NEW GEOMETRIC LARGE SETS

by

Michael Robert Hurley

A Dissertation Submitted to the Faculty of

The Charles E. Schmidt College of Science

In Partial Fulfillment of the Requirements for the Degree of

Doctor of Philosophy

Florida Atlantic University

Boca Raton, FL

December 2016

New Geometric Large Sets

by

Michael Robert Hurley

This dissertation was prepared under the direction of the candidate's dissertation advisor, Dr. Spyros S. Magliveras, Department of Mathematical Sciences, and has been approved by the members of his supervisory committee. It was submitted to the faculty of the Charles E. Schmidt College of Science and was accepted in partial fulfillment of the requirements for the degree of Doctor of Philosophy.

SUPERVISORY COMMITTEE:

Spyros S. Magliveras, Ph.D.
Dissertation Advisor

Fred Richman, Ph.D.

Aaron Meyerowitz, Ph.D.

Robert Jajcay, Ph.D.

Rainer Steinwandt, Ph.D.

Rainer Steinwandt, Ph.D.
Chair, Department of Mathematical Sciences

Janet Blanks, Ph.D.
Interim Dean, Charles E. Schmidt College of Science

Deborah L. Floyd, Ed.D.
Dean, Graduate College

November 21, 2016
Date

ACKNOWLEDGEMENTS

I would like to thank my advisor Dr. Spyros S. Magliveras for his guidance and inspiration during my years at Florida Atlantic University. Whether it was his courses in coding theory and group theory, his attending many combinatorics and cryptography conferences with me, his knowledge and advice while writing this dissertation, or just being a friend and mentor to me, he is the reason I am where I am now as a graduate student, a researcher, and a person. His hard work, patience, and dedication in the classroom, in the writing and research process, and in the world of networking in mathematics is a standard that we should all strive to have ourselves. He changed my mind when I was a student, he changed my mathematics career, and I hope he continues to change my life as a friend and colleague for many years to come. I am proud to have been the protege of a great mind and man like Dr. Spyros S. Magliveras.

I would like to thank my advisory members of my Ph.D dissertation committee. Thanks to Dr. Rainer Steinwandt, Dr. Aaron Meyerowitz, Dr. Fred Richman, and Dr. Robert Jajcay for agreeing to go on this journey with me. Thank you to the many faculty members of Florida Atlantic University who taught the graduate courses I took, including Dr. Vincent Naudot, Dr. Warren McGovern, Dr. Paul Yiu, Dr. Tomas Schonbek, Dr. Xiao-Dong Zhang, Dr. Heinrich Niederhausen, and Dr. Koray Karabina. I would like to thank Dr. Stephen Locke, Dr. Lee Klingler, Dr. Yuan Wang, Dr. Charles Roberts, Dr. Fred Hoffman, and Dr. Maria Provost for being the leaders of the mathematics department and giving me administrative advice. I also want to thank the rest of the mathematics administrative staff of Florida Atlantic University, including Emily Cimillo, Beth

Broer, Helen Randall, and Sonia Kimbrough. I am grateful to the many coordinators of the classes I have taught and the tutoring center I have worked at over these years, and so I thank Dr. Brittanney Amento, Dr. Roger Goldwyn, Dr. Susan Moosai, Dr. Jorge Viola-Prioli, Dr. Barry Booton, Dr. Lisa Greenberg, Dr. Philip Pina, and Ms. Aibeng Radulovic.

I thank the many colleagues I have worked with over the years in one form or another, including Dr. Bal Khadka and Michael Epstein, who contributed and aided me in the programming and writing of this dissertation. I thank my friends who were always there for me during my time at Florida Atlantic University, including my office mates Brandon Langenberg, Hai Pham, Jesse Adamski, Sher Chheritri, and Oscar Lopez, my co-workers Yarema Boryshchak, Emmanuel Fleurantin, Alan Goldstein, Jorge Gonzalez, Daniel Gray, Aaron Hutchinson, Jean Joseph, Hasala Karunaratne, Shane and Janna Kepley, Durga Kutal, Alexandra Milbrand, Shaun Miller, Shifat Mithila, Maxime Murray, Binod Rimal, Angela Robinson, Steven Romanow, Andrew Thomack, Jessica Thune, Olivia Turner, Ashley Valentijn, Tareq Vurdubakis, Duval Zephirin, Andrea Schwab, Yonas Abraha, Keiko Ito, and my many colleagues who completed their program while I was completing mine.

Finally I want to thank my family and friends who were always there to support me during my many high points and low points. I am grateful to Kelley Cartwright Sapp, Kevin Sapp, and Kalen Sapp for being dear Florida friends. My parents, Paul and Pao-Lin Hurley, my siblings James, Anna, Alex, and Kathryn Hurley, my niece, Violet Hurley, I love you all more than anything in the world, and I am grateful to all of you for being in my life, especially over these years when I was away.

ABSTRACT

Author:	Michael Robert Hurley
Title:	New Geometric Large Sets
Institution:	Florida Atlantic University
Dissertation Advisor:	Dr. Spyros S. Magliveras
Degree:	Doctor of Philosophy
Year:	2016

Let V be an n-dimensional vector space over the field of q elements. By a *geometric* t-$[q^n, k, \lambda]$ design we mean a collection $\mathcal{D}$ of k-dimensional subspaces of V, called blocks, such that every t-dimensional subspace T of V appears in exactly λ blocks in $\mathcal{D}$. A *large set*, $LS\,[N]\,[t, k, q^n]$, of geometric designs is a collection of N disjoint t-$[q^n, k, \lambda]$ designs that partitions $\begin{bmatrix} V \\ k \end{bmatrix}$, the collection of k-dimensional subspaces of V. In this work we construct non-isomorphic large sets using methods based on incidence structures known as the Kramer-Mesner matrices. These structures are induced by particular group actions on the collection of subspaces of the vector space V. Subsequently, we discuss and use computational techniques for solving certain linear problems of the form $AX = B$, where A is a large integral matrix and X is a $\{0, 1\}$ solution. These techniques involve (i) lattice basis-reduction, including variants of the LLL algorithm, and (ii) linear programming. Inspiration came from the 2013 work of Braun, Kohnert, Östergard, and Wassermann, [17], who produced the first nontrivial large set of geometric designs with $t \geq 2$. Bal Khadka and Michael Epstein provided the know-how for using the LLL and linear programming algorithms that we implemented to

construct the large sets.

2000 Mathematics Subject Classification: 05B25, 05B40, 05E18.

Key words. Geometric t-designs, large sets of geometric t-designs, t-designs over $GF(q)$, parallelisms, lattice basis reduction, LLL algorithm.

To my parents, Paul and Pao-Lin Hurley, my siblings, James, Anna, Alex, and Kathryn Hurley, my niece, Violet Hurley, and in loving memory of Bettie Guertin Hurley, who heard the good news of my entrance to the FAU grad program just before she left us forever.

NEW GEOMETRIC LARGE SETS

CHAPTER 1

INTRODUCTION

This work discusses the construction, comparison, and applications of *geometric t-designs*. The terminology used for design theory has varied over the years, but the earliest discoveries were of *ordinary t-designs*, and predate Euler.

1.1 THE HISTORY OF ORDINARY DESIGNS

Some of the earliest work in design theory appears to be by Seok Jeong Choi - 1646-1715 - from Korea. Choi used orthogonal latin squares of order 9 to make magic squares, and conjectured that a pair of orthogonal latin squares of order 10 could not exist. Euler himself contributed to aspects of design theory, for example the existence/non-existence of orthogonal latin squares. He conjectured that for $n \equiv 2 \pmod 4$ a pair of orthogonal latin squares could not exist. This conjecture was disproved in 1958 by R. C. Bose and S. S. Shrikhande, [11], and E. T. Parker, [13].

Not unlike the Euclidean geometry of points and lines on a plane, where any two points determine a unique line, or the geometry of points and circles where any three points determine a circle, a t-design is a general type of geometry where t points determine exactly λ blocks.

An ordinary, simple t-(v, k, λ) design is a pair $(X, \mathcal{B})$, where X is a set of v points and $\mathcal{B}$ is a collection of k-subsets of X, called blocks, such that any t-subset of X appears in exactly λ blocks. Ordinary designs have been studied for centuries, even predating Euler's 36 officers problem in 1782. Orthogonal latin squares have been studied at least since the 13th century, and a set of $(n-1)$ mutually orthogonal

latin squares has since been proven to have a one-to-one relationship with a special type of a 2-$(n^2+n+1, n+1, 1)$ design known as a *finite projective plane*. [72]

Other kinds of ordinary designs include *Steiner systems*, that is, ordinary t-$(v, k, 1)$, with some of the more famous types being Steiner triple systems where $t = 2, k = 3$, and Steiner quadruple systems where $t = 3, k = 4$. These Steiner systems are often designated by their value of v, called their order. One of the first constructions of a t-design was in 1835, when J. Plücker found a Steiner triple system of order 9, [69], and his work continued through 1839 when he claimed that Steiner triple systems can only exist when $v \equiv 1,\ 3 \pmod 6$, [70].

More early work on constructing ordinary t-designs dates back to the 1850's, [49], in which T.P. Kirkman stated the famous schoolgirl problem [50], whose solution corresponds to finding a resolvable 2-(15,3,1) design.

E. Witt's 5-(12,6,1) and its derived designs, had the famous Matthieu group M_{12} and its stabilizers, as their automorphism groups. These designs had already been found and proven to be unique in 1908 by J. A. Barrau, [8]. In 1938 E. Witt constructed a remarkable 5-(24,8,1) design, [81, 82]. This design is connected to the famous Golay error-correcting code, and the Leech Lattice, [60]. The automorphism group of the 5-(24,8,1) is the famous sporadic simple group M_{24}, while the automorphism group of the Leach lattice is Conway's group Co_0, from which several new sporadic groups were constructed by J. H. Conway, [23].

The Steiner triple systems were the subject of Hanani and Hartman's work in the 1960's that included the result that a Steiner quadruple system of order v exists if and only if $n \equiv 2, 4 \pmod 6$, [34]. Hanani also proved that the well-known necessary conditions for the existence of a 2-$(v, 3, \lambda)$ design are sufficient for all λ, [35]. R. H. F. Denniston's work during 1969-83 involved the construction of new t-(v, k, λ) designs with prescribed automorphism groups, and the construction of

biplanes, [26, 27].

Necessary conditions for the existence of ordinary t-designs can be easily stated, however R. Wilson in 1973 wrote an interesting paper titled *The Necessary Conditions for t-Designs Are Sufficient for Something*, [80]. This important paper proved that given t, k, v, an ordinary t-(v, k, λ) design exists, perhaps with repeated blocks, if λ is sufficiently large, and the necessary conditions for the existence of a t-design are satisfied. These designs require that λ be large, higher than a lower bound we denote by $N(t, k, v)$. The better known discoveries involved constructing the more rare t-(v, k, λ) designs with small λ.

W. O. Alltop constructed entire classes of infinitely many 4-designs, [4] and 5-designs, [5], and devised methods to extend existing t-designs to $(t + 1)$-designs, [6]. Alltop's work inspired others like X. Hubaut and Tran Van Trung to construct additional infinite families of 4- and 5-designs, [42, 77].

There is extensive work on the existence of finite projective planes, too long to list here, but includes work of R. H. Bruck, H. J. Ryser, Marshall Hall, D. Hughes, O. Veblen, R. Baer, G. Fano, J. Thas, and M. Resmini.

