where E and F are octads with $|E \cap F| = 2$, and let $A = \{a_1, a_2, a_3, a_4, a_5\}$ be a 5 element subset of D. By definition, A is contained in exactly one octad, call it G. By Theorem 3.2.1, G cannot be contained in D, so $|G \cap D| < 8$. However, since $|G \cap E|$ and $|G \cap F|$ are both even, it follows that G must contain another element of D, call it a_i. Then $A \cup \{a_i\} \subseteq G$ is a special hexad. But note that the 6 5-sets of $\{a_1, \ldots, a_2, a_i\}$ all determine the same special hexad. Therefore, since A was an arbitrarily chosen 5-set of D, it follows that D contains $\frac{1}{6}\binom{12}{5} = 132$ special hexads. □

Interestingly enough, we can use D to construct a Steiner system $S(5, 6, 12)$. To do this, we let D be the 12 element base set, and let the 6-sets of the system be the special hexads contained in D. By the proof of the above lemma, each 5-element subset of D uniquely determines a sixth element, where the 5-set together with this sixth element forms a special hexad. Thus, each 5-set of D is contained in exactly one of the 6-sets of the system. That is, we have a $S(5, 6, 12)$. Furthermore, by Theorem 2.2.1, the number of 6-sets of $S(5, 6, 12)$

is

$$\frac{\binom{12}{5}}{\binom{6}{5}} = \frac{792}{6} = 132,$$

which matches the number of special hexads contained in D. As a further application of this lemma, we can also now determine exactly how many dodecads can be created.

Theorem 3.2.3. *The number of dodecads is 2576.*

Proof. Each special hexad is contained in exactly 16 dodecads. To see this, consider the special hexad $H = \{a_1, \ldots, a_6\}$. Recall that H can be contained in exactly one octad, call it G. Let g_1, g_2 be the two elements of $G - H$. Then the number of dodecads which contain H is the same as the number of octads whose intersection with G is $\{g_1, g_2\}$. By the proof of part (ii) of Theorem 3.1.3, this number is 16.

Then
(# dodecads) $\cdot$ (# special hexads in a dodecad)

$$= \quad (\#\text{ special hexads}) \cdot (\#\text{ dodecads that contain each special hexad}),$$

which implies that

$$\text{number of dodecads} = \frac{759 \cdot \binom{8}{6} \cdot 16}{132} = 2576.$$

□

We are now ready to prove the aforementioned result about the intersect of octads and dodecads.

Theorem 3.2.4. *Let D be a dodecad and G be an octad. Then $|D \cap G| = 2, 4,$ or 6.*

Proof. Let $T = \{a_1, a_2, a_3, a_4\}$ be a tetrad of D. Since $|D - T| = 8$, we can form a quintuple of D by adding an element to T in 8 ways. By Lemma 3.2.2, a quintuple of D uniquely determines a special hexad. So each of these 8 quintuples determines a special hexad. However, suppose $T \cup \{a_i, a_j\}$ is a special hexad, call it H. Then H is determined by both $T \cup \{a_i\}$ and $T \cup \{a_j\}$. Thus, each tetrad of D is contained in $8/2 = 4$ special hexads in D. Now, recall that each tetrad is contained in 5 octads. So, for each tetrad, 4 of the 5 octads will intersect

D in a special hexad (containing the tetrad) and 1 will intersect D in just the tetrad. There are $\binom{12}{4} = 495$ tetrads in D, and, by Lemma 3.2.2, D contains 132 special hexads. That is, $|D \cap G| = 4$ for 495 octads G, and $|D \cap G| = 6$ for 132 octads G.

Now, consider two elements $a_1, a_2 \in D$. Since $|D - \{a_1, a_2\}| = 10$, we can form a quintuple of D by adding an element to T in $\binom{10}{3} = 120$ ways. Again, by Lemma 3.2.2, each of these 120 quintuples determines a special hexad. However, suppose $\{a_1, a_2, a_i, a_j, a_k, a_m\}$ is a special hexad, call it H_1. Then H_1 is determined by $\{a_1, a_2\} \cup A$, where A is any triple of $\{a_i, a_j, a_k, a_m\}$. There are $\binom{4}{3} = 4$ such triples, and thus $\{a_1, a_2\}$ is contained in $\frac{1}{4} \cdot 120 = 30$ special hexads in D. Recall that each pair is contained in 77 octads. There are $\binom{10}{2} = 45$ tetrads in D which contain $\{a_1, a_2\}$, and so, for each pair, 30 of the 77 octads will intersect D in a special hexad (containing that pair) and 45 will intersect D in just a tetrad (containing the pair). Thus, there are $77-45-30 = 2$ octads which must intersect D in only $\{a_1, a_2\}$.

Since there are $\binom{12}{2} = 66$ pairs of elements in D, it follows that $|D \cap G| = 2$ for $2 \cdot 66 = 132$ octads G. Thus we have found $132 + 495 + 132 = 759$ octads. Since these are all the octads, it follows that $|D \cap G| = 2, 4$, or 6 for all octads G. □

Note that the complement of a dodecad also has 12 elements. However, since a dodecad must be the symmetric difference of two octads, it is a nontrivial statement to claim that the complement of a dodecad is a dodecad.

Theorem 3.2.5. *Let D be a dodecad. Then $B - D$ (the complement of D) is a dodecad.*

Proof. Since D is a dodecad, then $D = E + F$ for some octads E and F with $|E \cap F| = 2$. Let G be one of the 30 octads which are disjoint from E and let $H = (E+G)'$. By Theorem 3.1.4, H is an octad. Note that we cannot have $G \cap F = \emptyset$. Suppose otherwise. Then $H \cap F = (E+G)' \cap F = 6$, and thus $H = F$. But this is impossible since H is disjoint from E but F is not. So $G \cap F \subseteq F - E$, which means $|G \cap F| = 2$ or 4. Suppose $|G \cap F| = 2$. Then $|H \cap F| = 4$, and $H + F$ is an octad by Theorem 3.1.6. But then $D' = G + (H + F)$. Note that if $|G \cap F| = 4$, then $|H \cap F| = 2$, $G \cap F$ is an octad, and $D' = (G + F) + H$. □

3.3 Constructing the Group K

Let G be the group of subsets of the base set $B = \{1, \ldots, 24\}$ with the operation of symmetric difference, and let K be the smallest subgroup of G to contain all the octads.

Let $M = \{\ \emptyset,\ \ \mathrm{B},\ \ 759 \text{ octads},\ \ 759 \text{ complements of octads},\ \ 2576 \text{ dodecads}\ \}$.
Note that $|M| = 4096 = 2^{12}$. In this section, we will prove that $K = M$. To do so, we must first show that $M \subseteq K$. Then, to show that M is exactly K, we must show that M is closed under symmetric difference. The idea for this proof can be found in Anderson [1, p. 109]. However, the author's explanation is brief and many of the details regarding the dodecads are omitted. We supply those details here.

Theorem 3.3.1. *$K = M$.*

Proof. We first show that $M \subseteq K$. By definition, K contains the 759 octads of $S(5, 8, 24)$. Furthermore, since K is a group, it contains all sets of the form $E + F$, where E and F are octads. Thus, K contains all 2576 dodecads. Also $E + E = \emptyset \in K$. Lastly, recall that each octad G belongs to 15 trios. Thus, there exists octads E_1 and F_1 such that $G' = E_1 + F_1 \in K$. Therefore, K contains the complement of each of the 759 octads. We conclude that $M \subseteq K$.

We must now show that M is closed under symmetric difference.

Case 1: Symmetric difference with $\emptyset$: Note that $\emptyset + A = A$ for all $A \in M$.

Case 2: Symmetric difference with B:

2a) $B + B = \emptyset \in M$.

2b) Let E be an octad. Then $B + E = E' \in M$ and $B + E' = E \in M$.

2c) Let D be a dodecad. Then $B + D = D' \in M$, since D' is a dodecad by Theorem 3.2.5.

Case 3: Symmetric difference with an octad E:

3a) Let F be another octad. Then $E+F$ is either the complement of an octad (by Theorem 3.1.4), a dodecad, or an octad (by Theorem 3.1.6). In each case $E+F \in M$.

3b) Let C be the complement of an octad F. Then

$$\begin{aligned} E+C &= E+F' = E+\emptyset+F' = E+(F+F)+F' = E+F+(F+F') \\ &= E+F+B = (E+F)' \end{aligned}$$

By 3a), $(E+F)'$ is either an octad, a dodecad, or the complement of an octad. Thus, $E+C \in M$.

3c) Let D be a dodecad. By Theorem 3.2.3, $|D \cap E| = 2, 4$, or 6.
If $|D \cap E| = 2$, then $|D+E| = 16$, and so $D+E$ must be the complement of an octad. That is $(D+E)'$ is an octad. To prove this, we mimic the proof of Theorem 3.1.4. That is, suppose for contradiction that $(D+E)' = \{a_1, \ldots, a_8\}$ is not an octad. Then, we find the unique octad G which contains $\{a_1, a_2, a_3, a_4, a_5\}$ and continue similar to before. The only difference is that to derive contradictions, we must use the fact that D cannot contain an octad.

If $|D \cap E| = 4$, then $|D+E| = 12$, and so $D+E$ must be a dodecad. Recall that $D = H_1 \cup H_2$, where H_1 and H_2 are special hexads. That is, $H_1 = D \cap F$ and $H_2 = D \cap G$ for some octads F and G. Without loss of generality, suppose $D \cap E \subseteq H_1$, as shown in Figure 3.1. Then $|H_1 \cap E| = 4$. But $H_1 \subseteq F$, and so $|E \cap F| = 4$. Thus,

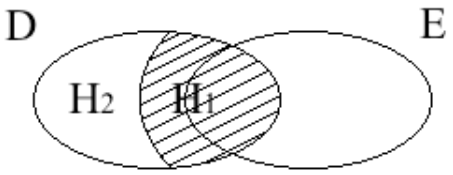


Figure 3.1: Size-4 intersection of a dodecad and octad.

$|E+F| = 8$, and so, by Theorem 3.1.6, $E+F$ is an octad. But note that $D = F+G$. Then $D+E = (F+G)+E = (E+F)+G$. Therefore, $D+E$ is a dodecad.

If $|D \cap E| = 6$, then $|D + E| = 8$, and so $D + E$ must be an octad. As in 3c), this can be proved by mimicking the proof of Theorem 3.1.4.

Case 4: Symmetric difference with the complement of an octad E, denoted E':

4a) Let F' be the complement of an octad F. Then

$$E' + F' = E' + \emptyset + F' = E' + (E + E) + F' = B + (E + F') = (E + F')'$$

By 3b), $E + F'$ is either an octad, a dodecad, or the complement of an octad. Thus, $E' + F' = (E + F')' \in M$.

4b) Let D be a dodecad. So $D = F + G$ for some octads F and G with $|F \cap G| = 2$. Similar to 4a, $E' + D = (E + D)'$. But by 3c), $E + D$ is either the complement of an octad, a dodecad, or an octad. Thus, $E' + D = (E + D)' \in M$.

Case 5: Symmetric difference with a dodecad D_1:

Let D_2 be a dodecad. Then $D_2 = E + F$ for some octads E and F with $|E \cap F| = 2$. Then $D_1 + D_2 = D_1 + (E + F) = E + D_1 + F$. Note that $E + D_1 \in M$ by Case 3c). Then, whether $E + D_1$ is the complement of an octad, a dodecad, or an octad, since F is an octad, it follows by Case 3 that $(E + D_1) + F \in M$.

Therefore, M is closed under symmetric difference and thus is precisely equal to K. □

We postpone further talk of this important group until our section on sphere packings, where we describe how it can be used to create the densest known sphere packing in 24 dimensions. In the meantime, it serves as another fascinating example of information we can glean without ever viewing a copy of $S(5, 8, 24)$.

Chapter 4

Coding Theory

4.1 Introduction to (Binary) Error-Correcting Codes

In the previous section, we effectively studied $S(5, 8, 24)$ in a purely theoretical manner. However, to ensure that our study is complete, we would like to actually view the octads. As stated in the introduction, $S(5, 8, 24)$ can be constructed via the $(24, 12)$ Golay error-correcting code. Thus, to accomplish our next task, we must digress for a moment in order to discuss error-correcting codes. Much of this chapter was influenced by Thompson [8, Chapter 1], Bogart [2, Chapter 6 (Section 5)], and MacWilliams and Sloane [7, Chapter 1, Chapter 2 (Section 6)].

In this day and age, we have come to rely on the electronic transfer of data to make the sending and receiving of information a more efficient and instant process. For example, many people handle all of their financial affairs online, whether it be paying bills or filing taxes. But since this exchange is made from computer to computer (sometimes across noisy or busy networks), we cannot always guarantee our transmission will be error free. Thus, the field of error-correcting codes was born. The goal is to develop efficient methods of encoding messages so that if an error occurs during transmission, the receiver will not only know, but will perhaps even be able to correct the error.

Though error-correcting codes can be discussed over any alphabet, we will narrow our focus

to the case where a message consists of a sequence of binary strings of length n, called *binary n-blocks*. Recall that binary strings are composed solely of 0's and 1's, each of which is called a *bit*. For this fixed n, there are 2^n possible n-blocks. Now, to create a *binary code*, we choose a subset of the 2^n possible n-blocks to be called the *codewords* of the binary code. Ideally, we want to select our codewords in such a way that if an error occurs, the received message is not a codeword, thereby alerting the receiver of the error. Thus, we cannot let the codewords consist of every possible n-block. So, let's consider the following examples:

Definition 4.1.1. *Elementary Examples of Codes:*

- *A repetition code consists of two codewords of a fixed length n, one with all 0's and one with all 1's. In this code, we are able to detect up to $n-1$ errors in transmission. For example, if $n = 2$, then our codewords are $\{00, 11\}$. If 00 is sent and 01 received, the receiver will know that an error has occurred since 01 is not a codeword. However, the error is not correctable as the original codeword could have been either 00 or 11.*
- *The codewords of a block repetition code consist of s copies of all possible r-blocks for some fixed s and r. There are 2^r possible codewords (since there are 2^r possible r-blocks) and each has length $n = r \cdot s$. As before, a single error is detectable, but not correctable. Furthermore, multiple errors are not always detectable. For example, suppose $r = s = 2$ and 0101 is sent but 1111 received. Errors occurred in the 1st and 3rd bits, but since 1111 is a codeword (it is 11 repeated twice), the errors are undetectable.*

In the above examples, we have added more bits to each codeword than necessary in order to guard against errors. These extraneous bits are referred to as *check bits*, while the others are referred to as *message bits*. More generally, an (n, r) *binary block code*, also called an (n, r) code, consists of codewords of length n with r message bits and $n - r$ check bits. The repetition code is an $(n, 1)$ code and the block repetition code is an (rs, r) code. As can be seen in the examples, while error detection is somewhat feasible, error correction seems to be a daunting task. However, let's investigate an idea that can be used to aid in the process.