N. Singhi's work with his advisor, S. S. Shrikhande, includes several publications on residual designs, while R. C. Bose and D. M. Mesner's work on the Bose-Mesner Algebra, as well as their and D. G. Higman's work on association schemes and coherent configurations were applied to strongly regular graphs, distance transitive graphs, and designs.

A major theorem by E. S. Kramer and D. M. Mesner in 1976 created a simple, but useful method for finding t-designs with matrices, [53]. By 1980 A. S. Hedayat and S. Kageyama had accumulated a survey for finding t-designs, [37]. D. R. Stinson, a student of R. Wilson, has been extremely active in the last 40 years in a variety of combinatorial areas, including design theory, providing innovative

solutions to many problems in computer science and cryptography.

Some famous mathematicians, like Dan R. Hughes, student of Bruck, and inventor of the Hughes non-Desarguesian projective plane, was skeptical about the existence of simple 6-designs simply because 6-transitive groups, besides $\mathcal{S}_n$ and $\mathcal{A}_n$ do not exist, [43]. However, in 1981, S. S. Magliveras and D. W. Leavitt managed to construct the first ever 6-(33,8,36) simple design, [64]. This inspired many more constructions, including those of R. Laue, A. Betten, A. Wassermann who are still active today. Subsequently, considerable and significant work in design and coding theory was undertaken by Gholamreza Khosrovshahi and his school of design theorists, including B. Tayfeh-Rezaie, Z. Eslami, S. Akbari, N. Ghareghani, E. Ghorbani, and H. R. Maimani.

In 1983, H. Hanani, A. Hartman, and E. S. Kramer were able to show that there is also a numerical upper bound on $N(t, v, k)$ where $t = 3$, and $k \leq v \leq 32$, allowing them to construct 3-designs with bounded λ for $k \leq v \leq 32$, [36].

A most significant design theory discovery however, came in 1985 when L. Teirlinck made the incredible discovery that ordinary t-designs exist for all t, [74]. Unfortunately, Teirlinck's construction involved gigantic values of λ, hence the search for more desirable (small) λ continued. Different 6-designs continued to be found, such as E. S. Kramer, D. W. Leavitt, and S. S. Magliveras' 6-(20,9,112) designs, [54], and D. Kreher and S. P. Radziszowski's 6-(14,7,4) designs, [55]. Tran Van Trung's highly innovative recursive method of constructing a family of 4- and 5-designs motivated S. S. Magliveras and T. E. Plambeck to devise new infinite families of simple 5-designs, [65].

After Teirlinck's result, for several decades, the critical unsolved problem in design theory became the question of existence of Steiner systems, t-$(v, k, 1)$ designs for $t \geq 6$. The problem remained unsolved until 2014, at which time P. Keevash announced his astounding result that t-Steiner systems exist for all t, [47].

1.2 SHORT HISTORY OF GEOMETRIC DESIGNS

However, our work is on geometric t-designs on a vector space V, which has a less extensive history. A t-$[q^n, k, \lambda]$ design on an n-dimensional vector space of order q is a collection $\mathcal{B}$ of k-dimensional subspaces, called blocks, such that any t-dimensional subspace is a subspace of exactly λ blocks. Such a design is denoted by $(V, \mathcal{B})$. Projective planes can be viewed as geometric designs, but the study of geometric designs formally began with P.J. Cameron in 1974, [19, 20], and P. Delsarte in 1976, [25], who applied their work on locally symmetric designs, association schemes, and regular semilattices to finite fields.

Brackets instead of parentheses are used as well to distinguish between ordinary and geometric t-designs, which is a notation distinction that is used repeatedly in this work. Previous authors have used non-standard terminology for geometric designs, including t-designs over a finite field, designs on vector spaces, or $\mathbb{F}_q$-analogs of ordinary t-(v, k, λ) designs. We choose to call them geometric designs due to their relations to other situations, such as geometric strongly regular graphs.

S. Thomas constructed the first infinite family of simple geometric 2-designs in 1987, [76]. New geometric designs and families of geometric designs were constructed by H. Suzuki, [73], M. Miyakawa et al., [67], and T. Itoh, [45], in the 1990's. Geometric t-designs that can allow repeated blocks were also studied and constructed in 1994 by D.K. Ray-Chaudhuri and E.J. Schram, [71]. M. Braun, A. Kerber, and R. Laue, [18], constructed the first simple geometric 3-design in 2005, and Braun et al., [15], constructed a 2-$[2^{13}, 3, 1]$ design in 2013. This was the first construction of a simple, geometric t-design with $\lambda = 1$, called a q-Steiner system.

For a time, the only known large sets of geometric designs were of $t = 1$; such a large set is called a *spread*. Many of the earliest constructions of spreads were in projective geometry, where a large set of 1-$[q^n, k, 1]$ designs, called $(k-1)$-spreads, in $PG(n-1, q)$ is called a $(k-1)$-parallelism of $PG(n-1, q)$. The existence and

construction of parallelisms were studied by A. Beutelspacher in 1974, [10], R. D. Baker in 1976, [7], F. Wettl in 1991, [79], and T. Penttila and B. Williams in 1998, [68], the latter of which was an extension of the work of G. Lunardon in 1984, [62]. In 2013, [17], M. Braun, A. Kohnert, P. Östergard, and A. Wassermann constructed the first large set of geometric 2-designs, with dimensions $LS[3][2,3,2^8]$, invariant under a Singer subgroup in $GL_8(2)$.

Further study was and is still being done on finding more geometric t-designs. This includes a preprint by A. Fazeli, S. Lovett, and A. Vardy, "*Nontrivial t-Designs over Finite Fields Exist for All t*", [29], who claim they have proved that nontrivial geometric t-designs exist for all t. This would be the analog to geometric designs of Teirlinck's famous result. However, we wish to make the following comments: (i) This is not a final accepted journal paper, so the proof is still under scrutiny. (ii) The authors claim that their proof is probabilistic and is based on a preprint paper by G. Kuperberg, S. Lovett, and R. Peled, "*Probabilistic Existence of Regular Combinatorial Structures*", [58], which is also still under review. (iii) If the proof holds, it still is a proof of existence, and the authors are aware that constructions of the objects need to be provided by efficient algorithms. In fact, they actually state:

"We note that this proof technique is purely existential: there is no known efficient algorithm which can produce t-$[q^n,k,\lambda]$ design over $\mathbb{F}_q$ for $t>3$. Hence, we pose the following as an open problem:

Problem 1.1 *Design an efficient algorithm to produce simple nontrivial t-$[q^n,k,\lambda]$ designs for $t \geq 3$.* "

1.3 DESIGN THEORY PROBLEMS

This has created more desire to find simple geometric t-designs. In this paper we construct and present 11 pairwise non-isomorphic $LS[3][2,3,2^8]$ large sets, all non-isomorphic from the large set constructed by Braun et al. For 9 of these large

sets, our computation involves our APL package *knuth* for group theoretic matters, and various LLL variants in the NTL library, augmented by certain optimization techniques. We then discuss our construction of two additional large sets found quickly using linear programming techniques and the software package GUROBI. The dissertation includes these two additional large sets. This new LP-based technique and software availability can certainly be used in the future in similar or more complex problems.

1.4 APPLICATIONS

The motivation for the recent work on geometric t-designs has stemmed from present day *coding theoretic* applications as discussed in [28], and [52]. The process of finding designs, geometric or otherwise, has other applications in other fields of study. Ordinary design theory has proven applications in optical orthogonal coding, secure transmission of messages from multiple sources, erasure codes and information dispersal, creating functions that are correlation immune, and other uses, [22].

Some of the more important applications of geometric designs include the ability to find *perfect codes*, like the Golay and Hamming codes. A perfect code C is a collection of codewords of length n from an alphabet A of q letters such that the distance d between any two codewords in the collection is at least $2e + 1$, and any word created from the alphabet A of length n has a distance of no more than e from any codeword in C. The process of sending messages in codewords in C is flawless, as it would be impossible for any codeword sent to be mistaken by errors for being something different. It has been proven that q-Steiner systems, the geometric analog to ordinary Steiner systems, yield perfect codes in $\mathbb{F}_q^n$, [1].

An application of the codes found from these geometric designs is coding for errors in random network coding, [52]. Random linear network coding is the

communication between sources in series of rounds of generating and injecting packets of information into a network, the packets being random row vectors of length N over a finite field $\mathbb{F}_q$. The packets are randomly selected and can be transmitted anywhere at random in the network, so codes that will minimize errors and be capable of erasing errors made in the packets include the codes constructed by geometric designs and large sets.

The names of the people we have mentioned in ordinary or geometric design history are listed on the following page. We first explain some important definitions and theorems of group theory, and some important design theory lemmas and procedures that we used.

Name	Name	Name
Alltop, William	Hartman, Alan	Radziszowki, Stanislaw
Baer, Reinhold	Hedayat, Abdossamad	Ray-Chaudhuri, Dwijendra
Baker, Ronald	Higman, Donald	Resmini, Ronald
Barrau, Johan	Howell, Edwin	Rosa, Alex
Beutelspacher, Albrecht	Hubaut, Xavier	Ryser, Herbert
Betten, Anton	Kageyama, Sanpei	Schram, Erin
Bose, Raj	Keevash, Peter	Schröder, Ernst
Braun, Michael	Kerber, Adelbart	Choi Seok-Jeong
Bruck, Richard	Khosrovshahi, Gholamreza	Shannon, Claude
Cameron, Peter	Kirkman, Thomas	Shrikhande, Mohan
Carmichael, Robert	Kramer, Earl	Shrikhande, Sharadchandra
Cayley, Arthur	Kreher, Donald	Singer, James
Chowla, Sarvadaman	Kuperberg, Greg	Singhi, Navin
Colbourn, Charles	Laue, Reinhard	Steiner, Jakob
Cole, Frank	Leavitt, David	Stinson, Douglas
Conway, John	Leech, John	Sylvester, James
Delsarte, Phillip	Lindener, Kurt	Tarry, Gaston
Denniston, Robin	Lovett, Shachar	Tayfeh-Rezaic, Behruz
Dinitz, Jeffrey	Magliveras, Spyros	Teirlinck, Luc
Eslami, Ziba	Maimani, Hamid Reza	Thas, Joseph
Euler, Leonhard	Mendelsohn, Nathan	Thomas, Simon
Fano, Gino	Mesner, Dale	Todd, John
Fazeli, Asad	Mitchell, John	Tonchev, Vladimir
Fisher, Ronald	Moore, Eliakim	Tran Van Trung
Ghareghani, Narges	Netto, Eugen	Vardy, Alexander
Ghorbani, Ebrahim	Paley, Raymond	Veblen, Oswald
Golay, Marcel	Parker, Ernest	Wassermann, Alfred
Hadamard, Jacques	Peled, Ron	Wettl, Ferenc
Hall, Marshall	Penttila, Tim	Williams, Blair
Hall, Philip	Petersen, Julius Peter	Wilson, Richard
Hamming, Richard	Plambeck, Thane	Witt, Ernst
Hanani, Haim	Plücker, Julius	Yates, Frank

CHAPTER 2

PRELIMINARIES

We assume the reader's familiarity and understanding of basic algebraic and combinatorial structures.

2.1 ORDINARY t-DESIGNS

Let X be a set of v elements. We denote by $\binom{X}{t}$ the collection of all t-subsets of X.