Definition 4.1.2. *The* Hamming distance*, D, between two binary n-blocks is the number of coordinates in which the corresponding values differ. Equivalently, it is the number of ones in the bitwise addition modulo 2 of the two n-blocks. For example, $D(0010, 0110) = 1$.*

By construction, D is a metric. That is,

i) $D(x, y) \geq 0$ for all x, y and $D(x, y) = 0$ if and only if $x = y$.

ii) $D(x, y) = D(y, x)$ for all x, y.

iii) $D(x, z) \leq D(x, y) + D(y, z)$ for all x, y, z.

How does this help with error correction? Suppose we have a repetition code with codewords of length 4 and suppose 0000 is sent but 0010 is received. This is not a codeword and so we know that an error has occurred. But recall that our two codewords are 0000 and 1111 and $D(0000, 0010) = 1$ while $D(1111, 0010) = 3$. Since one error is more likely than three, we will conclude that 0000 was the original message. This method is referred to as *minimum distance decoding*. More generally, using this strategy in an n length repetition code, we will be able to correct up to $\lfloor \frac{n-1}{2} \rfloor$ errors (where $\lfloor\ \rfloor$ denotes the floor function) by selecting the codeword "closest" to the received word.

Let the *minimum distance* of a code be the minimum of all the distances between two nonidentical codewords. Thus we see that a decent strategy for error correction is to choose a set of codewords where the minimum distance between codewords is as large as possible. Using minimum distance decoding, a code with minimum distance d has the ability to detect up to $d - 1$ errors and correct up to $\lfloor \frac{d-1}{2} \rfloor$ errors.

Codes can also be viewed geometrically; that is, the possible n-blocks are n-tuples in E^n. More specifically, the words can be viewed as the vertices of the unit cube in E^n. For example, Figure 4.1 shows the case when $n = 3$.

Thus, if $\epsilon > 0$, we can define a *sphere of radius* ϵ, centered on a vertex of the unit cube in E^n, as the set of all vertices of the cube with Hamming distance at most ϵ from the given vertex. Now, suppose for a code of length n and for some fixed ϵ, we center an ϵ-sphere on each n-tuple corresponding to a codeword. In order for the minimum distance decoding to be effective, we want to choose our codewords such that for each pair of distinct codewords x and y, an ϵ-sphere around x and an ϵ-sphere around y have no words in common. Note that each ϵ-sphere contains $\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{\epsilon}$ n-tuples. A code is called *perfect* if it makes

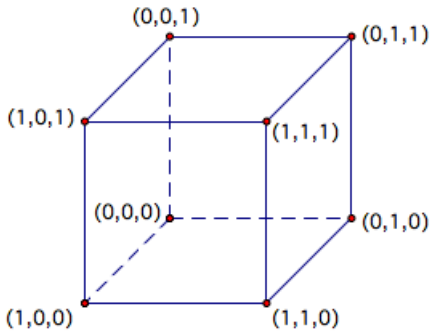


Figure 4.1: Possible 3-blocks.

"perfect" use of the spheres around codewords; that is, an ϵ-error correcting code which can correct precisely up to ϵ errors. More specifically, we have the following.

Definition 4.1.3. *A* perfect code *(of length n) is one for which there exists an integer $\epsilon \geq 0$ such that the ϵ-spheres centered on the codeword n-tuples are pairwise disjoint and each vertex of the unit cube in E^n is contained in some ϵ-sphere.*

As an example of this, consider the $(3, 1)$ repetition code. If we take $\epsilon = \frac{n-1}{2}$, then we see that this code is perfect. On the other hand, the $(2, 1)$ repetition code is not perfect. To see this, note that 0-spheres centered at codewords miss two vertices, but k-spheres (with $k \geq 1$) centered at codewords overlap.

4.2 A First Look at Linear Codes: $(7, 4)$ Hamming Code

As per the name, the codewords of the $(7, 4)$ Hamming Code have length 7 with 4 message bits and 3 check bits, and thus there are $2^4 = 16$ codewords. Each of the check bits is a *parity check* (summation modulo 2) over a different subset of bits. Recall that a set of bits has *even parity* if the sum of the bits modulo 2 is 0, and has *odd parity* otherwise. Specifically, if C_i denotes a check bit and M_i denotes a message bit, each codeword will have the following format:

$$C_1 \ C_2 \ M_1 \ C_3 \ M_2 \ M_3 \ M_4$$

C_1 is a parity check over the 1st, 3rd, 5th, and 7th positions of the codeword,

C_2 is a parity check over the 2nd, 3rd, 6th, and 7th positions of the codeword, and

C_3 is a parity check over the 4th, 5th, 6th, and 7th positions of the codeword.

Why were these specific positions chosen? The answer relies on the binary representation of decimal numbers. Specifically, note the following:

Decimal	1	2	3	4	5	6	7
Binary	001	010	011	100	101	110	111

Thus the first parity check, C_1, is taken over the positions corresponding to decimal numbers whose binary representations have a 1 in the "ones digit," the second parity check, C_2, is taken over the positions corresponding to decimal numbers whose binary representations have a 1 in the "twos place", etc. Furthermore, since 1, 2, and 4 have a single 1 in their binary representations, C_1 is placed in position 1, C_2 is placed in position 2, and C_3 is placed in position 4. Therefore, each set of check bits is independent of the others.

Now, when a message is received, the receiver will perform these same parity checks in order, the result of which will be a binary string of length 3 called the *checking number* or *syndrome*. If the checking number is 000, then the received message is error-free. Otherwise, the checking number will tell the position of the error. For example, suppose we want to send 1010. Our codeword will be $C_1\ C_2\ 1\ C_3\ 0\ 1\ 0$ with $C_1 = 1 + 0 + 0 \equiv 1 \mod 2$, $C_2 = 1 + 1 + 0 \equiv 0 \mod 2$, and $C_3 = 0 + 1 + 0 \equiv 1 \mod 2$. Note that we only have 3 bits in each sum since the 1st, 2nd, and 4th positions of the codeword are initially empty. Thus, we send 1011010, and suppose 1010010 is received. The receiver performs the parity checks as follows:

- Positions 1, 3, 5, 7: $1 + 1 + 0 + 0 \equiv 0 \mod 2$.
- Positions 2, 3, 6, 7: $0 + 1 + 1 + 0 \equiv 0 \mod 2$.
- Positions 4, 5, 6, 7: $0 + 0 + 1 + 0 \equiv 1 \mod 2$.

Thus, the checking number is 100, which corresponds to 4 in decimal and correctly corresponds to the position of the codeword in which the error occurred. Thus we are able to obtain the original message. Though we will omit a proof, the $(7, 4)$ Hamming code is known to be a perfect single-error correcting code.

Now, note that each possible binary 7-block is "mapped" to a checking number of length three. Furthermore, the codewords are mapped to 000. Thus, we can think of the codewords as being the kernel of a linear transformation from $[GF(2)]^7$ to $[GF(2)]^3$, where $[GF(2)]^n$ denotes the set of $(n \times 1)$ column vectors with entries in $\mathbb{F}_2$. Specifically, consider the matrix

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

It turns out that H determines the proper linear transformation. For example, recall the 7-block 1010010 from before which was incorrectly received, and consider it as a 7×1 row vector $\vec{x}$. Then

$$H\vec{x}^T = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$$

gives the correct checking number. Note that ^{T} denotes the transpose of a vector.

Thus, we refer to the $(7, 4)$ Hamming Code as a *linear code* and the matrix H as the *parity-check matrix.* In general, a linear code is a code which can be viewed as a subspace of some vector space. That is, for some $(n - r) \times n$ parity-check matrix H, the codewords of the linear code (n, r) are all row vectors $\vec{x}$ such that $H\vec{x}^T = \vec{0}^T$. In H, a leading one occurs in each of the columns corresponding to a check bit. Therefore, H has rank $n - r$.

Two codes are called *equivalent* if they differ only in the order of the bits of each codeword. Therefore, interchanging the columns of a parity-check matrix for a given (n, r) linear code will give a parity-check matrix for an equivalent (n, r) code. For example, the matrix

$$H' = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

is the parity-check matrix for a linear code equivalent for the $(7,4)$ Hamming Code described above. In this new code, the parity checks will be the last three bits of each codeword.

Now, suppose we have a parity-check matrix in the same form as H' above. That is, $[A \mid I_{n-r}]$ where A is some fixed $(n-r)\times r$ matrix of 0's and 1's and I_{n-r} is the $(n-r)\times(n-r)$ identity matrix. By definition, the codewords will be the vectors $\vec{x}$ such that $[A \mid I_{n-r}]\vec{x}^T = \vec{0}^T$. But then

$$[A \mid I_{n-r}]\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix} \quad \Longrightarrow \quad \begin{bmatrix} x_{r+1} \\ \vdots \\ x_n \end{bmatrix} = -A\begin{bmatrix} x_1 \\ \vdots \\ x_r \end{bmatrix} = -A\begin{bmatrix} m_1 \\ \vdots \\ m_r \end{bmatrix},$$

where $m_1, \ldots, m_r$ are the r message bits. This makes sense since we do not change the message bits during encoding; we simply add check bits. That is, if $\vec{x}$ is a codeword, then $x_1 = m_1, \ldots, x_r = m_r$. Now, since we are working with binary entries, $A = -A$. Thus, we have the following:

$$\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \left[\frac{I_r}{A}\right]\begin{bmatrix} m_1 \\ \vdots \\ m_r \end{bmatrix}.$$

Taking the transpose, we have $\vec{x} = \vec{m}G$, where $G = [I_r \mid A^T]$. G is called the *generator matrix* of the linear code. Since $\vec{x}$ is a codeword, we see that the codewords are all possible linear combinations of the rows of G, and so usually a linear code will be defined by its generator matrix as opposed to its parity check matrix. In an upcoming section, we will explore a (12×24) generator matrix associated with the $(24, 12)$ Golay Code. However, before doing so, we will explore one more interesting feature of the $(7, 4)$ Hamming Code.

4.3 Obtaining $(7, 3, 1)$ from the $(7, 4)$ Hamming Code

Recall the previous parity check matrix H of the $(7, 4)$ Hamming Code:

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

Furthermore, the set of codewords is the kernel of matrix H, that is, all vectors $\vec{x}$ for which $H\vec{x}^T = \vec{0}^T$. Let $\vec{v} = [a_1\ a_2\ \ldots\ a_7]^T$ be a 7×1 column vector. Then

$$\begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \end{bmatrix} = \begin{bmatrix} a_4 + a_5 + a_6 + a_7 \\ a_2 + a_3 + a_6 + a_7 \\ a_1 + a_3 + a_5 + a_7 \end{bmatrix}.$$

So, $a_1 = a_3 + a_5 + a_7$, $a_2 = a_3 + a_6 + a_7$, and $a_4 = a_5 + a_6 + a_7$. Therefore,

$$\begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \end{bmatrix} = \begin{bmatrix} a_3 + a_5 + a_7 \\ a_3 + a_6 + a_7 \\ a_3 \\ a_5 + a_6 + a_7 \\ a_5 \\ a_6 \\ a_7 \end{bmatrix} = a_3 \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} + a_5 \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} + a_6 \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} + a_7 \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{bmatrix},$$

and we see that the kernel of H has rank 4. Specifically, this means that there are $2^4 = 16$ codewords of the $(7, 4)$ Hamming Code. We compute these codewords as follows:

One of $\{a_3, a_5, a_6, a_7\} = 1$	Two of $\{a_3, a_5, a_6, a_7\} = 1$	Three of $\{a_3, a_5, a_6, a_7\} = 1$
1 1 1 0 0 0 0	0 1 1 1 1 0 0	0 0 1 0 1 1 0
1 0 0 1 1 0 0	1 0 1 1 0 1 0	1 0 1 0 1 0 1
0 1 0 1 0 1 0	0 0 1 1 0 0 1	0 1 1 0 0 1 1
1 1 0 1 0 0 1	1 1 0 0 1 1 0	0 0 0 1 1 1 1
	0 1 0 0 1 0 1	
$a_3 = a_5 = a_6 = a_7 = 0$	1 0 0 0 0 1 1	$a_3 = a_5 = a_6 = a_7 = 1$
0 0 0 0 0 0 0		1 1 1 1 1 1 1

The *weight* of a codeword is defined as the number of 1's it contains. Now, consider the codewords of weight three in the above lists. Note that three is the minimum weight of any codeword in the $(7, 4)$ Hamming Code.

	Codewords of Weight 3		Blocks of System
Indices :	**1 2 3 4 5 6 7**		
	1 1 1 0 0 0 0	$\rightarrow$	123
	1 0 0 1 1 0 0	$\rightarrow$	145
	1 0 0 0 0 1 1	$\rightarrow$	167
	0 1 0 1 0 1 0	$\rightarrow$	246
	0 1 0 0 1 0 1	$\rightarrow$	257
	0 0 1 1 0 0 1	$\rightarrow$	347
	0 0 1 0 1 1 0	$\rightarrow$	356

Interestingly enough, this is an $S(2, 3, 7)$ system. Somewhat frequently, the codewords of minimum weight can form an interesting design. In the next section, we will see another example of deriving a Steiner system from the codewords of a code with minimum weight. Specifically, we will examine the $(24, 12)$ Golay code in which the codewords of weight eight form an $S(5, 8, 24)$ system.

4.4 The $(24, 12)$ Golay Code

In 1949, a man named Marcel J. E. Golay presented a generating matrix for what he claimed was a perfect 3-error correcting $(23, 12)$ linear code. While this code is fascinating in its own right, we are more interested in the $(24, 12)$ Golay code, denoted $\mathcal{G}_{24}$, which can be obtained from the $(23, 12)$ Golay code. Specifically, we add either a 0 or a 1 to the end of each row of the generating matrix for the $(23, 12)$ Golay code to make the parity of each row even. The generating matrix for $\mathcal{G}_{24}$, which we will call H, is pictured below. Note that each blank entry of the matrix actually contains a 0, and recall that the codewords of $\mathcal{G}_{24}$ are the set of linear combinations of the rows of H. Since there are 12 rows, there are $2^{12} = 4096$ codewords.

1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	row
1	1												1	1		1	1	1				1		1
1		1												1	1		1	1	1				1	2
1			1										1		1	1		1	1	1				3
1				1										1		1	1		1	1	1			4
1					1										1		1	1		1	1	1		5
1						1										1		1	1		1	1	1	6
1							1						1				1		1	1		1	1	7
1								1					1	1				1		1	1		1	8
1									1				1	1	1				1		1	1		9
1										1				1	1	1				1		1	1	10
1											1		1		1	1	1				1		1	11
												1	1	1	1	1	1	1	1	1	1	1	1	12

Figure 4.2: Generator matrix for the extended Golay code $\mathcal{G}_{24}$.

Since each codeword C is in the row space of H, we can think of C as containing two halves, namely the first twelve bits of C, which are generated by the left half of H, and the last twelve bits of C, which are generated by the right half of H. This is the reason for the somewhat strange column headings in the above figure. We denote these halves of a codeword C as L and R and write $C = |L \mid R|$. Note that adding Row 12 to C forms the codeword $C = |L \mid R'|$ where R' is the complement of R (obtained by interchanging the 0's and 1's).

Furthermore, since each column of H contains an odd number of 1's, the summation of all rows of H gives $(1, \ldots, 1)$, which is therefore a codeword of $\mathcal{G}_{24}$. Since we may add the codeword $(1, \ldots, 1)$ to each codeword C, the complement of C, denoted C', is also a codeword.

Let A denote the 11×11 sub-matrix of H formed by the intersecting entries of the top 11 rows and the right most 11 rows. Then A, which is pictured below, is the incidence matrix for an $(11, 6, 3)$ design.

$$A = \left[\begin{array}{cccccccccccc} 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \end{array}\right]$$

To see this, consider the first row of the matrix which corresponds to the block $B_1 = \{2, 3, 5, 6, 7, 11\}$. Note that this is an $(11, 6, 3)$ difference set and the subsequent blocks are formed by adding $i \mod 11$ to each entry of the block for $1 \leq i < 11$ (as in Theorem 1.2.3). So any two distinct rows of A intersect in exactly three 1's. Furthermore, by our discussion in Chapter 1, A describes the complement of an $(11, 5, 2)$ design. Therefore, any two distinct rows of A intersect in exactly two 0's.

Lemma 4.4.1. *Any three distinct rows of A intersect in either one or two 1's.*

Proof. Without loss of generality, we may consider Row 1, Row 2, and an arbitrary Row i.

Position	1	2	3	4	5	6	7	8	9	10	11	
	1	1	0	1	1	1	0	0	0	1	0	Row 1
	0	1	1	0	1	1	1	0	0	0	1	Row 2
	$\underline{*}$	$\underline{\ }$	$\underline{*}$	$\underline{*}$	$\underline{\ }$	$\underline{\ }$	$\underline{*}$	$\underline{*}$	$\underline{*}$	$\underline{*}$	$\underline{*}$	Row i

In order for the intersection of these three rows to be empty, each of the six 1's of Row i must appear in one of the starred entries. However, since A describes the complement of an $(11, 5, 2)$ design, the three rows cannot intersect in a pair of zeros. Therefore, either the 8th or 9th position of Row i must contain a 1. Furthermore, since Row 1 and Row i must intersect in exactly 3 places, Row i must contain a 1 in positions 1, 4, and 10. In Row i, we now have positions 3, 7, 11 and either 8 or 9 available and two more 1's to place. But, however we place the remaining 1's, it is impossible for Row 2 to intersect with Row i in exactly three ones. Thus, we have a contradiction, and so it follows that any three distinct rows of A intersect in at least one 1.

Now, any three distinct rows cannot interest in more than three 1's since any two distinct rows only intersect in three 1's. Thus, it suffices to show that any three distinct rows of A do not intersect in three 1's. Again, without loss of generality, we consider Row 1, Row 2, and an arbitrary Row i.

Position	1	2	3	4	5	6	7	8	9	10	11	
	1	1	0	1	1	1	0	0	0	1	0	Row 1
	0	1	1	0	1	1	1	0	0	0	1	Row 2
	_	1	_	_	1	1	_	_	_	_	_	Row i

In order for the intersection to contain three 1's, we must have a 1 in positions 2, 5, and 6 of Row i. Now, we must place three more 1's in the remaining spaces of Row i. However we do this, Row i will intersect with either Row 1 or Row 2 in more than 3 places, which is a contradiction. □

By a similar technique, it can be shown that if three distinct rows intersect in exactly one 1, then they intersect in exactly one 0, and if three distinct rows intersect in exactly two 1's, then they do not intersect in any zeros. Recall that the weight of a codeword C, denoted $\mathrm{wt}(C)$, is the number of 1's it contains. We now introduce a series of results about the codewords. The first two are featured in Appendix A of Thompson [8], and the next three are featured in MacWilliams and Sloane [7].

Theorem 4.4.2. *Any two codewords of $\mathcal{G}_{24}$ have an even number of 1's in common.*

Proof. Based on [8, p. 188 (Lemma A2.1)]. We first show that any two rows of H have an

even number of 1's in common. Let Row i and Row j be two distinct rows chosen from the top 11 rows of H. Since A is the incidence matrix of an $(11, 6, 3)$ design, Row i and Row j have exactly four 1's in common (one on the left half and three on the right half). Note that Row i and Row 12 have no 1's in common of the left half and six 1's in common on the right.

Now, let A and B be distinct codewords, and let $\vec{R}_i$ be the ith row of H. By definition, $A = \alpha_1\vec{R}_1 + \alpha_2\vec{R}_2 + \cdots + \alpha_{12}\vec{R}_{12}$ and $B = \beta_1\vec{R}_1 + \beta_2\vec{R}_2 + \cdots + \beta_{12}\vec{R}_{12}$, where each α_i and β_j is either a 0 or a 1. Let AB be the Boolean product of A with B. By definition, this is the vector with 1's where both A and B have a 1 and 0's elsewhere. Then

$$\begin{aligned} AB &= (\alpha_1\vec{R}_1 + \alpha_2\vec{R}_2 + \cdots + \alpha_{12}\vec{R}_{12})(\beta_1\vec{R}_1 + \beta_2\vec{R}_2 + \cdots + \beta_{12}\vec{R}_{12}) \\ &= \alpha_1\beta_1\vec{R}_1\vec{R}_1 + \alpha_1\beta_2\vec{R}_1\vec{R}_2 + \cdots + \alpha_1\beta_{12}\vec{R}_1\vec{R}_{12} \\ &\quad + \ \ldots \ + \ \alpha_{12}\beta_1\vec{R}_{12}\vec{R}_1 + \cdots + \alpha_{12}\beta_{12}\vec{R}_{12}\vec{R}_{12}. \end{aligned}$$

The vector addition is modulo 2 componentwise. Now, each term $\alpha_i\beta_j R_i R_j$ is equal to either the zero vector or the boolean product of $\vec{R}_i$ with $\vec{R}_j$. In either case, we obtain an even number of 1's. But note that the sum of any two vectors with an even number of 1's has an even number of 1's. Thus, it follows that AB has an even number of 1's. That is, A and B have an even number of 1's in common. □

Theorem 4.4.3. *The weight of each codeword is divisible by* 4.

Proof. Based on [8, p. 188 (Corollary A2.2)]. Note that any row of H has weight divisible by 4. Now, consider the sum of any two rows of H. The number of 1's in the resulting codeword is the number of 1's in each row minus twice the number of 1's they have in common. If one of the rows is Row 12, then the resulting codeword has weight $8 + 12 - 2 \cdot 6 = 8$. Otherwise, if both of the rows come from the 11 rows of H, then the resulting codeword has weight $8+8-2\cdot 4 = 8$ (we have already shown that two such rows have exactly four 1's in common). In either case, the weight is divisible by 4.

Now, consider the sum of any three distinct rows of H. If we first add any two of them, by the above paragraph we will obtain a codeword with weight divisible by 4, say $4i$ for some

i. The remaining row (which is also a codeword) also has weight divisible by 4, say $4j$ for some j. By Theorem 4.4.2, these two codewords have an even number of 1's in common, say $2k$ for some k. If we add these two codewords together, the resulting codeword has weight

$$4i + 4j - 2(2k) = 4(i + j - k),$$

which is divisible by 4. Since every codeword of $\mathcal{G}_{24}$ is the linear combination of rows of H, we simply continue this process and the result follows. □

Theorem 4.4.4. *If $\mathcal{G}_{24}$ contains the codeword*

$$C = |\, l_1 l_2 l_3 l_4 \dots l_{12} \,|\, r_1 r_2 r_3 r_4 \dots r_{12} \,|,$$

then it also contains the codeword

$$D = |\, r_1 r_2 r_{12} r_{11} \dots r_3 \,|\, l_1 l_2 l_{12} l_{11} \dots l_3 \,.|$$

Equivalently, $\mathcal{G}_{24}$ is invariant under the permutation of coordinates

$$T = (l_1\ r_1)(l_2\ r_2)(l_3\ r_{12})(l_4\ r_{11}) \dots (l_{12}\ r_3).$$

Proof. Based on [7, p. 65 (Lemma 20)]. Since each codeword of $\mathcal{G}_{24}$ is a linear combination of the rows of H, it suffices to show that each row of H is invariant under T. For example, in the table below we have shown that Row 1 and Row 2 are invariant under T.

Original Row	Mapping under T
1, 1, 0000000000, 0, 1, 1011100010	0, 1, 0100011101, 1, 1, 0000000000
	Sum of rows 1, 3, 7, 8, 9, 11, and 12
1, 0, 1000000000, 0, 0, 1101110001	0, 0, 1000111011, 1, 0, 0000000001
	Sum of rows 2, 6, 7, 8, 10, 11, and 12

The case for the other rows are similar. □

Corollary 4.4.5. *If $\mathcal{G}_{24}$ contains a codeword $|L \mid R|$ with $\mathrm{wt}(L) = i$ and $\mathrm{wt}(R) = j$, then it also contains a codeword $|L' \mid R'|$ with $\mathrm{wt}(L') = j$ and $\mathrm{wt}(R') = i$.*

Theorem 4.4.6. *$\mathcal{G}_{24}$ contains no codewords of weight 4 or 20.*

Proof. Based on [7, p. 66 (Lemma 21)]. Note that each codeword has even weight. Furthermore, because of the first column in H, the left side of each codeword always has even weight, and thus the right side must have even weight as well.

Suppose $C = |L \mid R|$ is a codeword with weight 4. Then either

$$(1)\, \mathrm{wt}(L) = 0, \mathrm{wt}(R) = 4, \quad (2)\, \mathrm{wt}(L) = 4, \mathrm{wt}(R) = 0, \quad \text{or } (3)\, \mathrm{wt}(L) = \mathrm{wt}(R) = 2.$$

Because of Theorem 4.4.4, (1) and (2) are the same case. But case (1) (and thus case (2)) is impossible, since if $\mathrm{wt}(L) = 0$, then either C is the zero vector or C is Row 12 of H. Either way, $\mathrm{wt}(R) \neq 4$. Now, suppose $\mathrm{wt}(L) = 2$ as in case (3). Then either

$$\text{(a) } C = \mathrm{Row}_i + \mathrm{Row}_j \text{ for some distinct } i, j \neq 12 \quad \text{or} \quad \text{(b) } C = \mathrm{Row}_i + \mathrm{Row}_j + \mathrm{Row}_{12}.$$

In case (a), since any two rows of A intersect in exactly three 1's, $\mathrm{wt}(R) = 6$. In case (b), adding Row_{12} gives the complement of the current right hand side, and so $\mathrm{wt}(R) = 6$ as well. Therefore, case (3) is impossible as well, and thus $\mathcal{G}_{24}$ contains no codeword of weight 4.

Now, suppose $\mathcal{G}_{24}$ contains a codeword C_1 of weight 20. Since $I = (1, \ldots, 1)$ is a codeword, then $C_1 + I$ is a codeword as well. But $C_1 + I$ has weight 4, which is a contradiction to the argument of the above paragraph. So $\mathcal{G}_{24}$ contains no codeword of weight 20. □

By Theorem 4.4.3, the weight of each codeword in $\mathcal{G}_{24}$ is divisible by 4. But, from the above theorem, there are no codewords of weight 4 or 20. Thus, the possible weights of codewords in $\mathcal{G}_{24}$ are $0, 8, 12, 16, 24$. We now calculate the number of codewords of each weight, beginning with weight 8.

Theorem 4.4.7. *There are 759 codewords of weight 8.*

Proof. Recall that if $C = |L \mid R|$ is a codeword, then both $\mathrm{wt}(L)$ and $\mathrm{wt}(R)$ are even. Therefore, if $\mathrm{wt}(C) = 8$, we have the following possibilities:

$$\begin{aligned} &\text{Case 1} : \mathrm{wt}(L) = 2, \mathrm{wt}(R) = 6 && \text{Case 4} : \mathrm{wt}(L) = 8, \mathrm{wt}(R) = 0 \\ &\text{Case 2} : \mathrm{wt}(L) = 4, \mathrm{wt}(R) = 4 && \text{Case 5} : \mathrm{wt}(L) = 0, \mathrm{wt}(R) = 8 \\ &\text{Case 3} : \mathrm{wt}(L) = 6, \mathrm{wt}(R) = 2 \end{aligned}$$

However, Cases 4 and 5 are impossible. The only codeword to have weight 0 on the right half is the zero vector $(0, \ldots, 0)$. Furthermore, Row 12 is a codeword with weight 0 on the left half, but it has weight 12 on the right half. Thus, we need only count the other cases.

Number of codewords with $\text{wt}(L) = 2$, $\text{wt}(R) = 6$: $\quad 2(11 + \binom{11}{2})$
Let $C = |L \mid R|$ be one of the top 11 rows of H. Then C is a codeword with $\text{wt}(L) = 2$ and $\text{wt}(R) = 6$. Adding Row 12 to C forms the codeword $|L \mid R'|$ where R' is the complement of R. In this case, $\text{wt}(R) = \text{wt}(R')$, and so we have another codeword with the specified weights. Since we can do this for each of the top 11 rows of H, we have counted $2 \cdot 11$ codewords so far in this case.

Let $C_2 = |L_2 \mid R_2|$ be the sum of two of the (distinct) top 11 rows of H. Since R_2 is equivalent to the sum of any two distinct rows of A, it follows that $\text{wt}(R_2) = 6$. As before, $\text{wt}(R_2) = \text{wt}(R_2')$, and so we may add Row 12 to C_2 to obtain another codeword with the specified weights. Since we can sum together two of the top 11 rows of H in $\binom{11}{2}$ ways, we have found an additional $2 \cdot \binom{11}{2}$ codewords for this case.

Number of codewords with $\text{wt}(L) = 4$, $\text{wt}(R) = 4$: $\quad \binom{11}{3} + \binom{11}{4}$
Let $C_3 = |L_3 \mid R_3|$ be the sum of three of the (distinct) top 11 rows of H. By observation, we see that $\text{wt}(L_3) = 4$, and R_3 is equivalent to the sum of any three distinct rows of A, say Row i, Row j, and Row k, which, by Lemma 4.4.1, intersect in either one or two 1's. Suppose these three rows of A intersect in exactly one 1. Without loss of generality, say

$$\text{Row } i \cap \text{Row } j = \{2, 5, 6\}, \quad \text{Row } i \cap \text{Row } k = \{1, 4, 6\}, \quad \text{Row } j \cap \text{Row } k = \{3, 6, 7\},$$

which occurs when $i = 1$, $j = 2$, and $k = 3$. R_3 contains 11 positions total. By a previous note, these rows intersect in exactly one 0 as well, which contributes to a 0 in R_3. Furthermore, there are six intersections between pairs of rows which do not contribute to the overall intersection among the three rows, and each of these gives another 0 to R_3. Therefore, $\text{wt}(R_3) = 11 - 1 - 6 = 4$.