Definition 2.1.1. *An* ordinary t-(v, k, λ) design *on X is a pair $(X, \mathcal{B})$, where $\mathcal{B}$ is a multiset of k-subsets of X, called* blocks*, such that any t-subset T of X is a subset of exactly λ blocks in $\mathcal{B}$. $(V, \mathcal{B})$ is said to be* simple*, if $\mathcal{B}$ is a set; i.e., if there are no repeated blocks.*

All designs in this work are assumed to be *simple*. Any t-(v, k, λ) design is also an s-(v, k, λ_s) design for each s, $1 \leq s \leq t$, with $\lambda_s = \lambda \cdot \binom{v-s}{t-s} / \binom{k-s}{t-s}$, [56]. For $\mathcal{B} = \binom{X}{k}$, it is easy to check that $(X, \mathcal{B})$ is also a t-design, known as the *trivial* t-(v, k, λ) design, with $\lambda = \lambda_{max} := \binom{v-t}{k-t}$. Thus, we arrive at a set of necessary conditions for the existence of a t-(v, k, λ) design as follows:

Lemma 2.1.1. *For a t-(v, k, λ) design to exist, $\lambda_s = \lambda \cdot \binom{v-s}{t-s} / \binom{k-s}{t-s}$ must be an integer for $0 \leq s \leq t$.*

In particular note that the number of blocks in a t-(v, k, λ) design is $b = \lambda_0 = \lambda \binom{v}{t} / \binom{k}{t}$.

Definition 2.1.2. *Given an ordinary t-(v, k, λ) design $\mathcal{D} = (X, \mathcal{B})$, by the* complementary design *of $\mathcal{D}$ we mean the t-(v, k, λ') design formed by $(X, \binom{X}{k} - \mathcal{B})$.*

It is indeed not difficult to see that the above is a t-design. Moreover, we define another t-design related to a given t-(v, k, λ) design as follows:

Definition 2.1.3. *Given an ordinary t-(v, k, λ) design $\mathcal{D} = (X, \mathcal{B})$, the* supplementary design *$\mathcal{D}^s$ of $\mathcal{D}$ is defined by $\mathcal{D}^s = (X, \{X - B \mid B \in \mathcal{B}\})$.*

Definition 2.1.4. *Let $\mathcal{D} = (X, \mathcal{B})$ be a t-(v, k, λ) design, and let $x \in X$. Consider the collection $\mathcal{B}_x$ of $(k-1)$-subsets of X defined as follows:*

$$S \in \mathcal{B}_x \iff S = K - \{x\}, \text{where } x \in K \in \mathcal{B}$$

Then, $\mathcal{D}_x = (X - \{x\}, \mathcal{B}_x)$ is a $(t-1)$-$(v-1, k-1, \lambda)$ design, the so called derived design *of $\mathcal{D}$ with respect to x, denoted by $\mathcal{D}_x$.*

Note that the derived design with respect to x is the collection of all blocks of $\mathcal{B}$ containing x, with x deleted.

If we begin with a design $\mathcal{D} = (X, \mathcal{B})$ and a point $x \in X$, we can also consider the collection of all blocks in $\mathcal{B}$ that do not contain point x. This collection is a t-(v, k, λ^o) design called the residual design with respect to x.

By a *large set of ordinary t-designs*, denoted by $\text{LS}[N](t, k, v)$, we mean a set $\mathcal{L} = \{(X, \mathcal{B}_i)\}_{i=1}^N$ of N block-disjoint t-(v, k, λ) designs where $\{\mathcal{B}_i\}_{i=1}^N$ partitions $\binom{X}{k}$. Note that λ does not need to be listed in the parameters for the large set, since $\lambda = \lambda_{max}/N$. If the necessary conditions for the existence of a t-(v, k, λ) design, or large set, are satisfied, one may proceed to prove or disprove the existence of such a t-design or large set. Tables of parameters for which large sets of t-designs do not exist, can exist, or are known to exist, have been tabulated and documented over years of work by Laue and Wassermann as well as Laue, Magliveras, and Wassermann, [59].

2.2 GAUSSIAN BINOMIAL COEFFICIENTS

The *Gaussian binomial coefficients* $\begin{bmatrix} n \\ k \end{bmatrix}_q$ are analogous to the ordinary binomial coefficients $\binom{n}{k}$ in that they count the number of subspaces of dimension k of a vector space of dimension n over the field of q elements $\mathbb{F}_q$.

Given any natural number n and any prime power q, let

$$[n]_q = (1 + q + \cdots + q^{n-1}), \tag{2.1}$$

and in turn define,

$$[n]_q! = [1]_q[2]_q \cdots [n]_q. \tag{2.2}$$

Let $[0]_q = [0]_q! = 1$ for all q. Then, the *Gaussian Coefficient* $\begin{bmatrix} n \\ k \end{bmatrix}_q$ is defined as

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{[n]_q!}{[k]_q![n-k]_q!} \ . \tag{2.3}$$

It is an easy task to establish that $\begin{bmatrix} n \\ k \end{bmatrix}_q$ counts the total number of k-subspaces of an n-space over $\mathbb{F}_q$.

2.3 GEOMETRIC t-DESIGNS

Let V be an n-dimensional vector space over the field $\mathbb{F}_q$. If W is a subspace of V of dimension j, we say that W is a j-subspace of V. We denote the collection of j-subspaces in V by $\begin{bmatrix} V \\ j \end{bmatrix}_q$.

Definition 2.3.1. *A geometric t-$[q^n, k, \lambda]$ design is a pair $(V, \mathcal{B})$, where $\mathcal{B}$ is a multiset of k-subspaces of V, called blocks, such that every t-subspace T in $\begin{bmatrix} V \\ t \end{bmatrix}_q$ is contained in exactly λ blocks. $(V, \mathcal{B})$ is said to be* simple, if $\mathcal{B}$ is a set, i.e. if there are no repeated blocks.

Any t-$[q^n, k, \lambda]$ design is also an s-$[q^n, k, \lambda_s]$ design for every $0 \leq s \leq t$, where $\lambda_s = \lambda \begin{bmatrix} n-s \\ t-s \end{bmatrix}_q / \begin{bmatrix} k-s \\ t-s \end{bmatrix}_q$, [48]. Thus necessary conditions for a geometric $t - [q^n, k, \lambda]$ design to exist are that the λ_s be integers for all integers s such that $0 \leq s \leq t$.

The pair $\left(V, \begin{bmatrix} V \\ k \end{bmatrix}_q\right)$ is a t-$[q^n, k, \begin{bmatrix} n-t \\ k-t \end{bmatrix}_q]$ design for every $0 \leq t \leq k$, and is said to be the *trivial* design. A *large set* of t-$[q^n, k, \lambda]$ designs, denoted by LS$[N]$ $[t, k, q^n]$,

is a collection $\mathcal{L} = \{(V, \mathcal{B}_i)\}_{i=1}^{N}$ of N block-disjoint geometric t-$[q^n, k, \lambda]$ designs where $\{\mathcal{B}_i\}_{i=1}^{N}$ forms a partition of $\begin{bmatrix} V \\ k \end{bmatrix}_q$. Given any large set LS$[N]\,[t, k, q^n]$, the parameters of the geometric designs determine the value of N, namely $N = \begin{bmatrix} n-t \\ k-t \end{bmatrix}_q / \lambda$. Note that $\lambda_{max} = \begin{bmatrix} n-t \\ k-t \end{bmatrix}_q$ is a commonly used notation for geometric designs as well, and represents the parameter λ for the trivial geometric t-design. Thus far we see that there is a strong analogy between ordinary and geometric t-designs.

In practice, the field $\mathbb{F}_q$ is fixed for a particular application and we will frequently simplify notation by writing $\begin{bmatrix} n \\ s \end{bmatrix}$ instead of $\begin{bmatrix} n \\ s \end{bmatrix}_q$.

2.3.1 Geometric analogs of $\mathcal{D}_x$ and $Res_x(\mathcal{D})$

Some of the definitions used to describe ordinary t-designs and large sets from existing ordinary t-designs and large sets have analogous definitions for geometric designs. While the complement of a t-set $T \subset X$ in X can be expressed by $X - T$, the analogous complement of a t-space $T \leq V$ where V is a vector space is expressed as:

$$T^{\perp} = \{x \in V \mid (x, t) = 0 \ \ \forall t \in T\}$$

where (x, t) indicates the ordinary inner product in $\mathbb{F}_q$ between the vectors x and t.

The geometric analogue to a complementary ordinary design is thus defined as the following, ([48]) :

Definition 2.3.2. *Given a geometric* t-$[q^n, k, \lambda]$ *design* $\mathcal{D} = (V, \mathcal{B})$*, the* dual design $\mathcal{D}^{\perp}$ *is a* t-$[\ q^n,\ n-k,\ \lambda\begin{bmatrix} n-k \\ t \end{bmatrix} / \begin{bmatrix} k \\ t \end{bmatrix}\ ]$ *design defined as:*

$$\mathcal{D}^{\perp} = (V, \{B^{\perp} \mid B \in \mathcal{B}\})$$

This in particular allows us to narrow our search for geometric designs and large sets down to parameters where $k \leq n/2$, as designs and large sets with larger k would be dual geometric designs of these designs. Other analogues to ordinary designs include:

Definition 2.3.3. (Kiermaier and Laue, 2015, [48]) *Given a* t-$[q^n, k, \lambda]$ *design,* $\mathcal{D} = (V, \mathcal{B})$, *and* $U \in \begin{bmatrix} V \\ 1 \end{bmatrix}$, *the* derived design *of* $\mathcal{D}$ *with respect to* U *is a* $(t-1)$-$[q^{n-1}, k-1, \lambda]$ *design defined as:*

$$\mathcal{D}_U = (V - U \ , \ \{B - U \mid B \in \mathcal{B}, \ U \leq B\})$$

Definition 2.3.4. (Kiermaier and Laue, 2015, [48]) *Given* $\mathcal{D} = (V, \mathcal{B})$, *a* $t - [q^n, k, \lambda]$ *design, and* $H \in \begin{bmatrix} V \\ n-1 \end{bmatrix}$, *the residual design of* $\mathcal{D}$ *with respect to* H *is a* $(t-1)$-$[q^{v-1}, k, \mu]$ *design defined as:*

$$\mathrm{Res}_H(\mathcal{D}) = (H \ , \ \{B \mid B \in \mathcal{B}, \ B \leq H\})$$

where

$$\mu = \lambda \cdot \begin{bmatrix} v-k \\ 1 \end{bmatrix} / \begin{bmatrix} k-t+1 \\ 1 \end{bmatrix} = \lambda \cdot \frac{q^{v-k}-1}{q^{k-t+1}-1}$$

2.4 LINEAR TRANSFORMATIONS

Let V be a vector space of dimension n over $\mathbb{F}_q$. The *general linear group* $GL_n(q)$ is the collection of all nonsingular linear transformations of V onto itself. By choosing a particular basis of V over $\mathbb{F}_q$, we represent the elements of $GL_n(q)$ by $n \times n$ nonsingular matrices over $\mathbb{F}_q$. $GL_n(q)$ acts naturally on the elements as well as on the subspaces of V.