Now, suppose Row i, Row j, and Row k intersect in exactly two 1's. Without loss of generality, say

$$\text{Row } i \cap \text{Row } j = \{3, 6, 7\}, \quad \text{Row } i \cap \text{Row } k = \{3, 5, 6\}, \quad \text{Row } j \cap \text{Row } k = \{3, 6, 8\},$$

which occurs when $i = 2$, $j = 3$, and $k = 5$. There are three intersections between pairs of rows which do not contribute to the overall intersection among the three rows, and each of these gives a 0 to R_3. By a previous note, these three rows do not intersect in any 0's, and therefore, $\text{wt}(R_3) = 11 - 3 = 8$. However, we may add Row 12 to C_3 to obtain a codeword $|L_3 \mid R_3'|$ with $\text{wt}(L_3) = 4$ and $\text{wt}(R_3') = 4$. Since we can sum three of the top 11 rows of H in $\binom{11}{3}$ ways, we have found $\binom{11}{3}$ codewords in this case so far.

Let $C_4 = |L_4 \mid R_4|$ be the sum of four of the (distinct) top 11 rows of H. By observation, $\text{wt}(L_4) = 4$, and R_4 is equivalent to the sum of any four distinct rows of A. Suppose we first add three of these rows together to create the intermediate codeword $C = |L \mid R|$, and then (if necessary) add Row 12 to C to ensure that $\text{wt}(L) = 4$ and $\text{wt}(R) = 4$. Let Row i be the remaining row of the original four to be added. By Theorem 4.4.2, Row i and C have an even number of 1's in common. Since the left half of Row i and L intersect in exactly one 1, namely the 1 in the far left position, the right side of Row i and R must intersect in either one or three 1's (recall that $\text{wt}(R) = 4$). If the right side of Row i and R intersect in exactly one 1, then $\text{wt}(R_4) = (4-1) + (6-1) = 8$, and so we may add Row 12 to C_4 to obtain the codeword $|L_4 \mid R_4'|$ with $\text{wt}(L_4) = 4$ and $\text{wt}(R_4') = 4$. Otherwise, $\text{wt}(R_4) = (4-3) + (6-3) = 4$, and thus C_4 has the specified weights. Since we can sum four of the top 11 rows of H in $\binom{11}{4}$ ways, we have found $\binom{11}{4}$ additional codewords in this case.

Number of codewords with $\text{wt}(L) = 6$, $\text{wt}(R) = 2$: $\quad 2(11 + \binom{11}{2})$
By Theorem 6.4.4, this is the same as the number of codewords with $\text{wt}(L) = 2, \text{wt}(R) = 6$.

Then, the number of codewords of weight 8 in $\mathcal{G}_{24}$ is

$$2\left(11 + \binom{11}{2}\right) + \binom{11}{3} + \binom{11}{4} + 2\left(11 + \binom{11}{2}\right) = 2 \cdot 132 + 165 + 330 = 759.$$

□

Now, there is exactly one codeword of weight 0, namely $(0, \ldots, 0)$, and one codeword of weight 24, namely $(1, \ldots, 1)$. Since the complement of each codeword is a codeword, it follows that the number of codewords of weight 8 is precisely the same as the number of codewords of weight 16 (since $24 - 8 = 16$). Thus, using Theorem 4.4.7, there are 759 codewords of weight 16. Since the possible weights of codewords in $\mathcal{G}_{24}$ are $0, 8, 12, 16$, and 24,

there are $4096 - 2 - 2 \cdot 759 = 2576$ codewords of weight 12. Note that this is precisely the number of octads, complements of octads, and dodecads associated with $S(5, 8, 24)$, and it is not a coincidence.

Theorem 4.4.8. *The codewords of weight* 8 *in* $\mathcal{G}_{24}$ *form a Steiner system* $S(5, 8, 24)$.

Proof. It suffices to show that any binary vector of weight 5 and length 24 is contained in exactly one codeword of weight 8. Let S be such a vector, and suppose by contradiction that S is contained in two distinct codewords of weight 8, say C_1 and C_2. That is, C_1 and C_2 intersect in at least five 1's. Therefore, $0 < \text{wt}(C_1 + C_2) \leq 8 + 8 - 2 \cdot 5 = 6$, which is a contradiction all nonzero codewords have weight greater than 8. Thus, each binary vector of weight 5 is contained in exactly one codeword of weight 8. □

Therefore, as said before, the octads of $S(5, 8, 24)$ can indeed be constructed via the $(24, 12)$ Golay code. Perhaps the easiest way to do this is to first generate the entire row space of the generator matrix H, which will contains all 4096 codewords. Then, we simply loop through this space and find the codewords of length 8. However, this is probably not the most efficient option. For example, by the proof of Theorem 4.4.7, none of the codewords of weight 8 are a linear combination of more than six rows (since the left side of any such codeword has weight at most 6). Therefore, in generating the entire row space we are unnecessarily considering $\binom{12}{7} + \binom{12}{8} + \binom{12}{9} + \binom{12}{10} + \binom{12}{11} + \binom{12}{12} = 792 + 495 + 220 + 66 + 12 + 1 = 1586$ codewords. An interesting problem lies in trying to develop the most efficient method of finding the codewords of weight 8. However, we did not have sufficient time to consider this topic. The Matlab code found in Appendex A uses the naive row space approach discussed above.

Chapter 5

Automorphism Groups of Steiner Systems

In abstract algebra, we define an automorphism of a group G to be an isomorphism (a mapping that is both one-to-one and onto) from G onto itself. That is, an automorphism of G is a permutation on the set G that preserves the group operation. The set of all automorphism of G is denoted as $\mathrm{Aut}(G)$. Defined in a similar way, each Steiner system $S(l, m, n)$ has an automorphism group, but with an added restriction: each permutation of the blocks must be obtained by a permuting the n elements. We define this precisely as follows:

Definition 5.0.9. *An* automorphism *of a Steiner system $S(l, m, n)$ is a permutation α of the n varieties in the base set that is simultaneously a permutation of the m-sets amongst themselves. The* automorphism group*, denoted $\mathrm{Aut}(S(l, m, n))$ is the group of all such permutations. If $\alpha \in \mathrm{Aut}(S(l, m, n))$, we say that α induces a permutation on the blocks.*

A particularly interesting problem involves how best to calculate the order of an automorphism group. Because the structure of one system varies greatly from another, there is no set formula and no way of even providing an estimate or plausible upper bound. However, if we had unlimited time (as well as unlimited patience), all of these orders, no matter how large the system, could be calculated using the Orbit-Stabilizer Theorem from abstract algebra. Even for smaller systems such as $S(2, 3, 9)$, which we will explore in the next section, this

technique can prove tedious. When handed a system as large as $S(5, 8, 24)$, the task seems impossible. In this case, we are saved by a property of $S(5, 8, 24)$ known as 5-transitivity, the significance of which we will explain in Section 5.2.

5.1 $\mathrm{Aut}(S(2, 3, 9))$

To familiarize ourselves with the concept of an automorphism group, we will begin with an illustrative example: calculating $|\mathrm{Aut}(S(2, 3, 9)|$. The following is a clever way to construct the blocks of $S(2, 3, 9)$. We first take the 3×3 grid with the numbers $1 - 9$ placed as in the dial pad of a telephone. This grid is shown below.

1	2	3
4	5	6
7	8	9

The three rows and columns, namely 123, 456, 789, 147, 258, and 369, make up six of the twelve blocks of $S(2, 3, 9)$. Now, suppose we position an identical grid next to the original one like so:

1	2	3	1	2	3
4	5	6	4	5	6
7	8	9	7	8	9

Notice that we have created the following diagonals in the left and right directions:

1	2	3			
	5	6	4		
		9	7	8	

		3	1	2	
	5	6	4		
7	8	9			

These diagonals constitute the remaining six blocks of $S(2, 3, 9)$. Thus, in lexicographic order, the blocks of $S(2, 3, 9)$ are as follows:

$$
\begin{array}{lll}
B_1 = 123 & B_5 = 249 & B_9 = 357 \\
B_2 = 147 & B_6 = 258 & B_{10} = 369 \\
B_3 = 159 & B_7 = 267 & B_{11} = 456 \\
B_4 = 168 & B_8 = 348 & B_{12} = 789
\end{array}
$$

Now, as mentioned before, to find $|\operatorname{Aut}(2,3,9)|$, we will use the Orbit-Stabilizer Theorem. Before stating the theorem, we begin with a few necessary definitions.

Definition 5.1.1. *Suppose that G is a group of permutations on the set S. Let $g \in G$ and let $T \subseteq S$.*

i) $g(T) = \{g(t) : t \in T\}$.

ii) An element $g \in G$ leaves T setwise fixed *if $g(T) = T$.*

iii) The stabilizer *of T in G, denoted $\operatorname{Stab}_G(T)$, is the set of all permutations $g \in G$ that leave T setwise fixed. Note that if $T = \{t\}$ then $\operatorname{Stab}_G(t)$ is the set of all permutations $g \in G$ that fixed t.*

iv) The orbit *of T, denoted $\operatorname{Orb}_G(T)$, is the set of all $Y \subseteq S$ for which $Y = g(T)$ for some permutation $g \in G$.*

Theorem 5.1.2. *(The Orbit-Stabilizer Theorem) Let G be a finite group of permutations of a set S and let $T \subseteq S$. Then*

i) $\operatorname{Stab}_G(T)$ *is a subgroup of G.*

ii) $|G| = |\operatorname{Stab}_G(T)| \cdot |\operatorname{Orb}_G(T)|$.

A proof can be found Dummit and Foote [5, p. 51, p. 114 (Proposition 2)]. Now, to use the theorem, we begin by defining the groups G, H, and K as follows:

$$\begin{aligned} G &= \operatorname{Aut}(S(2,3,9)) \\ H &= \operatorname{Stab}_G(B_1) = \{\text{automorphisms in } G \text{ that leave } B_1 \text{ setwise fixed}\} \\ K &= \operatorname{Stab}_H(1) = \{\text{automorphisms in } H \text{ that leave 1 fixed}\} \end{aligned}$$

Then, by repeated use of the Orbit-Stabilizer Theorem,

$$\begin{aligned} |G| &= |H| \cdot |\operatorname{Orb}_G(B_1)| \\ &= |K| \cdot |\operatorname{Orb}_H(1)| \cdot |\operatorname{Orb}_G(B_1)| \\ &= |\operatorname{Stab}_K(2)| \cdot |\operatorname{Orb}_K(2)| \cdot |\operatorname{Orb}_H(1)| \cdot |\operatorname{Orb}_G(B_1)| \end{aligned}$$

Even though we seem to be making the problem more complicated, we are in fact doing the opposite. The size of orbits, in general, are much easier to determine than the size of stabilizers. Thus, it is beneficial to simplify as much as possible the one stabilizer whose order we must compute, in this case $\mathrm{Stab}_K(2)$. Leaving the stabilizer for last, we now calculate the size of the orbits.

$|\operatorname{Orb}_G(B_1)|$:

Recall that $B_i \in \operatorname{Orb}_G(B_1)$ if there exists an automorphism f such that $f(B_1) = B_i$. Thus, to calculate $|\operatorname{Orb}_G(B_1)|$, we must determine to which blocks B_1 can be mapped.

Let id_S be given by $\mathrm{id}_S(v) = v$ for all $v \in \{1, 2, \ldots, 9\}$. Then id_S induces the identity mapping on the blocks. Particularly, B_1 is sent to itself, and thus $B_1 \in \operatorname{Orb}_G(B_1)$.

Let $\beta_1 = (1\ 4\ 7)(2\ 5\ 8)(3\ 6\ 9)$.
Then β_1 induces the permutation $(B_2)(B_6)(B_{10})(B_1\ B_{11}\ B_{12})(B_3\ B_8\ B_7)(B_4\ B_5\ B_9)$ on the blocks, which can be seen below:

B_1	123	$\to$	456	B_{11}	B_7	267	$\to$	591	B_3
B_2	147	$\to$	471	B_2	B_8	348	$\to$	672	B_7
B_3	159	$\to$	483	B_8	B_9	357	$\to$	681	B_4
B_4	168	$\to$	492	B_5	B_{10}	369	$\to$	693	B_{10}
B_5	249	$\to$	573	B_9	B_{11}	456	$\to$	789	B_{12}
B_6	258	$\to$	582	B_6	B_{12}	789	$\to$	123	B_1

So $B_{11} = 456 \in \operatorname{Orb}_G(B_1)$.

Now, suppose we were to "reverse" β. That is, instead of sending $1 \to 4$, $4 \to 7$, $7 \to 1$, and so on, we send $4 \to 1$, $7 \to 4$, $1 \to 7$, etc. In doing so, we will still have an permutation of the varieties that simultaneously permutes the blocks amongst themselves. Thus $(\beta)^{-1} = (1\ 7\ 4)(2\ 8\ 5)(3\ 9\ 6)$ is an automorphism of $S(2, 3, 9)$. More generally, the inverse of any automorphism is itself an automorphism. Similarly, the composition of two automorphisms is an automorphism.

We now both summarize and continue our discussion in the following table, though we

will not take the time or space to verify the mappings.

Element Permutation	**Block Permutation**	**Image of B_1**
id_S	$(B_1)(B_2)\dots(B_{12})$	B_1
$\beta_1 = (1\ 4\ 7)(2\ 5\ 8)(3\ 6\ 9)$	$(B_2)(B_6)(B_{10})(B_1\ B_{11}\ B_{12})(B_3\ B_8\ B_7)(B_4\ B_5\ B_9)$	B_{11}
$(\beta_1)^{-1} = (1\ 7\ 4)(2\ 8\ 5)(3\ 9\ 6)$	$(B_2)(B_6)(B_{10})(B_1\ B_{12}\ B_{11})(B_3\ B_7\ B_8)(B_4\ B_9\ B_5)$	B_{12}
$\beta_2 = (1)(2\ 4\ 5\ 8\ 3\ 7\ 9\ 6)$	$(B_1\ B_2\ B_3\ B_4)(B_5\ B_{11}\ B_6\ B_8\ B_9\ B_{12}\ B_{10}\ B_7)$	B_2
$(\beta_2)^{-1} = (1)(2\ 6\ 9\ 7\ 3\ 8\ 5\ 4)$	$(B_1\ B_4\ B_3\ B_2)(B_5\ B_7\ B_{10}\ B_{12}\ B_9\ B_8\ B_6\ B_{11})$	B_4
$(\beta_2)^2 = (1)(2\ 5\ 3\ 9)(4\ 8\ 7\ 6)$	$(B_1\ B_3)(B_2\ B_4)(B_5\ B_6\ B_9\ B_{10})(B_7\ B_{11}\ B_8\ B_{12})$	B_3
$\beta_3 = (2)(1\ 5\ 7\ 9\ 3\ 8\ 6\ 4)$	$(B_1\ B_6\ B_7\ B_5)(B_2\ B_3\ B_9\ B_{12}\ B_{10}\ B_8\ B_4\ B_{11})$	B_6
$(\beta_3)^{-1} = (2)(1\ 4\ 6\ 8\ 3\ 9\ 7\ 5)$	$(B_1\ B_5\ B_7\ B_6)(B_2\ B_{11}\ B_4\ B_8\ B_{10}\ B_{12}\ B_9\ B_3)$	B_5
$(\beta_3)^2 = (2)(1\ 7\ 3\ 6)(4\ 5\ 9\ 8)$	$(B_1\ B_7)(B_5\ B_6)(B_2\ B_9\ B_{10}\ B_4)(B_3\ B_{12}\ B_8\ B_{11})$	B_7
$\beta_4 = (3)(1\ 8\ 5\ 6\ 2\ 4\ 7\ 9)$	$(B_1\ B_8\ B_9\ B_{10})(B_2\ B_{12}\ B_3\ B_4\ B_6\ B_{11}\ B_7\ B_5)$	B_8
$(\beta_4)^{-1} = (3)(1\ 9\ 7\ 4\ 2\ 6\ 5\ 8)$	$(B_1\ B_{10}\ B_9\ B_8)(B_2\ B_5\ B_7\ B_{11}\ B_6\ B_4\ B_3\ B_{12})$	B_5
$(\beta_4)^2 = (3)(1\ 5\ 2\ 7)(4\ 9\ 8\ 6)$	$(B_1\ B_9)(B_8\ B_{10})(B_2\ B_3\ B_6\ B_7)(B_4\ B_{11}\ B_5\ B_{12})$	B_9

Thus, it follows that $|\operatorname{Orb}_G(B_1)| = 12$.

$|\operatorname{Orb}_H(1)|$:
Recall that H consists of the automorphisms that leave B_1 setwise fixed. So $v \in \operatorname{Orb}_H(1)$ if there exists an automorphism f such that $f(B_1) = B_1$ and $f(1) = v$. This means that v must be an element of $\{1, 2, 3\}$. Our findings are displayed in the table below.

Element Permutation	**Block Permutation**	**Image of** 1
id_S	$(B_1)(B_2)\dots(B_{12})$	1
$\alpha_1 = (3)(1\ 2)(4\ 8)(5\ 7)(6\ 9)$	$(B_1)(B_8)(B_9)(B_{10})(B_2\ B_6)(B_3\ B_7)(B_4\ B_5)(B_{11}\ B_{12})$	2
$\alpha_2 = (2)(1\ 3)(4\ 9)(5\ 8)(6\ 7)$	$(B_1)(B_5)(B_6)(B_7)(B_2\ B_{10})(B_3\ B_8)(B_4\ B_9)(B_{11}\ B_{12})$	3

Thus, it follows that $|\operatorname{Orb}_H(1)| = 3$.

$|\operatorname{Orb}_K(2)|$:
Recall that K consists of the automorphism that fix 1 while leaving $B_1\backslash\{1\}$ setwise fixed. So $v \in \operatorname{Orb}_K(2)$ if there exists an automorphism f such that $f(1) = 1$, $f(B_1\backslash\{1\}) = B_1\backslash\{1\}$,

and $f(2) = v$. This means that v must be an element of $\{2, 3\}$. Our findings are displayed in the table below.

Element Permutation	**Block Permutation**	**Image of** 2
id_S	$(B_1)(B_2)\dots(B_{12})$	2
$\beta_2^4 = (1)(2\ 3)(4\ 7)(5\ 9)(6\ 8)$	$(B_1)(B_8)(B_9)(B_{10})(B_2\ B_6)(B_3\ B_7)(B_4\ B_5)(B_{11}\ B_{12})$	3

Thus, it follows that $|\operatorname{Orb}_K(2)| = 2$.

We now turn our attention to the stabilizer $\operatorname{Stab}_K(2)$, which consists of the automorphisms in K that leave 2 fixed. Recall that automorphisms in K must fix 1 pointwise and $B_1\backslash\{1\}$ setwise. Thus, an automorphism f is an element of $\operatorname{Stab}_K(2)$ if $f(1) = 1$, $f(2) = 2$, and $f(B_1\backslash\{1, 2\}) = B_1\backslash\{1, 2\}$. However, note that $B_1\backslash\{1, 2\} = \{3\}$, and so the automorphism f must fix 3 as well.

Now, if we fix one more variety (for example, we send $4 \to 4$), the automorphism must be the identity mapping. To see this, suppose f is an automorphism such that $f(1) = 1$, $f(2) = 2$, $f(3) = 3$, and $f(4) = 4$. Then the result of f so far is as follows:

B_1	1 2 3	$\to$	1 2 3	B_7	2 6 7	$\to$	2 _ _
B_2	1 4 7	$\to$	1 4 _	B_8	3 4 8	$\to$	3 4 _
B_3	1 5 9	$\to$	1 _ _	B_9	3 5 7	$\to$	3 _ _
B_4	1 6 7	$\to$	1 _ _	B_{10}	3 6 9	$\to$	3 _ _
B_5	2 4 9	$\to$	2 4 _	B_{11}	4 5 6	$\to$	4 _ _
B_6	2 5 8	$\to$	2 _ _	B_{12}	7 8 9	$\to$	_ _ _

Recall that each 2-set of $\{1, 2, \dots, 9\}$ is contained in only one 3-set of $S(2, 3, 9)$. Because f must be a permutation of the blocks and $\{1, 4\}$ appears in only B_2, it must be that $B_2 \mapsto B_2$, which means that $7 \mapsto 7$. Similarly, 8 must map to 8 to ensure that B_8 maps to B_8. This chain continues, eventually showing that $f = \mathrm{id}_S$.

Therefore, once we choose the variety to which 4 maps, the rest of our permutation will be decided automatically. Thus, the problem of calculating $|\operatorname{Stab}_K(2)|$ reduces to finding the number of varieties to which 4 can be mapped, while still keeping 1, 2, and 3 fixed. It turns out that there are 6 such automorphisms, each of which is given in the table below.

Element Permutation	**Image of 4**
id_S	4
(1)(2)(3)(4 5 6)(7 9 8)	5
(1)(2)(3)(4 6 5)(7 8 9)	6
(1)(2)(3)(4 7)(5 8)(6 9)	7
(1)(2)(3)(4 8)(5 9)(6 7)	8
(1)(2)(3)(4 9)(5 7)(6 8)	9

Thus, it follows that $|\operatorname{Stab}_K(2)| = 6$.

Using the above results, we conclude that

$$|G| = |\operatorname{Stab}_K(2)| \cdot |\operatorname{Orb}_K(2)| \cdot |\operatorname{Orb}_H(1)| \cdot |\operatorname{Orb}_G(B_1)| = 6 \cdot 2 \cdot 3 \cdot 12 = 432$$

However, note that while we have computed the size of $\mathrm{Aut}(S(2,3,9))$, we have not determined the actual automorphisms. Fortunately, our knowledge of the automorphism group for $S(5,8,24)$ is more extensive. Not only can we determine the size of the group using the Orbit-Stabilizer Theorem, but we can also define the group in terms of a set of three generators. Thus, we have a way of describing the actual automorphisms.

5.2 $\mathrm{Aut}(S(5,8,24))$: The Mathieu Group M_{24}

We begin with a discussion of the classification of finite simple groups. Recall that a group G is called *simple* if $|G| > 1$ and the only normal subgroups of G are 1 and G. The classification was completed in 1980, and the following theorem from Dummit and Foote [5, p. 104] summarizes the results.

Theorem 5.2.1. *There is a list consisting of* 18 *infinite families of simple groups and 26 simple groups (called the* sporadic groups*) not belonging to these families such that every finite simple group is isomorphic to one of the groups in this list.*

Several of the infinite families are introduced in a standard abstract algebra class. For example, one such family consists of the groups of prime order, and another family consists of the alternating groups, A_n, for $n \neq 4$. On the other hand, up until 1965, only five of the sporadic groups had been discovered. These five groups, denoted M_{11}, M_{12}, M_{22}, M_{23}, and M_{24}, were discovered by Emile Mathieu in 1861 and 1873, and thus named the Mathieu groups. Aside from being sporadic groups, each of the Mathieu groups has another interesting and rare property: a high degree of transitivity.

Definition 5.2.2. *A permutation group on a k-set is n-ply transitive if, for any two sequences of n distinct elements of the k-set, say $\{x_1, x_2, \ldots, x_n\}$ and $\{y_1, y_2, \ldots, y_n\}$, there exists an element ϕ of the group such that $\phi(x_i) = y_i$ for $i = 1, 2, \ldots, n$.*

The symmetric group on k letters, denoted S_k, is n-ply transitive for all $1 \leq n \leq k$. However, other than the symmetric groups and the alternating groups, M_{11}, M_{12}, M_{23}, and M_{24} are the only known quadruply transitive groups, and M_{12} and M_{24} are the only known quintuply transitive groups. As a note, other than S_n, where $n \geq 6$, and A_n, where $n \geq 7$, no other permutation groups are known to be sextuply transitive.

Of particular interest to this paper is M_{24}. It is the largest of the above five Mathieu groups, and in fact contains each of the others. There are two seemingly inequivalent definitions for M_{24}, one of which makes the reason for its inclusion in this thesis immediately apparent. A proof of their equivalence can be found in Thompson [8, Appendix 4 (Theorem A4.1)].

Definition 5.2.3.

i) *M_{24} is the automorphism group of $S(5, 8, 24)$.*

ii) *M_{24} is the subgroup of S_{24} generated by the following three permutations:*

$$\begin{aligned}
\alpha &= (24)(1\ 2\ 3\ \ldots\ 23) \\
\gamma &= (1\ 24)(2\ 23)(3\ 12)(4\ 16)(5\ 18)(6\ 10)(7\ 20)(8\ 14)(9\ 21)(11\ 17)(13\ 22)(15\ 19) \\
\delta &= (24)(1)(4)(16)(2\ 19\ 5\ 3\ 7)(6\ 22\ 21\ 11\ 8)(9\ 17\ 14\ 10\ 13)(12\ 20\ 23\ 15\ 18)
\end{aligned}$$

Recall that $S(5, 8, 24)$ is unique up to a permutation of the elements of the 24-set, and thus,

by the above definition, M_{24} is unique. So, exactly how large is $\mathrm{Aut}(S(5,8,24))$? In the previous section, we used the Orbit-Stabilizer Theorem to calculate the order of $\mathrm{Aut}(S(2,3,9))$. However, since $S(5,8,24)$ has a 24-element base set and 759 octads, this approach might seem cumbersome. Luckily, since M_{24} is 5-transitive, this is not the case.

Consider the $S(5,8,24)$ system, call it S, generated by the Matlab code in Appendix A

```
>> S = S5824();
```

and modified by the call

```
>> S = S.iso([6,14,7,18,8,23,14,6,18,7,23,8]);
```

The system S now contains the block $B_1 = \{1,2,3,4,5,6,7,8\}$. Note that our method of calculating the order of $\mathrm{Aut}(S(5,8,24))$ does not require this to be a block; we simply make it so to avoid unnecessary complication. We now define the following groups:

$$\begin{array}{rclcrcl} G &=& \mathrm{Aut}(S(5,8,24)) & & & & \\ H &=& \mathrm{Stab}_G(B_1) & & H_3 &=& \mathrm{Stab}_{H_2}(3) \\ H_1 &=& \mathrm{Stab}_H(1) & & H_4 &=& \mathrm{Stab}_{H_3}(4) \\ H_2 &=& \mathrm{Stab}_{H_1}(2) & & & & \end{array}$$

By repeated use of the Orbit-Stabilizer Theorem, we have the following:

$$\begin{aligned} |G| &= |H| \cdot |\,\mathrm{Orb}_G(B_1)| \\ &= |H_1| \cdot |\,\mathrm{Orb}_H(1)| \cdot |\,\mathrm{Orb}_G(B_1)| \\ &\vdots \\ &= |\,\mathrm{Stab}_{H_4}(5)| \cdot |\,\mathrm{Orb}_{H_4}(5)| \cdot |\,\mathrm{Orb}_{H_3}(4)| \\ &\quad \cdot |\,\mathrm{Orb}_{H_2}(3)| \cdot |\,\mathrm{Orb}_{H_1}(2)| \cdot |\,\mathrm{Orb}_H(1)| \cdot |\,\mathrm{Orb}_G(B_1)| \end{aligned}$$

We first consider $|\,\mathrm{Orb}_G(B_1)|$. Let $B_i \neq B_1$ be one of the octads, and let $\{x_1,\ldots,x_5\}$ and $\{y_1,\ldots,y_5\}$ be 5-sets of B_1 and B_i, respectively. Since M_{24} is 5-transitive, there exists $\phi_i \in M_{24}$ such that $\phi_i(x_j) = y_j$ for $j = 1,2,\ldots,5$. But since each 5-set appears in exactly one of the octads, it must be that the elements of $B_1 \backslash \{x_1,\ldots,x_5\}$ map to the elements of $B_i \backslash \{y_1,\ldots,y_5\}$. That is, ϕ_i maps B_1 to B_i. Since B_i was arbitrarily chosen, it follows that $|\,\mathrm{Orb}_G(B_1)| = 759$.

We now consider $|\operatorname{Orb}_H(1)|$. Note that $v \in \operatorname{Orb}_H(1)$ if there exists an automorphism f such that $f(B_1) = B_1$ and $f(1) = v$. Again, since M_{24} is 5-transitive, for each $x \in B_1$, there exists ϕ_x such that $\phi_x(1) = x$ and ϕ_x maps four of the other elements of B_1 to distinct elements of $B_1 \backslash \{x\}$. Since each quintuple is contained in exactly one octad, this implies that ϕ_x fixes B_1 setwise, and so $x \in \operatorname{Orb}_H(1)$. Therefore, $|\operatorname{Orb}_H(1)| = 8$. By a similar reasoning, $|\operatorname{Orb}_{H_1}(2)| = 7$, $|\operatorname{Orb}_{H_2}(3)| = 6$, $|\operatorname{Orb}_{H_3}(4)| = 5$, and $|\operatorname{Orb}_{H_4}(5)| = 4$.