If $T \in GL_n(q)$, $\alpha \in \mathbb{F}_q$, and $u, v \in V$, as a linear transformation, T satisfies:

$$T(\alpha u + v) = \alpha T(u) + T(v).$$

If θ is a field automorphism of $\mathbb{F}_q$ and

$$T(\alpha u + v) = \alpha^{\theta} T(u) + T(v),$$

then T is said to be a *semilinear transformation.* We denote the multiplicative group of all semilinear transformations of V over $\mathbb{F}$ by $\Gamma L_n(q)$. Clearly $GL_n(q) \leq \Gamma L_n(q)$ and the elements $T \in \Gamma L_n(q)$ induce bijective mappings of

V onto itself. As a vector space, V is isomorphic to the additive group of the field $\mathbb{F}_{q^n}$, so we identify V with the additive group of $\mathbb{F}_{q^n}$. V now inherits the multiplication operation of $\mathbb{F}_{q^n}$, and if $a \in V^*$ the mapping:

$$\sigma_a : x \mapsto ax, \ x \in V \tag{2.4}$$

is a linear transformation of the additive group V^+, that is $\sigma_a \in GL_n(q)$. In what follows we adopt this nature of V as a field of order q^n.

$\Gamma L_n(q)$ is the semidirect product of $GL_n(q)$ with the Galois group $V/\mathbb{F}_q = \mathbb{F}_{q^n}/\mathbb{F}$. The latter is generated by the *Frobenius automorphism*, which we denote by ζ and define by: $\zeta : v \mapsto v^q$, $v \in V$. Thus,
$\Gamma L_n(q) = \langle GL_n(q), \zeta \rangle = GL_n(q) \cdot \langle \zeta \rangle$.

Now, $\zeta \in \Gamma L_n(q)$ fixes $\mathbb{F}_q$ element-wise, but acts on V by sending any $v \in \mathbb{F}_{q^n}$ to v^q, and the Frobenius subgroup $\langle \zeta \rangle = \Phi_n$ has order n. A subgroup $G \leq GL_n(q)$ acts naturally on the collection of subspaces of V by matrix multiplication.

2.5 SINGER SUBGROUPS

If we let a be a generator of the multiplicative cyclic group V^* (i.e. a primitive element of the field V), then the mapping $\sigma_a : x \mapsto ax$ as in equation (2.4) fixes $0 \in V$ and acts *regularly* on V^*, i.e. transitively, in a single orbit of length $q^n - 1$ on the non-zero vectors of V. Such an element σ_a, of order $q^n - 1$ is known as a *Singer cycle*, and the subgroup $\langle \sigma_a \rangle$ as a *Singer subgroup* in $GL_n(q)$, ([32]).

Singer subgroups of $GL_n(q)$ play an important role in our research, as they will become the prescribed groups of automorphisms of the constituent designs in the large sets of geometric designs we intend to construct. The incidence between t-subspaces and k-subspaces, represented by an appropriate incidence matrix, is fused by the action of a Singer subgroup on V to produce the so called *Kramer-Mesner matrix* $A_{t,k}$ corresponding to this action. Finding constituent

designs then becomes a problem of solving, possibly hard, integer linear equations of the form $A_{t,k}X = \lambda J$, where X is a vector with entries in $\{0, 1\}$, and J is the all-ones column vector.

2.6 AUTOMORPHISMS OF GEOMETRIC t-DESIGNS

Let $\mathcal{B}$ and $\mathcal{B}'$ be the collections of blocks of two distinct geometric t-$[q^n, k, \lambda]$ designs, on the vectors of $V = \mathbb{F}_q^n$. We say that $\mathcal{B}$ is *isomorphic* to $\mathcal{B}'$ if there exists $g \in GL_n(q)$ such that $\mathcal{B}^g = \mathcal{B}'$. This means that $B^g \in \mathcal{B}'$ for each $B \in \mathcal{B}$. Such an element g is called an *isomorphism* from $\mathcal{B}$ to $\mathcal{B}'$. An isomorphism g from $\mathcal{B}$ onto itself is called an *automorphism* of $\mathcal{B}$. The collection of all automorphisms of $\mathcal{B}$ is a group under composition of functions, called the automorphism group of $\mathcal{B}$, denoted by $Aut(V, \mathcal{B})$.

If V is a vector space of dimension n over $\mathbb{F}_q$ and $G \leq GL_n(q)$ then G acts on V in a natural way. For $0 \leq s \leq n$, this action induces an action of G on $\begin{bmatrix} V \\ s \end{bmatrix}$. Let $\mathcal{L} = \{\mathcal{B}_i\}_{i=1}^N$ be a large set of $t - [q^n, k, \lambda]$ designs. An element $g \in GL_n(q)$ such that $\mathcal{B}_i^g \in \{\mathcal{B}_i\}_{i=1}^N$ for $1 \leq i \leq N$ is called an *automorphism* of $\mathcal{L}$. The collection of all automorphisms of $\mathcal{L}$ is a group denoted by $Aut(\mathcal{L})$. If $G \leq Aut(\mathcal{L})$ then we say that $\mathcal{L}$ is G-*invariant*, moreover if for all $g \in G$, $\mathcal{B}_i^g = \mathcal{B}_i$ then $\mathcal{L}$ is said to be $[G]$-*invariant*. In 1976 E.S. Kramer and D.M. Mesner, articulated a simple, but powerful theorem which provides necessary and sufficient conditions for the existence of an *ordinary* G-invariant t-(v, k, λ) design, [53]. We describe an analogous theorem for the existence of $[G]$-invariant t-$[q^n, k, \lambda]$ designs. The theorem of Kramer and Mesner summarizes knowledge by many authors, [12], [39], [40], [63], [80], [51], [41], [53]. For example, the Kramer-Mesner matrices are essentially the Wilson matrices, [80], fused under the action of the prescribed automorphism group. Interestingly, the ideas of these incidence matrices go at least as far back as E.T. Moore, [54].

2.7 GROUP ACTIONS

A group action $G|X$ is a triple $(X, G, \exp)$ where X is a set, G is a group, and exp is a mapping

$$\begin{aligned} \exp: \quad & X \times G \to X \\ & (x, g) \to x^g \end{aligned}$$

satisfying the following two axioms:

(i) $(\alpha^g)^h = \alpha^{gh}$ for all $\alpha \in X,\ g, h \in G$

(ii) $\alpha^1 = \alpha$ for all $\alpha \in X$, where 1 is the identity of G.

We define a relation "$\sim$" on X by: $a \sim b$ if and only if there exists some $g \in G$ such that $a^g = b$. It easily follows that "$\sim$" is an equivalence relation on X. The $\sim$-equivalence classes are called the *G-orbits* of X. If $S \subset X$ and $H \subset G$ we write S^H for $\{x \mid x = s^h, s \in S, h \in H\}$. In turn we simplify $\{x\}^H$ to x^H for any $x \in X$, and any $H \subset G$. Similarly, for any $S \subset X$ and $g \in G$, we write S^g for $S^{\{g\}}$. Thus, for any $x \in X$, x^G is the G-orbit that contains x.

For any $x \in X$, the *stabilizer* of x in G, G_x, is defined by:

$$G_x = \{g \in G \mid x^g = x\}$$

It is easily shown that $G_x \leq G$ for every $x \in X$. We define the *kernel* K of a group action by:

$$K = \bigcap_{x \in X} G_x$$

It is easy to see that K is a normal subgroup of G. If the kernel of $G|X$ is $\{1\}$, then the group action $G|X$ is called *faithful*. The following lemmas and corollaries are well known:

Lemma 2.7.1. *Let $G|X$ be a group action, then $G_{x^g} = (G_x)^g$.*

Corollary 2.7.1. *If $\beta \in \alpha^G$, then G_α and G_β are isomorphic, and thus $|G_\alpha| = |G_\beta|$.*

Lemma 2.7.2. *Let $G|X$ be a group action, then the size of an orbit is the index of the stabilizer in G:*

$$|\alpha^G| \ = \ [G : G_\alpha]$$

For $g \in G$, we define *Fix(g)* by: $Fix(g) = \{\alpha \in X \mid \alpha^g = \alpha\}$. The following lemma is erroneously credited to W. Burnside:

Lemma 2.7.3. (Cauchy-Frobenius Lemma, [54]) *For a given group action, $G|X$,*

$$[number\ of\ G\text{-}orbits\ on\ X] = \frac{1}{|G|}\sum_{g\in G}|Fix(g)|$$

. A *Sylow p-subgroup* of a group G is a subgroup of order p^n where p^n divides $|G|$ exactly. We assume familiarity of the reader with the properties and theorems of Sylow p-subgroups.

Definition 2.7.1. *The* centralizer, *$C_G(H)$ of $H \leq G$ is the set of elements*

$\{x \in G \mid h^x = h, \ \forall h \in H\}$. *The* normalizer, *$N_G(H)$ is the set*
$\{x \in G \mid H^x = H\}$.

Proposition 2.7.1. *Suppose that $H \leq G$, and $x \in G$, then:*

(i) *$H \trianglelefteq N_G(H)$, and $C_G(H) \ \trianglelefteq \ N_G(H)$,*

(ii) *$C_G(H^x) \ = \ (C_G(H))^x$, and $N_G(H^x) \ = \ (N_G(H))^x$,*

(iii) *$N_G(H)/C_G(H) \cong Q \leq Aut(H)$.*

CHAPTER 3

INCIDENCE AND FUSION

3.1 DEFINITIONS

Let $G \leq \Gamma L_n(q)$ and V an n-dimensional vector space over $\mathbb{F}_q$. For each integer $s,\ 0 \leq s \leq n,\ G$ acts on $\begin{bmatrix} V \\ s \end{bmatrix}$. For $0 \leq t < k \leq n$, the action of G partitions $\begin{bmatrix} V \\ t \end{bmatrix}$ and $\begin{bmatrix} V \\ k \end{bmatrix}$ into orbits as follows:

$$\begin{bmatrix} V \\ t \end{bmatrix} = \Delta_1 + \Delta_2 + \ldots + \Delta_{\rho(t)}$$

$$\begin{bmatrix} V \\ k \end{bmatrix} = \Gamma_1 + \Gamma_2 + \ldots + \Gamma_{\rho(k)}$$

where $\rho(s)$ denotes the number of G-orbits on $\begin{bmatrix} V \\ s \end{bmatrix}$. The *Kramer-Mesner matrix* $A_{t,k}$ is defined as the $\rho(t) \times \rho(k)$ matrix $A_{t,k} = (a_{t,k}(i,j))$ with

$$a_{t,k}(i,j) = |\{K \in \Gamma_j : T \leq K \ , \text{ for fixed } T \in \Delta_i\}|$$

where T is any fixed t-subspace in the orbit Δ_i. The value of $a_{t,k}(i,j)$ is independent of the choice of $T \in \Delta_i$, [53] .

In other words, the matrix entries indicate the number of k-subspaces $K \in \Gamma_j$ which contain a fixed t-subspace $T \in \Delta_i$, and this number is constant regardless of what $T \in \Delta_i$ is chosen. A dual Kramer-Mesner matrix $B_{t,k}$ can also be defined by

$B_{t,k} = (b_{t,k}(i,j))$, with :

$$b_{t,k}(i,j) = |\{T \in \Delta_i : T \leq K\}|$$

where $K \in \Gamma_j$ is any fixed k-subspace. Once again, the value of $b_{t,k}(i,j)$ is independent of the choice of $K \in \Gamma_j$. We can define *vectors of orbit lengths* as

$L_t = (|\Delta_1|, |\Delta_2|, \ldots, |\Delta_{\rho(t)}|)$ and $L_k = (|\Gamma_1|, |\Gamma_2|, \ldots, |\Gamma_{\rho(k)}|)$.