It remains to calculate $|\operatorname{Stab}_{H_4}(5)|$, which is the number of automorphisms in H_4 that leave 5 fixed. However, recall that the automorphisms in H_4 must fix 1, 2, 3, and 4 as well. So each automorphism in $\operatorname{Stab}_{H_4}(5)$ must fix B_1 setwise, and therefore if $f \in \operatorname{Stab}_{H_4}(5)$, then $f(\{6,7,8\}) = \{6,7,8\}$. Thus, there are 3 elements to which 6 can be mapped.

Suppose $6 \mapsto k$ where $k \in \{6,7,8\}$. Since we have only chosen images for $1,2,3,4,5$, and 6, we have not decided the image of any quintuples not found in B_1 (Recall that each quintuple of $\{1,2,3,4,5,6\}$ can be contained only in B_1). Therefore, the only octad which is fixed setwise is B_1, and so it must be that the elements of $\{9,10,\ldots,24\}$ are fixed setwise. Specifically, note that each tetrad of $\{1,2,3,4,5,6\}$ is contained in four octads other than B_1, and these four octads partition the elements of the 24-set which are not contained in B_1. So, consider one of these $24 - 8 = 16$ elements not found in B_1, say 9. As said before, 9 cannot be mapped to $6,7,8$, but it can be mapped to any of the other elements not found in B_1. Suppose $9 \mapsto m$ where $m \in \{9,10,\ldots,24\}$.

At this point, we want to determine whether we have fixed anymore quintuples, and thus octads. Well, it turns out that we have. To see this, note that there are $\binom{6}{4} = 15$ tetrads of $\{1,2,3,4,5,6\}$. Since each quintuple is contained in exactly one octad, it follows that 9 appears with each of the 15 tetrads in exactly one octad. We have listed the corresponding octads below (again obtained from the Matlab output):

1	2	3	4	9	14	18	20		1	2	5	6	9	14	16	22		2	3	4	5	9	15	22	23
1	2	3	5	9	10	11	24		1	3	4	5	9	12	13	16		2	3	4	6	9	16	17	24
1	2	3	6	9	13	15	21		1	3	4	6	9	11	19	22		2	3	5	6	9	12	18	19
1	2	4	5	9	17	19	21		1	3	5	6	9	17	20	23		2	4	5	6	9	11	13	20
1	2	4	6	9	10	12	23		1	4	5	6	9	15	18	24		3	4	5	6	9	10	14	21

Therefore, each of these 15 octads has another octad to which it is setwise fixed. Furthermore, note that each of the remaining 15 elements $\{10, 11, \ldots, 24\}$ appears in exactly three of the above octads. For example, consider the three octads in the above set which contain the element 10. Using our current mapping of elements, we obtain the following mapping of octads, where $a_1, \ldots, a_9 \in \{10, \ldots, 24\}$:

$$\begin{array}{cccccccccccccccc}
1 & 2 & 3 & 5 & 9 & 10 & 11 & 24 & \mapsto & B_2 = & 1 & 2 & 3 & 5 & m & a_1 & a_2 & a_3 \\
1 & 2 & 4 & 6 & 9 & 10 & 12 & 23 & \mapsto & B_3 = & 1 & 2 & 4 & k & m & a_4 & a_5 & a_6 \\
3 & 4 & 5 & 6 & 9 & 10 & 14 & 21 & \mapsto & B_4 = & 3 & 4 & 5 & k & m & a_7 & a_8 & a_9,
\end{array}$$

Since the three octads on the left intersect in exactly one element, and B_2, B_3, and B_4 are the images of these distinct octads, it follows that $\{a_1, a_2, a_3\}$, $\{a_4, a_5, a_6\}$ and $\{a_7, a_8, a_9\}$ must have exactly one element in common, call it a_i. To continue building an automorphism, we must map 10 to a_i. But note that each of the elements $11, 12, \ldots, 24$ are fixed in a similar manner. Thus there is exactly one way to map the elements $\{10, \ldots, 24\}$, and hence there is exactly one way to map both 7 and 8. That is, by choosing an image for both of the elements 6 and 9, each of the remaining 15 elements has exactly one element to which it can be mapped.

For example, suppose we map 6 to 7 and 9 to 10. We must then have the following mappings:

$$\begin{array}{cccccccc|ccc|cccccccc}
1 & 2 & 3 & 4 & 9 & 14 & 18 & 20 & \mapsto & 1 & 2 & 3 & 4 & 10 & 16 & 21 & 22 \\
1 & 2 & 3 & 5 & 9 & 10 & 11 & 24 & \mapsto & 1 & 2 & 3 & 5 & 10 & 9 & 11 & 24 \\
1 & 2 & 3 & 6 & 9 & 13 & 15 & 21 & \mapsto & 1 & 2 & 3 & 7 & 10 & 12 & 13 & 18 \\
1 & 2 & 4 & 5 & 9 & 17 & 19 & 21 & \mapsto & 1 & 2 & 4 & 5 & 10 & 13 & 14 & 15 \\
1 & 2 & 4 & 6 & 9 & 10 & 12 & 23 & \mapsto & 1 & 2 & 4 & 7 & 10 & 11 & 19 & 20 \\
1 & 2 & 5 & 6 & 9 & 14 & 16 & 22 & \mapsto & 1 & 2 & 5 & 7 & 10 & 17 & 22 & 23 \\
1 & 3 & 4 & 5 & 9 & 12 & 13 & 16 & \mapsto & 1 & 3 & 4 & 5 & 10 & 18 & 19 & 23 \\
1 & 3 & 4 & 6 & 9 & 11 & 19 & 22 & \mapsto & 1 & 3 & 4 & 7 & 10 & 9 & 15 & 17 \\
1 & 3 & 5 & 6 & 9 & 17 & 20 & 23 & \mapsto & 1 & 3 & 5 & 7 & 10 & 14 & 16 & 20 \\
1 & 4 & 5 & 6 & 9 & 15 & 18 & 24 & \mapsto & 1 & 4 & 5 & 7 & 10 & 12 & 21 & 24 \\
2 & 3 & 4 & 5 & 9 & 15 & 22 & 23 & \mapsto & 2 & 3 & 4 & 5 & 10 & 12 & 17 & 20 \\
2 & 3 & 4 & 6 & 9 & 16 & 17 & 24 & \mapsto & 2 & 3 & 4 & 7 & 10 & 14 & 23 & 24 \\
2 & 3 & 5 & 6 & 9 & 12 & 18 & 19 & \mapsto & 2 & 3 & 5 & 7 & 10 & 15 & 19 & 21 \\
2 & 4 & 5 & 6 & 9 & 11 & 13 & 20 & \mapsto & 2 & 4 & 5 & 7 & 10 & 9 & 16 & 18 \\
3 & 4 & 5 & 6 & 9 & 10 & 14 & 21 & \mapsto & 3 & 4 & 5 & 7 & 10 & 11 & 13 & 22
\end{array}$$

Using the aforementioned process, we obtain the following:

$10 \mapsto 11$	$14 \mapsto 22$	$18 \mapsto 21$	$22 \mapsto 17$
$11 \mapsto 9$	$15 \mapsto 12$	$19 \mapsto 15$	$23 \mapsto 20$
$12 \mapsto 19$	$16 \mapsto 23$	$20 \mapsto 16$	$24 \mapsto 24$
$13 \mapsto 18$	$17 \mapsto 14$	$21 \mapsto 13$	

It now remains to find the image of 7 and 8. To do so, we consider any non-B_1 octad containing 7 and its mapping. For example:

$$1\ 2\ 3\ 7\ 9\ 16\ 19\ 23 \quad \mapsto \quad 1\ 2\ 3\ \underline{?}\ 10\ 23\ 15\ 20.$$

The only octad which contains the 5-set $\{1, 2, 3, 10, 23\}$ is $\{1, 2, 3, 8, 10, 15, 20, 23\}$. Thus, it must be that $7 \mapsto 8$, which forces $8 \mapsto 6$, and so we have found the following automorphism:

$$(1)(2)(3)(4)(5)(24)(6\ 7\ 8)(9\ 10\ 11)(12\ 19\ 15)(13\ 18\ 21)(14\ 22\ 17)(16\ 23\ 20).$$

Since there are three choices for 6 and 16 choices for 9, then there are $3 \cdot 16 = 48$ automorphisms which fix $\{1, 2, 3, 4, 5\}$ pointwise and B_1 setwise. That is, $|\operatorname{Stab}_{H_4}(5)| = 48$. Therefore

$$|\operatorname{Aut}(S(5, 8, 24))| = 48 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 759 = 244,823,040,$$

which can be verified using an alternative proof in [8, Appendix 4 (Theorem A4.2)].

Chapter 6

Sphere Packings

The following is a problem which has intrigued mathematicians for years:

> Let E^n be the Euclidean n-space. How should open and congruent n-spheres be positioned in E^n such that none are overlapping and the volume of E^n covered by the spheres is maximal?

This problem is referred to as the sphere packing problem. Different packings of spheres are judged by how much of the given space they leave uncovered by spheres; the less space left uncovered, the better the packing. Essentially, this reduces to finding an appropriate set of points in E^n on which to center congruent n-spheres. For simplicity, most people choose to study packings that occur on a lattice, which is an array of points that continues in a regular pattern in all directions. The precise definition is listed below.

Definition 6.0.4. *Let Λ be a set of points. Λ is a lattice if the following conditions are satisfied:*

i) $\vec{0} \in \Lambda$.

ii) *If* $\vec{x} \in \Lambda$, *then* $-\vec{x} \in \Lambda$.

iii) *If* $\vec{x} \in \Lambda$ *and* $\vec{y} \in \Lambda$, *then* $\vec{x} + \vec{y} \in \Lambda$.

Ideally, we would like to have some kind of numerical figure that gives us a sense of how good a packing is. There are two main ways to estimate this mathematically, and we define them as follows.

Definition 6.0.5.

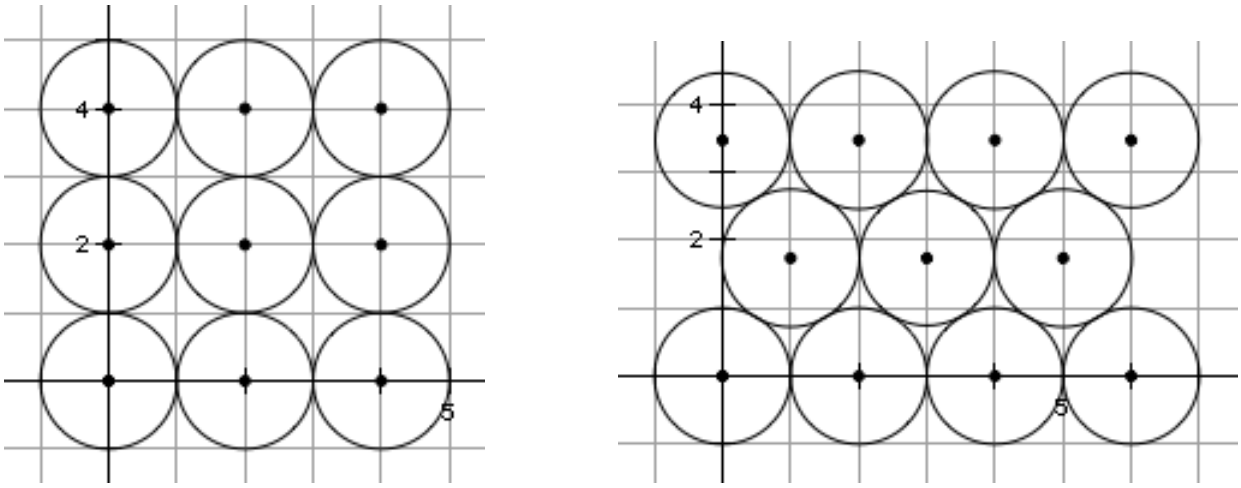
i) The density *of a sphere packing is the fraction of E^n covered by the spheres. In other words, let s be an n-sphere. Then the density is the volume of s divided by the amount of space of E^n which lies closer to the center of s than that of any other sphere.*

ii) Suppose that each open sphere is replaced by its closure. Then the contact number *of a sphere packing is the number of spheres each sphere touches. In a lattice packing, this will be the same for any sphere.*

These two mathematical entities are actually closely related. A packing where each sphere touches a large amount of spheres will yield a higher density than a packing where each sphere touches only a few spheres. Thus, to find a good packing, it suffices to look for a configuration in which each sphere touches as many others as possible. We will use this approach in E^{24} to avoid complications about n-dimensional volume.

6.1 Packings in E^2

To further aid our discussion of the topic, we examine two sphere (or in this case, circle) packings on a lattice in E^2, one of which is the densest known in that dimension. Recall that E^2 is simply the xy-plane. Consider the lattice packings pictured in Figure 6.1. To simplify matters, we have used the same size spheres in each packing. Specifically, each sphere has radius 1 and area π. By observation, we see that the contact number of the packing on Λ_0 is 4, while the contact number of the packing on Λ_1 is 6. Now, we want to calculate the density of each packing. In the packing on Λ_0, note that each 2×2 square contains one circle. Thus, the fraction of each 2×2 square covered by a sphere is $\frac{\pi}{4} \approx 0.7853$, which is then also the density of the entire packing because of its regularity.



(a) $\Lambda_0 = \{m(2,0) + n(0,2) : m, n \in \mathbb{Z}\}$ (b) $\Lambda_1 = \{m(2,0) + n(1,\sqrt{3}) : m, n \in \mathbb{Z}\}$

Figure 6.1: Two lattice packings in E^2.

Calculating the density of the packing on Λ_1 is slightly trickier. First note that we can create a parallelogram P with vertices $\{(2,0),(4,0),(3,\sqrt{3}),(1,\sqrt{3})\}$. Since P has height $\sqrt{3}$ and width 2, then area(P) $= 2\sqrt{3}$. Furthermore, note that P contains the equivalent of one disk, although it is divided into four pieces. Thus, the fraction of each P covered by a sphere is $\frac{\pi}{2\sqrt{3}} \cong 0.9068$, which is then also the density of the entire packing.

The packing on Λ_1 is denser than the packing on Λ_0, and, in fact, the packing on Λ_1 is the densest possible packing in E^2. But the question remains, how do we know that it is the absolute densest packing in E^2? To answer this, we need to discuss the theoretical upper bounds associated with the density sphere packings, and we do so in the next section.

6.2 Rogers' and Coxeter's Upper Bounds for Sphere Packings

Since we can view E^2, perhaps one could claim that Λ_1 "obviously" produces the densest sphere packing in two dimensions. However, what happens when the dimension is greater than three and we can no longer even visualize our sphere packings? At this point, we want

some way of deciding how good a sphere packing is compared with what sphere packings are possible to construct. That is, for each dimension, we would like an upper bound for density and/or contact number. Fortunately, we have both. Though the derivations of each are beyond the scope of this paper, a mention of them is necessary.

The upper bound for the density of a sphere packing in E^n is credited to C. A. Rogers. Before we state the bound, we first define the following:

Definition 6.2.1.

i) The convex hull *of $n+1$ points is the minimal convex set containing them.*

ii) An n-simplex *is a an n-dimensional polytope (geometric object with flat sides) which is the convex hull of its $n+1$ vertices.*

Note that a 1-simplex is a line segment, a 2-simplex is an equilateral triangle, and a 3-simplex is a regular tetrahedron.

Now, Rogers' claim is this (which he proved in 1958):

> The density of a packing in E^n cannot exceed the fraction of a regular n-simplex of a side length two which is interior to the $n+1$ unit spheres whose centers are the vertices of the simplex [8, p. 67].

Let's look at what this means in E^2. That is, the case where $n = 2$. Consider three points in the plane x, y, z where $d(x, y) = d(y, z) = d(x, z) = 2$. A 2-simplex of side length 2 is the equilateral triangle formed by these three points. Now, suppose we center a circle of radius 1 (a unit circle) on each of the points. Let A be the fraction of the 2-simplex contained in one of these three circles. By Rogers' claim, the density of a packing in E^2 cannot be larger than A, which is displayed in Figure 6.2. Note that the portion shaded in black constitutes one half of a unit circle. Thus, $A = \frac{\frac{1}{2}\pi(1)^2}{\frac{1}{2}(2)\sqrt{3}} = \frac{\pi}{2\sqrt{3}}$. But note that this is precisely the density of the packing on Λ_1, which proves that it is indeed the densest possible packing.

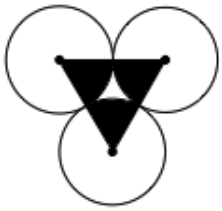


Figure 6.2: Rogers' upper bound in E^2.

Now, for dimension n, the precise formula for this upper bound is given as follows. First, we define $F_n(\alpha)$ recursively by

$$F_{n+1}(\alpha) = \frac{2}{\pi} \int_{\frac{\operatorname{arcsec}(n)}{2}}^{\alpha} F_{n-1}(\beta)\, d\theta,$$

where $\sec(2\beta) = \sec(2\theta) - 2$ and $F_1(\alpha) = F_0(\alpha) = 1$. As a side note, this function was originally defined by Schläfli. Then the upper bound for density is given by

$$\frac{(n+1)^{\frac{1}{2}}(n!)^2\, \pi^{\frac{n}{2}}}{2^{\frac{3n}{2}}\, \Gamma\left(\frac{n}{2}+1\right)} F_n\left(\frac{1}{2}\operatorname{arcsec} n\right),$$

where $\Gamma(x)$ is the Gamma function $\int_0^\infty t^{x-1}e^{-t}dt$. [8, p. 68]

Recall our earlier statement that an upper bound exists for both density and contact number. We now address the latter one to which H. S. M. Coxeter is given credit. Again, the details are omitted, but readers who wish to delve deeper into the subject can find their curiosities satisfied by Coxeter's article [4]. The initial form of the upper bound for contact number is given by the following formula:

$$\frac{2F_{n-1}\left(\frac{1}{2}\operatorname{arcsec} n\right)}{F_n\left(\frac{1}{2}\operatorname{arcsec} n\right)},$$

where F_n is defined as before. While Coxeter is given credit for derivation, John Leech is given credit for computation of $n \leq 8$, where he chose to simplify matters by writing $f_n(\sec 2\alpha)$ for $F_n(\alpha)$. Then $f_n(x) = F_n\left(\frac{1}{2}\operatorname{arcsec} x\right)$, and thus the upper bound becomes:

$$\frac{2f_{n-1}(n)}{f_n(n)}.$$

In the table below, we list the upper bounds for density and contact number for certain dimensions n. The values related to density use Rogers' upper bound and can be found in Thompson [8, Appendix 1], which contains results for dimensions 1 through 24 and a few even greater than 24. The values related to contact number use Coxeter's upper bound and can be found in both Anderson [1, p. 114] and Coxeter [4, p. 68].

n	**Maximum Density Attained**	**Density Upper Bound**	**Maximum Contact Number Attained**	**Contact Number Upper Bound**
1	1.0	1.0	2	2
2	0.9068	0.9068	6	6
3	0.7404	0.7796	12	12
4	0.6168	0.6477	24	26
5	0.4652	0.5256	40	48
8	0.2536	0.2567	240	244
24	0.002455	0.001929	196560	263285

6.3 Leech's Lattice

Though we cannot visualize dimensions above three, sphere packing problems exist in all dimensions. Thus, in one great leap, we now enter the realm of E^{24} in which John Leech discovered a surprisingly dense lattice packing. The underlying lattice has appropriately been given the name Leech's lattice, and though no one has been able to verify whether or not a denser packing exists, many people are confident that one does not.

One of the most interesting facts about Leech's lattice, and the reason for its inclusion in this thesis, is that it can be derived from the Steiner system $S(5, 8, 24)$. To do this, we use the group K, which we described earlier in Section 3.3. Recall that if G is the group of subsets of the base set B with the operation of symmetric difference, then K is the smallest subgroup of G to contain all the octads of $S(5, 8, 24)$. In the aforementioned section, we showed that K has size 2^{12} and consists of the octads, their complements, the dodecads, the empty set, and the base set B. We are now ready to define Leech's lattice.

Definition 6.3.1. *Let $C \in K$ and $m \in \mathbb{Z}$. Let $C(m)$ denote the set of all twenty-four-dimensional vectors $\mathbf{x} = (x_1, x_2, \ldots, x_{24})$ such that*

(a) each x_i is an integer, and $\sum_{i=1}^{24} x_i = 4m$,

(b) $x_i \equiv m (\mathrm{mod}\, 4)$ if $i \notin C$,

(c) $x_i \equiv m + 2 (\mathrm{mod}\, 4)$ if $i \in C$.

Let Λ be the union of all the sets $C(m)$. Then Λ is called Leech's lattice.

Before we continue, we first verify that Leech's lattice is indeed a lattice.

Theorem 6.3.2. *Λ is a lattice.*

Proof. Based on [1, p. 112]. We must verify the three necessary conditions.

(i) $\underline{\mathbf{0} \in \Lambda}$: Let $m = 0$ and note that $\emptyset \in K$. Then $\mathbf{0} = (0, 0, \ldots, 0) \in \emptyset(0)$.

(ii) $\underline{\text{If } \mathbf{x} \in \Lambda, \text{ then } -\mathbf{x} \in \Lambda}$: Suppose $\mathbf{x} \in \Lambda$. Then $\mathbf{x} \in C(m)$ for some $C \in K$ and $m \in \mathbb{Z}$. So $-\mathbf{x} \in C(-m)$, and thus $-\mathbf{x} \in \Lambda$.

(iii) $\underline{\text{If } \mathbf{x} \in \Lambda \text{ and } \mathbf{y} \in \Lambda, \text{ then } \mathbf{x} + \mathbf{y} \in \Lambda}$: Suppose $\mathbf{x}, \mathbf{y} \in \Lambda$. Then $\mathbf{x} \in C(m)$ and $\mathbf{y} \in D(n)$ for some $C, D \in K$ and $m, n \in \mathbb{Z}$. We will show that $\mathbf{x} + \mathbf{y} \in (C + D)(m + n)$ by considering the ith component. Note that this is possible since $C + D \in K$.

Case 1 : $i \in C$ and $i \in D$. Then $i \notin C + D$. Furthermore, $x_i \equiv m + 2 (\mathrm{mod}\, 4)$ and $y_i \equiv n + 2 (\mathrm{mod}\, 4)$. Thus $x_i + y_i \equiv m + n (\mathrm{mod}\, 4)$, so condition (b) holds for i.

Case 2 : $i \in C$ and $i \notin D$. Then $i \in C + D$. Furthermore, $x_i \equiv m + 2 (\mathrm{mod}\, 4)$ and $y_i \equiv n (\mathrm{mod}\, 4)$. Thus $x_i + y_i \equiv m + n + 2 (\mathrm{mod}\, 4)$, so condition (c) holds for i

Case 3 : Similar to Case 2.

Case 4 : $i \notin C$ and $i \notin D$. Then $i \notin C + D$. Furthermore, $x_i \equiv m (\mathrm{mod}\, 4)$ and $y_i \equiv n (\mathrm{mod}\, 4)$. Thus $x_i + y_i \equiv m + n (\mathrm{mod}\, 4)$, so condition (b) holds for i.

Since i denoted an arbitrary component, we conclude that $\mathbf{x} + \mathbf{y} \in (C + D)(m + n)$.

Since the three necessary conditions holds, it follows that Λ is a lattice. □

To obtain a sphere packing, we will center a sphere of radius $\frac{1}{2}b(\Lambda)$ on each of the points in Λ, where $b(\Lambda)$ is the shortest distance of a point of Λ from the origin. That is, $b(\Lambda)$ is the minimum value of $\sqrt{(x_1^2 + \cdots + x_{24}^2)}$ such that $(x_1, \ldots, x_{24}) \neq (0, \ldots, 0)$ and conditions (a), (b), and (c) of Definition 6.3.1 hold for some $C \in K$ and $m \in \mathbb{Z}$. Note that we have borrowed the notation "$b(\Lambda)$" from Anderson [1, p. 113]. Furthermore, the proofs which follow are heavily influenced by his work in [1], though they have been expanded upon.

Before we begin, suppose $C \in K$ is an octad. Then sixteen elements of the base set B are not in C and eight elements of B are in C. Thus, by the definition of Λ, there are sixteen x_i's which are congruent to $m \bmod 4$ and eight x_i's which are congruent to $m+2 \bmod 4$. This idea is extended to the other elements of K in the table below.

	# of x_i's $\equiv m (\bmod 4)$	# of x_i's $\equiv m+2 (\bmod 4)$
Base set	0	24
Empty set	24	0
Octad	16	8
Complement of an octad	8	16
Dodecad	12	12

We now compute $b(\Lambda)$ in the following theorem.

Theorem 6.3.3. *$b(\Lambda) = \sqrt{32}$.*

Proof. Based on [1, p. 113-114]. Let $\vec{x} = (x_1, \ldots, x_{24}) \in \Lambda \backslash (0, \ldots, 0)$. By conditions (b) and (c) of Definition 6.3.1, either all of the x_i are even or all of the x_i are odd, depending on whether m is even or odd. Thus, in computing the minimum distance of $\vec{x}$ from the origin, we must consider both the case where $\vec{x}$ contains all even coordinates as well as when $\vec{x}$ contains all odd coordinates.

Case 1 : m is even, and thus all of the x_i are even.

Case 1a : All x_i are multiples of 4.

Then $\vec{x} = (4k_1, \ldots, 4k_{24})$ for some $k_1, \ldots, k_{24}$, and $\sum_{i=1}^{24} x_i = 4m$. If $m = 0$, then $\sum_{i=1}^{24} x_i = 0$. But $\vec{x}$ is not the origin, and so at least one x_i is nonzero, say x_1. Since the above summation is 0, there exists x_j such that $x_j = -x_1$.

Note that ± 4 are the multiples of 4 with smallest nonzero magnitude. Therefore, $\sum_{i=1}^{24} x_i^2 \geq 4^2 + 4^2 = 32$, and so $b(\Lambda) \geq \sqrt{32}$.

If $m \geq 2$, then $\sum_{i=1}^{24} x_i \geq 4 \cdot 2 = 8$, and so either one x_i is at least 8, or there are two x_i's which have magnitude at least 4. In either case, $\sum_{i=1}^{24} x_i^2 \geq 32$, which again gives $b(\Lambda) \geq \sqrt{32}$. If $m \leq -2$, then $\sum_{i=1}^{24} x_i \leq 4 \cdot (-2) = -8$, and by a similar argument, $b(\Lambda) \geq \sqrt{32}$.

Case 1b : There exists at least one $x_i \not\equiv 0 \bmod 4$.

Without loss of generality, suppose $x_1 \not\equiv 0 \bmod 4$, which implies that $x_1 \equiv 2 \bmod 4$ since x_1 is even. If $m \equiv 0 \bmod 4$, then $x_1 \equiv m + 2 \bmod 4$. By the above table, there exists at least seven other x_i's which are congruent to $m + 2$ modulo 4, which implies that $|x_i| \geq 2$ for at least eight of the x_i's. On the other hand, if $m \equiv 2 \bmod 4$, then $x_1 \equiv m \bmod 4$, which again implies that eight of the x_i's satisfy $|x_i| \geq 2$. Therefore, $\sum_{i=1}^{24} x_i^2 \geq 8 \cdot 2^2 = 32$, and thus $b(\Lambda) \geq \sqrt{32}$.

Case 2 : m is odd, and thus all of the x_i are odd.

Then each $|x_i| \geq 1$. If one coordinate, say x_1 has magnitude strictly larger than 1, then $|x_1| \geq 3$ and thus $\sum_{i=1}^{24} x_i^2 \geq 3^2 + 23 \cdot 1 = 32$. So suppose all $x_i = \pm 1$. Since $1 \not\equiv -1 \bmod 4$, if $1 \equiv m (\bmod 4)$, then $-1 \equiv m + 2 (\bmod 4)$. Thus, by the chart, we can have the following possible breakdowns of $+1$'s and -1's within an 24-tuple, along with the corresponding sums of their coordinates:

$+\mathbf{1}$'s	$-\mathbf{1}$'s	$\sum_{\mathbf{i=1}}^{\mathbf{24}} \mathbf{x_i}$
0	24	-24
8	16	-8
12	12	0
16	8	8
24	0	24

In each case, $4n = \sum_{i=1}^{24} x_i = 4m$ for some $n \in \mathbb{Z}$, which is a contradiction to our assumption that m is odd. Thus we cannot have all $x_i = \pm 1$, and so $b(\Lambda)$ is still greater than or equal to $\sqrt{32}$, as from Case 1.

In every possible case, we have shown that $b(\Lambda) \geq 32$, and we have also shown that this lower bound can be attained. Therefore, we conclude that $b(\Lambda) = \sqrt{32}$. □

By the above theorem, in order to create a sphere packing on Leech's lattice, we center a sphere of radius $\frac{1}{2}\sqrt{32} = 2\sqrt{2}$ on each point of the lattice. Recall that the upper bound for the contact number of a sphere packing in E^{24} is $263,285$. To show how this sphere packing compares to the theoretical upper bound, we will compute the contact number.

Theorem 6.3.4. *The contact number of* Λ *is 196,560.*

Proof. Based on [1, p. 115-116]. First note that since Λ is a lattice, the contact number of each sphere in the packing will be the same. Thus, it suffices to calculate the number of spheres that touch the sphere centered at the origin. To do this, we will count the number of points that are distance $\sqrt{32}$ from the origin. Again, since each 24-tuple in the lattice consists of either all even or all odd entries, we must consider these cases separately.

Case 1 : Let $\vec{x} = (x_1, \ldots, x_{24})$, where each x_i is even, $|\vec{x}| = \sqrt{32}$, and $\sum_{i=1}^{24} x_i^2 = 32$.