Finally, a third matrix $C_{t,k}$ is defined from the group action $G|V$. Given a fixed $K \in \Gamma_i$, let $c_{i,j}$ be the number of blocks in Γ_j that intersect K in t-dimensional subspaces. That is, $C_{t,k}$ is a $\rho(k) \times \rho(k)$ matrix such that $C_{t,k} = (c_{i,j})$, with

$$c_{ij} = |\{K' \in \Gamma_j \ : \ \dim(K \cap K') = t\}|,$$

where K is a fixed k-subspace in Γ_i. An action $G|V$, where $V = AG_n(q) = \mathbb{F}_q^n$, induces in a natural way an action $G|PG_{n-1}(q)$, thus the matrices discussed above provide necessary and sufficient conditions for the existence of *projective* G-invariant t-$[q^n, k, \lambda]$ designs as well. We have defined these matrices in the context of geometric t-designs, and we will state the analog of the Kramer-Mesner theorem.

3.2 PROPERTIES

The geometric analogs of the properties of the $A_{t,k}$, $B_{t,k}$, $C_{t,k}$, as they were defined above, satisfy the following lemma, which is analogous to the ordinary t-design case in [54]:

Lemma 3.2.1. (i) *If* $t \leq s \leq k \leq n$, *then* $\begin{bmatrix} k-t \\ k-s \end{bmatrix} A_{t,k} = A_{t,s} \cdot A_{s,k}$,

(ii) $A_{t,k}$ *has constant row sums* $\begin{bmatrix} n-t \\ k-t \end{bmatrix}$,

(iii) $|\Delta_i| \cdot A_{t,k}(i,j) = |\Gamma_j| \cdot B_{t,k}(i,j)$,

(iv) $\begin{bmatrix} k \\ t \end{bmatrix} L_k = L_t A_{t,k}$,

(v) $C_{t,k} = B_{t,k}^T A_{t,k} - \sum_{i=t+1}^{k} \begin{bmatrix} i \\ t \end{bmatrix} C_{i,k}$

Proof. (i) Given $G|V$, let the following represent the orbit decomposition in the action of G on $\begin{bmatrix} V \\ t \end{bmatrix}$, $\begin{bmatrix} V \\ s \end{bmatrix}$, $\begin{bmatrix} V \\ k \end{bmatrix}$, respectively, where $t \leq s \leq k$:

$$\begin{bmatrix} V \\ t \end{bmatrix} = \Delta_1 + \Delta_2 + \ldots + \Delta_{\rho(t)}$$

$$\begin{bmatrix} V \\ s \end{bmatrix} = \Psi_1 + \Psi_2 + \ldots + \Psi_{\rho(s)}$$

$$\begin{bmatrix} V \\ k \end{bmatrix} = \Gamma_1 + \Gamma_2 + \ldots + \Gamma_{\rho(k)}$$

Suppose T is a fixed member of the orbit Δ_i, and we want the total number of $K \in \Gamma_j$ where $T \subset K$. There exists $a_{t,s}(i,l)$ incidences of T in any $S \in \Psi_l$, for $1 \leq l \leq \rho(s)$. For any given $S \in \Psi_l$ there in turn exists $a_{s,k}(l,j)$ incidences of S in any $K \in \Gamma_j$. Therefore the product $a_{t,s}(i,l) \cdot a_{s,k}(l,j)$ is the number of $K \in \Gamma_j$ containing T via the orbit Ψ_l. The sum $\sum_{l=1}^{\rho(s)} a_{t,s}(i,l) \cdot a_{s,k}(l,j)$ counts the total number of $K \in \Gamma_j$ containing T via any s-space orbit. This sum is the inner product of the ith row of $A_{t,s}$ and the jth column of $A_{s,k}$. However, given T and K where $T \subset K$, there are $\begin{bmatrix} k-t \\ k-s \end{bmatrix}$ different $S \subset K$ that contain T. Counting $K \in \Gamma_j$ that contain a fixed T via s-space orbits will count by factors of the number of $\begin{bmatrix} k-t \\ k-s \end{bmatrix}$ since each $K \in \Gamma_j$ containing T will count an incidence of $T \subset K$ for every $S \subset K$ containing T. Therefore, the product $A_{t,s} \cdot A_{s,k}$ is $A_{t,k}$ multiplied by a factor of $\begin{bmatrix} k-t \\ k-s \end{bmatrix}$.

(ii) The row sums of $A_{t,k}$ is the total number of ways any t-subspace T can be extended to a k-subspace in $\begin{bmatrix} V \\ k \end{bmatrix}$. This is of course $\begin{bmatrix} n-t \\ k-t \end{bmatrix}$, independent of $T \in \begin{bmatrix} V \\ t \end{bmatrix}$.

(iii) $B_{t,k}(i,j)$ represents the number of $T \in \Delta_i$ in any fixed $K \in \Gamma_j$, so $B_{t,k}(i,j) \cdot |\Gamma_j|$ counts all t-subspaces in Δ_i in blocks of Γ_j. $A_{t,k}(i,j)$ represents the number of $K \in \Gamma_j$ containing any fixed $T \in \Delta_i$, so $|\Delta_i| \cdot A_{t,k}(i,j)$ counts the number of times a t-subspace in Δ_i is contained in a block of Γ_j. These two products are equal.

(iv) The row vector $L_t A_{t,k}$ counts the number of t-subspaces in each Δ_i within each Γ_j, which is also the number of t-subspaces (not necessarily unique) contained in each Γ_j orbit. This is also the number of t-subspaces found in each k-subspace in the orbit, that is, $\begin{bmatrix} k \\ t \end{bmatrix}$ times the number of k-subspaces in the orbit,

which is the length of Γ_j.

(v) The (i,j)th entry of $B_{t,k}^T A_{t,k}$ is an inner product of the ith column of $B_{t,k}$ and the jth column of $A_{t,k}$. Any nonzero term in this inner product will be the result of any $b_{t,k}(s,i) \cdot a_{t,k}(s,j)$ where both factors are nonzero, implying there is a fixed $K \in \Gamma_i$ containing $b_{t,k}(s,i)$ different $T \in \Delta_s$, and there is a fixed $T' \in \Delta_s$ contained in $a_{t,k}(s,j)$ different $K' \in \Gamma_j$. The factors do not change in value regardless of what $K \in \Gamma_j$ or $T' \in \Delta_s$ is fixed, therefore $b_{t,k}(s,i) \cdot a_{t,k}(s,j)$ is the total number of $T \in \Delta_s$ contained in both a fixed $K \in \Gamma_i$ and any $K' \in \Gamma_j$. The inner product of the two columns is the total number of $T \in \begin{bmatrix} V \\ t \end{bmatrix}$ contained in both a fixed $K \in \Gamma_i$ and any $K' \in \Gamma_j$, implying that every instance of $T \subset K \cap K'$ has K and K' sharing a subspace of at least dimension t. However, $\sum_{i=t+1}^{k} \begin{bmatrix} i \\ t \end{bmatrix} C_{i,k}$ counts up the total number of times that a fixed $K \in \Gamma_i$ and any $K' \in \Gamma_j$ share a subspace of dimension greater than t and up to k. □

3.3 THE KRAMER-MESNER THEOREM

Suppose that $G|X$ is a group action and that $A_{t,k}$ is the Kramer-Mesner matrix formed as in the definition. Then, the following theorem holds, presented by Kramer and Mesner in [53], and reformulated in [54].

Theorem 3.3.1. (Kramer and Mesner, 1976, [54]) *Given a group action of group G on a v-set V, there is a G-invariant simple t-(v,k,λ) design if and only if there is a $\rho(k) \times 1$ $\{0,1\}$ vector u which is a solution of the matrix equation*

$$A_{t,k}\, u = \lambda J \tag{3.1}$$

where J is the $\rho(t) \times 1$ vector of all 1's.

Lemma (3.2.1) allows us to extend the Kramer-Mesner theorem to geometric t-designs:

Theorem 3.3.2. *Let V be a vector space of dimension n over the field $\mathbb{F}_q$, and let $G \leq \Gamma L_n(q)$ act on V. Then, there is a G-invariant, simple, t-$[q^n, k, \lambda]$ design if and only if there is a $\rho(k) \times 1$ $\{0,1\}$ vector u which is a solution of the matrix equation*

$$A_{t,k}\, u = \lambda J \tag{3.2}$$

where J is the $\rho(t) \times 1$ vector of all 1's.

The 1's in the vector u select the G-orbits of $\begin{bmatrix} V \\ k \end{bmatrix}$ whose union will constitute the design. Next, we present the analog of a corollary by Cusack and Magliveras, as it applies to geometric t-designs:

Corollary 3.3.1. (Cusack, Magliveras, 1999, [24]) *There is an $LS[N][t, k, q^n]$ large set of G-invariant geometric designs if and only if there exist N distinct $\{0,1\}$ vector solutions $u_1, u_2, \ldots, u_N$, to the matrix equation $A_{t,k}\, u = \lambda J$, whose sum is the $\rho(k) \times 1$ all 1's vector.*

The problem of choosing columns of $A_{t,k}$ whose sum is the vector λJ is generally intractable, known as a *multidimensional knapsack problem* (MKP), [14]. Finding even a single solution has exponential complexity. We are mainly interested in the question of existence of solutions, with secondary priority being to find several distinct, or even non-isomorphic solutions. We consider two rather unrelated methods for finding designs and large sets in the above setting.

The first method is the primary topic of this dissertation, and involves creating designs and large sets from their automorphism groups, resulting in a finite number of designs and large sets that share elements within their automorphism groups. The second family of methods involves *recursive constructions* that create designs and large sets from appropriate recursive step(s) which create new designs/large sets by a composition of smaller designs/large sets, already known to exist. These techniques are based on *extensions* satisfying certain combinatorial conditions. The recursive construction methods usually result in infinite families of

designs and large sets, but can only work if *starter designs/large sets* have already been constructed by other methods. Our research has focused on the first method, creating new designs and large sets with a *prescribed group of automorphisms*. These can possibly serve as the starting designs/large sets for recursive constructions.

CHAPTER 4

RECURSIVE CONSTRUCTIONS

Finding processes for constructing designs and large sets from pre-existing designs has been a topic of study that has lead to several documented and well-known theorems for constructing new ordinary designs and large sets from known ones. This in turn allows for possibilities in determining more sets of parameters that can feasibly serve as parameters of designs and large sets. Some constructions can apply to designs and large sets that are geometric, or ordinary, such as the following designs formed from existing designs.

The following theorem is almost trivial, but provides an easy way to find large sets from a pre-existing one.

Theorem 4.0.3. *If there exists an $LS[M](t,k,v)$ and $N|M$, then there exists an $LS[N](t,k,v)$.*

Proof. Suppose that a large sets $\mathcal{L}$ on X exists with t-(v,k,λ) designs $\{B_i\}_{i=1}^{M}$. Let $r = M/N$ and consider any regular partition of the set $\{1,2,\ldots,M\}$ into N blocks each of size r. For each block of the partition, take the union of the designs $\mathcal{B}_i$ with indices in that block, thus forming N new designs, one for each partition block, resulting in N t-$(v,k,r\lambda)$ designs. □

While expressed in the notation of ordinary large sets, the previous theorem clearly applies to geometric large sets and designs. This is because the number of constituent designs and λ are the only parameters required to change from one large set and design to another. However, many of the following definitions, theorems, and recursive constructions are done by removing or adding elements to the v-set X

in the ordinary case of designs and large sets. As a result, analogous theorems for geometric large sets are not as obvious to determine or express.

4.1 ORDINARY RECURSIVE CONSTRUCTIONS

There are several well-known methods for constructing ordinary designs from pre-existing ones. For example, a new design $\mathcal{D}$ can be formed by allowing an existing design $\mathcal{C} \cong \mathcal{D}_x$ or $\mathcal{C} \cong Res_x(\mathcal{D})$, for some new element $x \notin X$.

If a given ordinary t-(v, k, λ) design $\mathcal{C}$ is isomorphic to $\mathcal{D}_x$, or $Res_x(\mathcal{D})$, then $\mathcal{D}$ is called an *extension* of $\mathcal{C}$.

This leads to a recursive method to find ordinary extensions of existing designs.

Theorem 4.1.1. (Alltop, 1975, [6]) *Given an ordinary* t-$(2k+1, k, \lambda)$ *design* $(X, \mathcal{B})$, *and* ∞ *a new point not in* X. *Define three collections of* $(k+1)$-*sets:*

$$\mathcal{B}' \;=\; \{B \cup \{\infty\} \;:\; B \in \mathcal{B}\}$$

$$\mathcal{B}'' \;=\; \{X - B \;:\; B \in \mathcal{B}\}$$

$$\mathcal{B}''' \;=\; \{X - B \;:\; B \in \binom{V}{k} - \mathcal{B}\}$$

1. *If* t *is even, then* $(X \cup \{\infty\}\ ,\ \mathcal{B}' \cup \mathcal{B}'')$ *is a* $(t+1)$-$(2k+2,\ k+1, \lambda)$ *design,*

2. *If* $(X, \mathcal{B})$ *is simple,* t *odd, and* $\lambda = \lambda_{max}/2$, *then* $(X \cup \{\infty\},\ \mathcal{B}' \cup \mathcal{B}''')$ *is a* $(t+1) - (2k+2, k+1, \lambda)$ *design.*

Some of the more well-known recursive constructions of ordinary large sets include the following:

Theorem 4.1.2. (Chee and Magliveras, 1998, [21]) *If there exist* $LS[M](t, k, v)$ *and* $LS[N](t, k+1, v)$, *then a* $LS[gcd(M, N)](t, k+1, v+1)$ *exists.*

Theorem 4.1.3. (Teirlinck, (1989), [75]) *For every natural number t, let* $\lambda(t) = \text{lcm}\{\binom{t}{m} : m = 1, \ldots, t\}$, $\lambda^*(t) = \text{lcm}\{1, 2, \ldots, t+1\}$, *and* $\ell(t) = \prod_{i=1}^{t} \lambda(i)\lambda^*(i)$. *Then, for all $N > 0$, there is an $LS[N](t, t+1, t+N\ell(t))$.*

Theorem 4.1.4. (Khosrovshahi, Ajoodani-Namini, (1991), [2]) *If there are $LS[N](t, t+1, v)$ and $LS[N](t, t+1, w)$, then, there is also an $LS[N](t, t+1, v+w-t)$.*

Theorem 4.1.5. (Qiu-rong Wu, (1991), [83]) *If there exist large sets $LS[N](t, k, v)$, $LS[N](t, k, w)$, $LS[N](k-2, k-1, v-1)$, $LS[N](k-2, k-1, w-1)$, then there exists a large set $LS[N](t, k, v+w-k+1)$.*

Corollary 4.1.1. (Qiu-rong Wu, (1991), [83]) *If there exist large sets $LS[N](t, k, v)$, and $LS[N](k-2, k-1, v-1)$, then there exists a large set $LS[N](t, k, v+m(v-k+1))$ for all $m \geq 0$.*

An interesting and powerful construction by Ajoodani-Namini, [3] produces a new large set of $(t+1)$-designs, from a large set of t-designs.

Theorem 4.1.6. (Ajoodani-Namini, (1996), [3]) *If there exists an $LS[N](t, m, v-1)$, and $mN < k < (m+1)N$, then an $LS[N](t+1, k, Nv)$ also exists.*

4.2 GEOMETRIC RECURSIVE CONSTRUCTIONS

Unfortunately, the frontiers of knowledge in recursive constructions are not extensive in the area of geometric t-designs and large sets. Thus, only a couple of the recursive constructions for ordinary designs and large sets carry over to their geometric analogs. In particular, these are theorems (4.0.3) and (4.1.2), and their proofs are straight forward. It is of considerable interest to try to state and prove analogs of theorems (4.1.3), (4.1.4), (4.1.5), and (4.1.6), as well as corollary (4.1.1).

We invite the reader to make progress in this direction.

However, we state here some recent results due to Kiermaier and Laue related to ordinary derived and residual designs, which may be used as partial machinery to recursively construct large sets of geometric designs in the future.

Proposition 4.2.1. (Kiermaier and Laue, 2015, [48]) *If there exists a geometric* $LS[N][t, k, q^n]$ *large set* $\mathcal{L}$ *with* $t \geq 1$*, then there also exists an* $LS[N][t-1, k-1, q^{n-1}]$ *large set, and an* $LS[N][t-1, k, q^{n-1}]$ *large set.*

Proof. Given the large set $\mathcal{L}$ defined on vector space V, fix a 1-dimensional subspace U, and form derived designs on V/U from $\mathcal{L}$. This forms the $LS[N][t-1, k-1, q^{n-1}]$ large set. Fix $H \in \begin{bmatrix} V \\ n-1 \end{bmatrix}$ and form residual designs from $\mathcal{L}$, and this forms the $LS[N][t-1, k, q^{n-1}]$ large set. □

Corollary 4.2.1. (Kiermaier and Laue, 2015, [48]) *If there exists a geometric* $LS[N][t, k-1, q^{n-1}]$ *and* $LS[N][t, k, q^{n-1}]$ *large set, then there exists an* $LS[N][t, k, q^n]$ *large set.*

Recursive construction requires known existing large sets and designs however. Thus, the work in being able to construct large sets and designs using automorphism groups is an equally important branch of study in design theory, and is our primary method of finding geometric large sets in this work. In particular, we have used two methods to create a number of non-isomorphic $LS[3][2, 3, 2^8]$ large sets.

CHAPTER 5

SOLVING MULTIDIMENSIONAL KNAPSACKS

5.1 LATTICE BASIS REDUCTION METHOD

Our first method of finding solutions was the method used in [17], and it is based on *lattice basis reduction*. In order to find a solution u that would solve the matrix equation (3.1), we create an *integral lattice basis* from our matrix $A_{t,k}$. A lattice in $\mathbb{R}^n$ is a discrete additive subgroup of $\mathbb{R}^n$. Given a collection of linearly independent vectors $B = \{b_1, b_2, \ldots, b_m\} \subset \mathbb{R}^n$, the lattice $\mathcal{L} = \mathcal{L}(B)$, spanned by B, is the set of all vectors v of the form

$$v = \sum_{i=1}^{m} x_i b_i, \qquad x_i \in \mathbb{Z}$$

B is said to be a *basis* for $\mathcal{L}$. A lattice $\mathcal{L}$ has infinitely many bases, and if B and B' are any two bases of $\mathcal{L}$, there exists an integral unimodular matrix U such that $B' = UB$. Critical problems in the theory of integral lattices are i) find a shortest nonzero vector in $\mathcal{L}$, ii) find a "short enough" vector, iii) find a basis consisting of relatively short vectors. Typically one approaches any of these problems by finding a short basis for the lattice, a basis B containing short vectors that are nearly orthogonal, i.e. have inner products close to 0. The problem is generally intractable. However, there exists a polynomial time algorithm (LLL, by A.K. Lenstra, H.W. Lenstra Jr., L. Lovácz, [61]) and several variations which can succeed in solving the above problems in certain types of lattices. A programming language APL, [46, 31] was used to create $A_{t,k}$ and run a program that uses a variation of LLL. This program helped us find our first collection of $LS[3][2, 3, 2^8]$ large sets.

5.1.1 The matrix equations

Many problems in combinatorial mathematics involve having to solve an integral matrix equation of the form

$$AX = B \tag{5.1}$$

where A is integral, and X and B are both a single column vector, with X is a $\{0, 1\}$ vector. This matrix equation and the equations that follow can have more general dimensions for A, X, B, but our research focused primarily on examples where X, B both have a single column. Typically A can have a very large number of rows and columns. It is clear that the above matrix equation is equivalent to the matrix equation seen below. Let I_n be the order n identity matrix, A be a matrix of dimension $m \times n$, B be a $m \times 1$ vector, X be a $n \times 1$ column vector, and $\vec{0}_i$ be the $i \times 1$ column vector of 0's.

$$\begin{bmatrix} I_n & \vec{0}_n \\ A & -B \end{bmatrix} \begin{bmatrix} X \\ 1 \end{bmatrix} = \begin{bmatrix} X \\ \vec{0}_m \end{bmatrix} \tag{5.2}$$

In this equation we have a product of a $(n + m) \times (n + 1)$ matrix with an $(n + 1) \times 1$ vector, resulting in an $(n + m) \times 1$ vector.

The $\{0, 1\}$ column vector X solves equation (5.1) if and only if it satisfies (5.2). The matrix multiplication in this equation can be broken up into two operations, multiplying the $(n + 1) \times 1$ vector with either the first n rows of the matrix or the last m rows of the matrix. The first operation found by multiplying the first n rows of the matrix $[I_n \ \ \vec{0}_n]$ with the vector $\left[\begin{smallmatrix} X \\ 1 \end{smallmatrix}\right]$ will give us $X + \vec{0}_n = X$. The second operation found by multiplying the last m rows of the matrix $([A \ \ -B])$ with the vector $\left[\begin{smallmatrix} X \\ 1 \end{smallmatrix}\right]$ will give us $AX - B$. Thus if X satisfies (5.2) then $AX - B = 0$, and so X is a solution to (5.1).

Since the vector $\left[\begin{smallmatrix} X \\ \vec{0}_m \end{smallmatrix}\right]$ on the right hand side of (5.2) is an integral linear combination of the columns of the matrix $\left[\begin{smallmatrix} I & 0 \\ A & -B \end{smallmatrix}\right]$, $\left[\begin{smallmatrix} X \\ 0 \end{smallmatrix}\right]$ belongs to the lattice

spanned by the columns of $\left[\begin{smallmatrix} I & 0 \\ A & -B \end{smallmatrix}\right]$, and it is a very short vector of the lattice. Thus a strategy for finding solutions X to very large matrix equation problems is to find short vectors in the corresponding lattice.

5.1.2 The lattice matrix

Our lattice $\mathcal{L}$ is formed by adjoining the identity matrix I of order $\rho(k)$ above the Kramer-Mesner matrix. To the right of this new matrix we adjoin a column vector which has zeros in the first $\rho(k)$ positions and $-\lambda$ in the remaining positions. This $(\rho(t)+\rho(k)) \times (\rho(k)+1)$ matrix we call M has rank $\rho(k)+1$, so the set of integer linear combinations of the columns of M form a lattice $\mathcal{L}$ in $\mathbb{R}^{\rho(t)+\rho(k)}$.

$$M = \begin{bmatrix} I_{\rho(k)} & \vec{0}_{\rho(k)} \\ A_{t,k} & -\lambda J \end{bmatrix}$$

Lemma 5.1.1. *Suppose that* $x = (x_1, x_2, \ldots, x_{\rho(k)+1}) \in \mathbb{Z}^{\rho(k)+1}$ *with* $x_i \in \{0,1\}$ *for* $1 \leq i \leq \rho(k)$, *and* $x_{\rho(k)+1} = 1$ *such that*

$$Mx^T = (u_1, \ldots, u_{\rho(k)+\rho(t)})^T$$

where $u_i \in \{0,1\}$ *for* $1 \leq i \leq \rho(k)$, *and* $u_i = 0$ *for* $i > \rho(k)$. *Then* $u = (u_1, \ldots, u_{\rho(k)+\rho(t)})$ *is a very short vector in* $\mathcal{L}$ *spanned by the columns of* M.