Case 1a : Eight of the $x_i = \pm 2$ and all other $x_i = 0$.

That is, eight of the $x_i \equiv 2 \bmod 4$ and sixteen of the $x_i \equiv 0 \bmod 4$. So either $m \equiv 0 \bmod 4$ and $\vec{x} \in E(m)$ where E is an octad, or $m \equiv 2 \bmod 4$ and $\vec{x} \in F(m)$ where F is the complement of an octad. Either way, the eight ± 2's will appear in coordinates which correspond to an octad. Recall that $S(5, 8, 24)$ contains 759 octads, and so momentarily ignoring the plus and minus signs, there are 759 ways of placing exactly eight 2's in $\vec{x}$. We must now distribute the plus and minus signs. Recall that $\sum_{i=1}^{24} x_i = 4m$, where m is even, which implies there must be an even number of $+2$'s, as well as an even number of -2's. To see this, let k and j denote the number $+2$'s and -2's, respectively. Then $k + j = 8$ and $2k - 2j = 4m$. So $k - j = 2m$, and adding this to $k + j = 8$ gives $2k = 2m + 8$. Thus, $k = m + 4$, which is even since m is even. But then j must be even as well. So the first seven 2's can be given either sign, and this can be done in 2^7 ways. The restriction that we have an even number of each sign fixes the 8th sign. Thus, we get $759 \cdot 2^7 = 97152$ points from this case.

Case 1b : Two of the $x_i = \pm 4$ and all other $x_i = 0$.

Therefore, all of the x_i are divisible by 4. So either $m \equiv 0 \bmod 4$ and $C = \emptyset$, or $m \equiv 2 \bmod 4$ and $C = B$, the base set. The possible sums $\sum_{i=1}^{24}$ are 0, 8, and -8. Therefore, if $C = \emptyset$ and $m \equiv 0 \bmod 4$, then $m = 0$ and $\sum_{i=1}^{24} = 0$. That is, $\vec{x}$ contains one 4 and one -4, which we can position in $24 \cdot 23 = 552$ ways. Now, if $C = B$ and $m \equiv 2 \bmod 4$, then $m = \pm 2$ and $\sum_{i=1}^{24} = 8$ or -8. That is, $\vec{x}$ contains either two 4's or two -4's, which accounts for $2 \cdot \binom{24}{2} = 552$ points. Therefore, we obtain an addition $2 \cdot 552 = 1104$ points from this case.

Note that this case excludes the possibility that $\vec{x}$ contains a mixture of 2's and 4's, for if $\vec{x}$ contains one ± 2, then $\vec{x}$ contains at least eight ± 2's. Then, if $\vec{x}$ also contains even one ± 4, $\sum_{i=1}^{24} x_i \leq 8 \cdot 2^2 + 4^2 = 32 + 16$, which further than $b(\Lambda)$ from the origin. Therefore, Case 1 has contributed $97152 + 1104 = 98256$ points with distance $\sqrt{32}$ from the origin.

Case 2 : Let $\vec{x} = (x_1, \ldots, x_{24})$, where each x_i is odd, $|\vec{x}| = \sqrt{32}$, and $\sum_{i=1}^{24} x_i^2 = 32$. Note that each $x_i > 1$. In the proof of Theorem 6.3.3, we saw that the only way to achieve $\sum i = 1^{24} x_i^2 = 32$ is if one of the coordinates of $\vec{x}$ is ± 3 and the other 23 coordinates are ± 1's. Suppose one of the coordinates is $+3$, and let n denote the number of -1's. Then there are $23 - n$ $+1$'s. Since m is odd, either $m \equiv 1 \bmod 4$ or $m \equiv 3 \bmod 4$. Let k denote the number of coordinates of $\vec{x}$ which are congruent to 1 modulo 4. Then, $k = 0, 8, 12, 16$, or 24.

$\underline{k = 0}$: Since $3 \equiv -1 \bmod 4$, there exists one $+3$ and 23 -1's. Then $\sum_{i=1}^{24} = 3 - 23 = -20 = 4m$, which implies that $m = -5$. In this case, the corresponding set C is $\emptyset$, and there are 24 positions in which to place the $+3$. Note that the remaining positions are each filled with a -1, and so we obtain 24 points from this case.

$\underline{k = 8}$: Then $23 - n = 8$, which implies that $n = 15$, and therefore $\sum_{i=1}^{24} x_i = 3 + 8 - 15 = -4 = 4m$, which implies that $m = -1$. So eight of the x_i's are $\equiv m + 2 \bmod 4$ and the corresponding set C is an octad. Since $3 \not\equiv m + 2 \bmod 4$, there are 16 positions in which to place the $+3$. We do not have a choice of where the $+1$'s and -1's appear. Since there are 759 octads, this gives us an additional $759 \cdot 16 = 12144$

points.

$\underline{k = 12}$: Then $23 - n = 12$, which implies that $n = 11$ and $m = 1$. So 12 of the x_i's are $\equiv m + 2 \bmod 4$ and the corresponding set C is a dodecad. Since $3 \not\equiv m + 2 \bmod 4$, there are 12 positions in which to place the $+3$. Since there are 2576 dodecads, this gives us an addition $2576 \cdot 12 = 30912$ points.

$\underline{k = 16}$: Then $23 - n = 16$, which implies that $n = 7$ and $m = 3$. So 16 of the x_i's are $\equiv m + 2 \bmod 4$ and the corresponding set C is the complement of an octad. Since $3 \not\equiv m + 2 \bmod 4$, there are 8 positions in which to place the $+3$. Since there are 759 complements of octads, this gives us an additional $759 \cdot 8 = 6072$ points.

$\underline{k = 24}$: Since $3 \not\equiv 1 \bmod 4$, this case is impossible.

Through these cases, we have found $24 + 12144 + 30912 + 6072 = 49152$ points with one $+3$ as a coordinate and distance $\sqrt{32}$ from the origin. However, note that the argument is almost identical if we suppose that one of the coordinates is -3. Specifically, each of the above cases will yield the same number of points, and thus we have actually found $2 \cdot 49152 = 98304$ points of distance $\sqrt{32}$ from the origin.

Combining the results of the two cases, we see that the contact number of the sphere packing on Λ is $98256 + 98304 = 196560$. □

To quote a few more statistics, we again adopt the notation of Anderson [1, p. 114] and denote $a(n)$ to be the largest known contact number of a packing in n dimensions and $d(n)$ to be the theoretical upper bound proposed by Coxeter. Consider the ratio $\frac{a(n)}{d(n)}$. For $n \leq 8$, the ratio is at least 0.82. However, for $n > 9$, the greatest ratio is obtained by the sphere packing on Leech's Lattice. This fact is absolutely astonishing and only helps to identify Steiner systems as extremely relevant and useful objects both in and beyond the field of discrete mathematics.

Appendix A

Matlab Code to Generate $S(5, 8, 24)$

The following code is written for Matlab and can be used to generate $S(5, 8, 24)$. As mentioned in Chapter 4, this code can be improved upon, but we will leave that to the curious and motivated reader.

The functionality is structured as a class in Matlab called "S5824." To create a new instance of the class, we type the following command into the command window:

```
>> s = S5824()
```

With this instance, we may view the octads as either 24-bit binary strings or as 24-tuples with entries in $\{1, \ldots, 24\}$ using the following commands:

```
>> s.octadsBin
>> s.octadsNum
```

Within the class, there is are two functions: "iso" and "octContains." A thorough description of each can be found in the comments of the code. Sample calls are provided below:

```
>> s = s.iso([1,7,7,1]);
>> s.octContains([1,2,3,4,5])
```

```
ans =

     1     2     3     4     5     8    10    19
```

Code begins here:

```
classdef S5824    %S(5,8,24) Generator

    properties
        octadsBin = []; % 2D matrix, stores the octads as 24-bit binary strings
        octadsNum = []; % 2D matrix, stores the octads as 8-tuples in {1,...,24}

        % generator matrix for G_{24}, the (24,12) Golay code
        % interchanging the rows and columns will give an equivalent system
        g24mat = [ 1,0,0,0,0,0,0,0,0,0,0,0,0,1,1,1,1,1,1,1,1,1,1,1;
                   0,1,0,0,0,0,0,0,0,0,0,0,1,1,0,1,0,0,0,1,1,1,0,1;
                   0,0,1,0,0,0,0,0,0,0,0,0,1,0,1,0,0,0,1,1,1,0,1,1;
                   0,0,0,1,0,0,0,0,0,0,0,0,1,1,0,0,0,1,1,1,0,1,1,0;
                   0,0,0,0,1,0,0,0,0,0,0,0,1,0,0,0,1,1,1,0,1,1,0,1;
                   0,0,0,0,0,1,0,0,0,0,0,0,1,0,0,1,1,1,0,1,1,0,1,0;
                   0,0,0,0,0,0,1,0,0,0,0,0,1,0,1,1,1,0,1,1,0,1,0,0;
                   0,0,0,0,0,0,0,1,0,0,0,0,1,1,1,1,0,1,1,0,1,0,0,0;
                   0,0,0,0,0,0,0,0,1,0,0,0,1,1,1,0,1,1,0,1,0,0,0,1;
                   0,0,0,0,0,0,0,0,0,1,0,0,1,1,0,1,1,0,1,0,0,0,1,1;
                   0,0,0,0,0,0,0,0,0,0,1,0,1,0,1,1,0,1,0,0,0,1,1,1;
                   0,0,0,0,0,0,0,0,0,0,0,1,1,1,1,0,1,0,0,0,1,1,1,0];

        rowSpace = [];  % 2D matrix which stores the row space of g24mat

    end %properties

    methods

        function obj = S5824()   %constructor
            % initializes the 2D matrices to contain all zeros
            obj.octadsBin = zeros(759,24);
            obj.octadsNum = zeros(759,8);
            obj.rowSpace = zeros(4096,24);
            linCombs = zeros(4096,12);
```

```
        % fills the matrix linCombs with all possible binary strings of length 12
        for i = 1:1:12
            index = (2^12) / (2^i);
            currIndex = 0;
            for k = 1:1:2^(i-1)
                for j = 1:1:index
                    linCombs(currIndex + j, i) = 0;
                    linCombs(currIndex + j + index, i) = 1;
                end
                currIndex = currIndex + 2*index;
            end
        end
        octadCount = 1;
        % uses the binary strings in linCombs to calculate the
        % row space of g24mat
        for i = 1:1:4096
            tempRow = 0;
            for j = 1:1:12
                tempRow = mod(tempRow + linCombs(i, j)*obj.g24mat(j,:), 2);
            end
            obj.rowSpace(i,:) = tempRow;
            % if we find a element of the row space with weight 8,
            % then we have found an octad
            if (sum(tempRow) == 8)
                obj.octadsBin(octadCount, :) = tempRow;
                octadCount = octadCount + 1;
            end
        end
        % converts the octads from 24-bit binary strings to 24-tuples
        % in {1,...,24}, stored in octadsNum
        for i = 1:1:759
            temp = zeros(1,8);
            octInd = 1;
            for j = 1:1:24
                if obj.octadsBin(i,j) == 1
                    temp(1,octInd) = obj.octadsBin(i,j)*j;
                    octInd = octInd + 1;
                end
            end
            obj.octadsNum(i,:) = temp;
        end
        % sorts the octads in lexicographical order
        obj.octadsNum = sortrows(obj.octadsNum, [1 2 3 4 5 6 7 8]);
    end %constructor
```

```
% creates an isomorphic S(5,8,24) system by permuting certain elements
% input: obj = instance of class
%        elems = array of elements (a_1, a_2, a_3, a_4, ..., a_{n-1}, a_n)
%                with n even and a_1 < a_3 < dots < a_{n-1}.
%                denotes the changes:
%                a_1 --> a_2, a_3 --> a_4, ..., a_{n-1} --> a_n.
% output: updated instance
% note: in command window, MUST use assignment statement to update instance.
function obj = iso(obj, elems)

    for i = 1:1:759
        % finds the indices of the elements to be changed, stored in array c
        index = zeros(length(elems),1);
        for k = 1:2:length(elems)
            c = find(obj.octadsNum(i,:) == elems(k));
            if (isempty(c) ~= 1)
                index(k) = c;
            end
        end
        % makes changes to octadsNum
        for k = 1:2:length(elems)
            if (index(k) ~= 0)
                obj.octadsNum(i,index(k)) = elems(k+1);
            end
        end
        % sorts each row after changes are made
        obj.octadsNum(i,:) = sort(obj.octadsNum(i,:));
    end
    % sorts the octads to appear in lexicographical order
    obj.octadsNum = sortrows(obj.octadsNum, [1 2 3 4 5 6 7 8]);
end %iso

% finds and returns the octads which contain certain elements
% input: obj = instance of class
%        elems = array of elements for which to search
% output: foundOcts = array of octads which contain the
%                     elements of elems
function [foundOcts] = octContains(obj, elems)

    foundOcts = [];
    for i = 1:1:759
        contains = 0;
        for j = 1:1:length(elems)
            % computes the sum of the find calls, if even one entry
            % is not found, then contains is an empty array
```

```
                    contains = contains + find(obj.octadsNum(i,:) == elems(j));
                    if (isempty(contains) == 1)
                        break;
                    end
                    if (j == length(elems))
                        foundOcts = [foundOcts; obj.octadsNum(i,:)];
                    end
                end
            end
        end %octContains

    end %methods

end %classdef
```

Bibliography

[1] Ian Anderson. *A first course in combinatorial mathematics*. Oxford University Press, 1974.

[2] Kenneth P. Bogart. *Introductory Combinatorics*. Academic Press, third edition, 2000.

[3] Ezra Brown. The Fabulous $(11, 5, 2)$ Biplane. *Mathematics Magazine*, pages 87–100, April 2004.

[4] H.S.M. Coxeter. An upper bound for the number of equal nonoverlapping spheres that can touch another of the same size. In *Proceedings of Symposia in Pure Mathematics, Volume VII*, pages 53–71. American Mathematical Society, June 13-15 1963.

[5] David S. Dummit and Richard M. Foote. *Abstract Algebra*. John Wiley & Sons, Inc., third edition, 2004.

[6] Marshall Hall, Jr. *Combinatorial Theory*. John Wiley & Sons, Inc., second edition, 1986.

[7] F.J. MacWilliams and N.J.A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland Publishing Company, 1977.

[8] Thomas M. Thompson. *From Error Correcting-Codes Through Sphere Packings to Simple Groups*. Carus Mathematical Monograph No. 21. The Mathematical Association of America, 1983.

[9] J.A. Todd. A representation of the Mathieu group M_{24} as a collineation group. *Annali Mat. pura appl.*, 1966.

[10] W.D. Wallis. *Introduction to Combinatorial Designs*. Taylor & Francis Group, LLC, second edition, 2007.