Corollary 5.1.1. *If lattice-basis reduction of* $\mathcal{L}$ *yields a short vector of the form*

$$u = (u_1, \ldots, u_{\rho(k)}, u_{\rho(k)+1}, \ldots, u_{\rho(k)+\rho(t)})$$

where $u_i \in \{0,1\}$ *for* $1 \leq i \leq \rho(k)$ *and* $u_i = 0$ *for* $i > \rho(k)$, *then there exists a vector* $x = (x_1, \ldots, x_{\rho(k)+1})$ *such that* $x_i \in \{0,1\}$ *for* $1 \leq i \leq \rho(k)$ *and* $x_{\rho(k)+1}$ *is an integer.*

Remark 5.1.1. *If lattice basis reduction of* $\mathcal{L}$ *yields a short vector* u *where the first* $\rho(k)$ *entries of* u *are in* $\{0,-1\}$, *then* $-u \in \mathcal{L}$ *and its first* $\rho(k)$ *entries are in* $\{0,1\}$.

We use lattice basis reduction on M in the hopes of finding a vector $u \in \mathcal{L}$ of the form in corollary (5.1.1) whose nonzero entries select the columns of $A_{t,k}$ to provide a solution to (3.1). The first $\rho(k)$ entries of any vector u of the form in corollary (5.1.1) will be a solution to $A_{t,k}u = d\lambda J$, [57] for some integer d, hopefully d equals 1.

The program that uses lattice basis reduction on M has variations on LLL that control the quality of the basis, that is, at the expense of run-time how short the basis vectors can be. All elements of $\mathcal{L}$ are integral sums of columns of M, and the LLL process used to find a short basis is outlined in [57]. These short vectors are collected in a new matrix $M' = MU$, a reduced form of M that serves as a short basis of $\mathcal{L}$.

The union of orbits of 3-spaces corresponding to the indices of the 1's in u will form a $t - [q^n, k, \lambda]$ design $\mathcal{D}_1$. After removing the 127 orbits corresponding to the 1's in u from $A_{t,k}$, we obtain a new $\rho(t) \times 254$ matrix $Q_{t,k}$. Next, a new matrix M is formed using $Q_{t,k}$ and the same procedure as before.

$$M = \begin{bmatrix} I_m & \vec{0}_m \\ Q_{t,k} & -\lambda J \end{bmatrix}$$

M spans a new lattice $\mathcal{L}$ that once again through lattice basis reduction can yield a solution to $Q_{t,k}u = d'\lambda J$, giving us a second design $\mathcal{D}_2$, disjoint from $\mathcal{D}_1$.

Removing the columns corresponding to the orbits forming $\mathcal{D}_2$ from $Q_{t,k}$ leaves columns that represent orbits that will form a final design $\mathcal{D}_3$. Therefore, $\mathcal{D}_1, \mathcal{D}_2, \mathcal{D}_3$ will be an $LS[3][t, k, q^n]$ large set.

5.1.3 Lattice basis variations

Throughout each stage of this process, it is not guaranteed that lattice basis reduction will yield a solution to (3.1). In order for basis reduction to find a solution u to (3.1), there must exist a column of the reduced M matrix that has the form

described in corollary (5.1.1). If no such column exists after reduction, the columns of the newly reduced lattice basis matrix M are reordered before the basis reduction is attempted again.

The output of the LLL algorithm depends on the order of the basis, as one particular order might yield a short vector, while another might not change the vectors at all.

A reordering of the columns followed by LLL reduction may give us a solution. LLL applied to the same ordered basis is an idempotent operator, so if the columns of M were not reordered after each lattice basis reduction, then the program would merely return the same basis and analogously, the same M matrix after every reduction. While the method in which the columns are reordered could have been random, the methods we used were designed to be distinguishable amongst one another, and were not to be changed from one basis reduction to another.

If basis reduction does not find a solution, the input to LLL is changed by permuting the columns of M in one of three ways:

$$\left.\begin{array}{ll} \text{(i)} & \text{Reordering by increasing weight} \\ \text{(ii)} & \text{Alternating between the beginning columns and the last columns} \\ \text{(iii)} & \text{Alternating between small weight and large weight columns} \end{array}\right\} \quad (5.3)$$

Weight is determined by the Euclidean norm of the columns.

This procedure was repeated anytime a solution to (3.1) is not found from M. The APL program would choose the same single method of permuting columns for every time a solution to (3.1) was not found. We found 9 large sets using lattice basis reduction, but the number of times the program had to repeat could cause the run-time to be fairly large. As a result, a much faster method was also used to find $LS[3][2, 3, 2^8]$ large sets, which we describe below.

5.2 LINEAR PROGRAMMING METHOD

Definition 5.2.1. *An integer linear programming (ILP) problem is the optimization of the value of an objective function:*

$$f(x) = c^T \cdot x$$

where $x = (x_1, x_2, \ldots, x_n) \in \mathbb{Z}^n$*, and* $c \in \mathbb{R}^n$ *is a coefficient vector of length* n*. the vector* x *is subject to the constraint matrix equation:*

$$Ax^T + s = b$$

where A *is a* $m \times n$ constraint coefficient *matrix,* $s = (s_1, s_2, \ldots, s_n)$ *is a* slack vector *where* $s_i \geq 0$ *for* $1 \leq i \leq n$*, and* $b = (b_1, b_2, \ldots, b_m)$ *is the vector of* constraint limits.

A $\{0,1\}$ ILP problems require $x_i \in \{0,1\}$ for all i, and our task is determining $\{0,1\}$ values of x_i that will maximize or minimize $f(x)$ while keeping all s_i nonnegative. Our linear programming problem is defined as follows:

$$\begin{array}{lll} \text{(i)} & \text{maximize} & f(x) = c^T \cdot x \\ \text{(ii)} & \text{subject to} & Ax^T + s = b, \\ \text{(iii)} & \text{where} & s \geq 0, \\ \text{(iv)} & \text{and} & x \in \{0,1\}^n \end{array} \tag{5.4}$$

In our particular case $A = A_{t,k}$, x is a $\rho(k) \times 1$ vector, the slack vector s is set to 0, and b is the $\rho(t) \times 1$ vector λJ. For the objective function $f(x)$, we set $c(i) = J$, the all ones vector of length n. This solution yields a single $t - [q^n, k, \lambda]$ design by allowing $u = x^T$ in (3.1). After removing the orbits corresponding to the 1's in solution vector x from $A_{t,k}$, we obtain a new matrix $Q_{t,k}$. We next solve a new $\{0,1\}$ ILP replacing A in (5.4) with $Q_{t,k}$.

A new solution will constitute another block-disjoint $t - [q^n, k, \lambda]$ design, and once these orbits are removed from $Q_{t,k}$ the remaining orbits constitute a

$t - [q^n, k, \lambda]$ design disjoint from the previous two. Thus we arrive at a $LS[3][t, k, q^n]$ large set. To obtain a different solution, the columns of $A_{t,k}$ are permuted at random, and the resulting matrix becomes the input to the above process.

5.2.1 GUROBI

GUROBI is a commercial analytic mathematical programming solver, which includes integer linear programming, [33]. While GUROBI has capability to solve other programming problems, we use it to solve our $\{0, 1\}$ ILP. The program requires specific spacing, formatting, and listing of the x_i variables, the objective equation, the objective coefficients (which for our ILP were all 1), the restraint equations, and the restraint variables $a_{i,j}$. The variables must also be designated as discrete, continuous, binary, or some other type. After preliminary programming to obtain this format, GUROBI identifies whether the objective is to maximize or minimize the objective equation, and creates a limit or goal objective value for the equation that it aims to attain through a proper combination of the variables that satisfies the restraints.

GUROBI examines *nodes* that represent different branching possibilities of what the objective can become if certain variables have already been chosen. These nodes are deemed *infeasible* by the program if the limit objective is unattainable from the node selected, in which case the program instead branches into a different node. The program labels solution possibilities from these infeasible nodes as unexplained. The search is exhaustive, and GUROBI stops and indicates the values of all the variables x_i chosen when it has achieved the objective limit it was looking for. Because $x_j \in \{0,\ 1\}$ for all i, these indicate the Γ_i orbits used to get our design. GUROBI stops otherwise only if it has exhausted every single node and combination of variables available.

GUROBI can also be altered for the restraints to be inequalities as opposed to

equations:

$$\begin{array}{lll} \text{(i)} & \text{maximize} & f(x) = J \cdot x \\ \text{(ii)} & \text{subject to} & A_{2,3}x^T + s = 21, \\ \text{(iii)} & \text{where} & s \geq 0, \\ \text{(iv)} & \text{and} & x \in \{0,1\}^n \end{array} \tag{5.5}$$

The program would output x that achieves a value relatively close to the limit it was looking for. These near-solutions found using inequalities instead of equations were deemed unhelpful for the purposes of finding a solution to (3.1). Unlike APL, we lack the ability of adjusting the program to include saving features or options to interrupt and resume the program later, making lengthier searches much more risky.

One advantage GUROBI has over APL is the ability to disprove the existence of a design from a given $A_{t,k}$, as an exhaustive search that results in no solution proves that a design cannot be found from a given $A_{t,k}$. However, the amount of nodes that GUROBI must test to disprove the existence of a design using $A_{t,k}$ can be numerous to the point that the time required to deem every node infeasible is almost implausible without multi-threaded programming. Even with extra processing power, the procedures are lengthy and can require so much time that some linear programming questions can approach implausible amounts of time to work through with either of our methods. Luckily, APL and GUROBI both have the capability of being run from several different computers that will increase the speed of the program. This makes GUROBI check nodes faster, using multiple sources to search and test nodes, though not necessarily in the same order they were checked before.

We were able to obtain two non-isomorphic solutions, but many more could have been constructed by this method. Unlike the program in APL used for lattice basis reduction method, the program we used with GUROBI can be interrupted, but not resumed. While GUROBI will eventually generate a solution or conclude that there is no solution, there is no way to save the progress of the program until that

happens. Therefore, GUROBI poses a greater risk of inter-process failure than lattice basis reduction.

Regardless of the method we used, our large sets were found by looking for G-invariant geometric designs, which required us to choose a group $G \in GL_8(2)$ in which to create our 2-subspace orbits and 3-subspace orbits. We allowed our group to be a Singer subgroup, and it was the same used by [17] for two reasons: the choice of which element of order $q^n - 1$ in $GL_n(q)$ we use is unimportant due to the conjugacy of all Singer subgroups in $GL_n(q)$, [44], and we could easily check the property of whether they were non-isomorphic not only to each other but to the large set found in [17]. We now present the actual data and results of our work.

CHAPTER 6

THE KRAMER-MESNER MATRIX

We construct 9 non-isomorphic large sets of geometric 2-$[2^8, 3, 21]$ designs using methods similar to those used in [17], and 2 more non-isomorphic large sets using linear programming methods. All of the solutions are $[G]$-invariant under the same Singer subgroup G of order 255, using the Kramer-Mesner matrix $A_{2,3}$, constructed from $G = \langle\alpha\rangle$. The generator α can be expressed by the matrix belonging to $\Theta = GL_8(2)$ appears below:

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

6.1 THE SUBSPACE ORBITS

There are 10795 2-subspaces in $\begin{bmatrix} V \\ 2 \end{bmatrix}$ where $V = \mathbb{F}_2^8$, and 97155 3-subspaces in $\begin{bmatrix} V \\ 3 \end{bmatrix}$. The G-orbits on $\begin{bmatrix} V \\ 2 \end{bmatrix}$ and $\begin{bmatrix} V \\ 3 \end{bmatrix}$ are computed using using our programs and subroutines in our APL system packages "*knuth*" and "*giant*". The results were stored both as orbits, and separately as the subspaces themselves. Our algorithm represents the members of $\begin{bmatrix} V \\ 2 \end{bmatrix}$ as Klein 4-groups, and $\begin{bmatrix} V \\ 3 \end{bmatrix}$ as elementary abelian groups of order 8. However, the 2-subspaces and 3-subspaces, viewed projectively, can be seen as collinear triples and Fano planes respectively in V. The collection of 97155 3-subspace blocks became a collection of orbits $\mathcal{K} = \{\Gamma_j\}_{j=1}^{381}$, all of length

255, while the 10795 2-subspaces became a collection of orbits $\mathcal{T} = \{\Delta_i\}_{i=1}^{43}$ all of length 255, except for Δ_{43} which is of length 85.

6.1.1 Orbit representatives

The orbits of both $\mathcal{T}$ and $\mathcal{K}$ can be all identified by a single representative each, and the lexically smallest subspace of the orbit is shown here as the lexically smallest basis of the subspace. G is transitive on the non-zero vectors, so each basis representative of each orbit includes the vector $1 \equiv 00000001$. Thus, by deleting the vector 1 from each basis, we can represent economically the 2-space $\langle\alpha\rangle$-orbits by the 43 vectors below:

2	4	6	8	10	12	14	16	18	20	24	28	30	32	34
36	38	40	42	44	50	54	56	58	60	62	70	74	76	78
80	86	88	96	100	106	114	128	136	146	164	210	218		

These orbits can be expressed as $\Delta_i \in \mathcal{T}$, indexed in lexicographic order. The representatives of the orbits in $\mathcal{K}$ are expressed similarly. There are 255 Fano planes in each orbit under G, and each Fano plane has a lexically smallest basis of 3 vectors, so we select the smallest basis of these 255 smallest bases. Take for example the bases of the 255 Fano planes of Γ_1 seen on the following page, all of which are the lexically smallest basis of 3 vectors of their respective Fano plane:

1	2	4	13	23	195	25	97	136	38	87	147	51	73	146
1	2	184	13	65	149	25	108	173	38	89	148	51	85	146
1	2	208	13	82	179	26	46	70	39	70	140	51	85	153
1	78	158	13	103	179	26	46	195	39	78	140	52	65	130
1	92	184	13	119	131	26	65	130	39	78	156	52	67	153
1	104	184	14	18	36	26	109	131	39	79	159	52	92	140
1	124	134	14	18	199	27	45	65	40	80	136	52	92	159
2	4	8	14	71	146	27	45	131	40	91	149	53	81	151
2	4	209	15	17	34	27	76	174	41	71	155	53	87	147
2	77	156	15	17	161	28	36	72	41	77	133	53	95	139
2	125	133	15	87	176	28	36	199	41	82	133	53	95	151
3	5	9	15	118	132	28	73	142	41	82	141	54	90	130
3	5	185	16	32	64	29	39	78	41	82	154	55	74	148
3	93	185	16	32	207	29	39	140	41	86	133	55	83	145
3	124	132	16	69	138	29	70	171	41	95	151	55	86	148
4	8	16	16	107	141	29	104	130	42	71	142	55	89	133
4	8	211	17	34	68	30	34	68	42	84	130	55	89	148
4	73	154	17	34	131	30	103	139	42	84	157	55	89	155
4	123	129	17	73	161	31	33	66	43	67	134	55	94	140
5	10	17	17	103	139	31	33	137	43	74	136	56	72	143
5	10	176	18	36	72	31	33	197	43	86	134	56	72	144
5	88	186	19	38	76	31	67	134	43	86	135	56	85	146
5	121	129	19	38	132	31	75	168	44	79	137	57	75	150
6	10	18	19	38	205	31	109	168	44	88	147	57	75	157
6	121	129	19	66	162	31	111	143	44	88	156	57	82	157
7	9	18	19	74	135	32	64	128	44	93	150	57	84	142
7	9	178	19	98	128	32	64	143	45	87	131	58	78	156
7	9	210	19	111	162	32	69	138	45	90	131	58	79	159
7	73	155	20	40	68	32	75	157	45	90	153	59	66	132
7	89	187	20	103	129	33	66	132	46	67	153	59	77	139
7	105	187	21	42	65	33	66	137	46	92	150	59	77	154
8	16	32	21	42	141	33	81	144	47	64	128	59	77	158
8	16	199	21	42	201	33	84	137	47	70	140	59	79	158
8	69	146	21	71	142	34	68	136	47	74	128	59	88	158
8	115	133	21	76	167	34	69	139	47	93	150	59	95	151
9	18	36	21	110	167	35	68	138	47	94	128	60	68	136
9	18	167	22	44	78	35	69	138	47	94	147	60	91	149
9	87	181	22	44	203	35	70	136	47	94	148	61	71	131
10	20	34	22	75	128	35	70	138	48	80	144	61	71	142
10	115	129	22	99	137	35	70	140	48	91	141	61	71	155
11	22	39	23	46	75	35	91	149	49	64	128	61	73	156
11	22	160	23	46	138	36	72	144	49	80	145	61	83	155
11	22	192	23	69	164	37	64	138	49	81	145	61	87	147
11	64	150	23	109	142	37	67	143	49	83	145	61	95	155
11	80	182	24	40	72	37	68	136	49	83	147	62	66	132
11	96	182	24	107	141	37	74	134	49	83	151	62	66	135
11	117	130	25	43	79	37	74	143	50	81	144	62	67	134
12	20	36	25	43	134	37	74	148	50	83	145	62	81	143
12	115	129	25	43	193	37	85	143	50	86	151	63	65	130
13	23	35	25	67	173	38	76	129	50	86	158	63	65	152
13	23	164	25	72	137	38	76	152	51	69	154	63	76	152

The lexically minimal basis of this collection of 255 bases is (1,2,4), therefore it is our representative for the orbit Γ_1. The lexically minimal basis of the lexically minimal representative of each orbit contains 1, so the representatives are listed by the two other vectors in $\mathbb{F}_2^8$ that together with 1 form the basis.

Our 43×381 matrix $B_{2,3}$ was first computed from these orbits. Any 3-space in any orbit of $\mathcal{K}$ can be expressed as a Fano plane F, making it simple to see how the 7 lines of F, that is the 7 collinear of F triples are distributed among the orbits $\Delta_i \in \mathcal{T}$. We observe that the entries of $B_{2,3}$ consist of 0's, 1's, and 3's, with 3's appearing exactly once per row, except for row 43 which consists of 0's and 1's only. $A_{2,3}(i,j)$ is then determined by multiplying each entry of $B_{2,3}$ by the ratio of the orbit lengths. That is, by using condition (iii) of lemma (3.2.1):

$$A_{2,3}(i,j) = \frac{|\Gamma_j|}{|\Delta_i|} B_{2,3}(i,j)$$

All ratios are 1, except for the ratio of 3 between orbits of $\mathcal{K}$ and orbit $\Delta_{43} \in \mathcal{T}$, which contains the 2-subspace representative $(1, 218)$. $B_{2,3}$ is equal to $A_{2,3}$ except for the 43rd row, where $A_{2,3}$ is 3 times $B_{2,3}$, thus $A_{2,3}$ has a row sum of 63 for all rows.

Of course, the row sum is the number of Fano planes that contain any given collinear triple. Take for example the collinear triple $(1, 2, 3)$. Note that $3 \in \langle 1, 2\rangle_+$, i.e. the dimension of the linear space spanned by $\{1, 2, 3\}$ is 2. Now, if $S = \mathbb{F}_2^8 - \langle 1, 2\rangle_+$, and $x \in S$, then $\langle 1, 2, 3, x\rangle_+ = \langle 1, 2, x\rangle_+$ is a linear 3-space, projectively a Fano plane. In particular for $x = 10$, we get the Fano plane:

$$\{1,\ 2,\ 3,\ 8,\ 9,\ 10,\ 11\}$$

However, this same Fano plane is formed if $8, 9$, or 11 is chosen, resulting in $\frac{1}{4}$ of the remaining vectors of $\mathbb{F}_2^8$ forming unique Fano planes. 63 Fano planes can be created that contain a given collinear triple, resulting in 63 being the row sum of every row of $A_{2,3}$.

6.2 THE $A_{2,3}$ MATRIX

Representing the matrix $A_{2,3}$ so that a reader who does not wish to compute the matrix can still check the results, requires a user-friendly matrix encoding. Each column of $A_{2,3}$ is a vector of 43 elements from $\{0, 1, 3\}$, so we proceed to get a compressed representation of the column using radix 4 words of length 3. In particular, we adjoin two extra 0's at the top of the column and transpose each of the 381 columns to get $\{v_i\}_{i=1}^{45}$, where $v_i \in \mathbb{Z}_4^{45}$. These vectors are then separated into 15 triples, each encoded using radix-4 notation to be an element of the following alphabet Λ_m with digits as values from 0 to 63:

$$0123456789abcdefghijklmnopqrstuvwxyz$$

$$ABCDEFGHIJKLMNOPQRSTUVWXYZ+-$$

An encoding is demonstrated below:

$$100011010100010100000000000000000000000000 \rightarrow$$

$$001000110101000101000000000000000000000000000 \rightarrow$$

$$001\ \ 000\ \ 110\ \ 101\ \ 000\ \ 101\ \ 000\ \ 000\ \ 000\ \ 000\ \ 000\ \ 000\ \ 000\ \ 000\ \ 000 \rightarrow$$

$$\Lambda_1\ \ \Lambda_0\ \ \Lambda_{20}\ \ \Lambda_{17}\ \ \Lambda_0\ \ \Lambda_{17}\ \ \Lambda_0\ \ \Lambda_0\ \ \Lambda_0\ \ \Lambda_0\ \ \Lambda_0\ \ \Lambda_0\ \ \Lambda_0\ \ \Lambda_0\ \ \Lambda_0 \rightarrow$$

$$10kh0h000000000$$

We display $A_{2,3}$ in this dissertation by exhibiting the columns of the matrix in this encoding scheme over the following three pages. Any string of fewer than 15 characters starts with the first non-zero character of the string. Each column is also labeled by the two vectors which together with 1, form the lexically smallest basis of the lexically smallest orbit representative of the orbit $\Gamma_j \in \mathcal{K}$ for that column. With $A_{2,3}$ formed, we could find our geometric t-designs and in turn our geometric large sets using our two solution methods.

1	2 4	3k0000000040004	44	2 176	10000g001105040	87	4 120	k10l0000040000
2	2 8	1lg000100000100	45	2 180	1000g01l0000010	88	4 122	g000400000ggk4
3	2 12	1k5000000011000	46	2 188	10000010004h40g	89	4 128	g000g004040gg4
4	2 16	111k0000g000040	47	2 192	100100k0100h000	90	4 130	k00l0100010000
5	2 20	10kh0h000000000	48	2 196	1010000g0014013	91	4 136	g000c400000050
6	2 24	1140M0400000000	49	2 200	1000010044g0gg0	92	4 138	gg000hg0500000
7	2 28	10h050000000013	50	2 204	10010011gg0000g	93	4 144	g0041g10401000
8	2 32	100g1k00000040g	51	2 212	100000000gh0504	94	4 146	h0000000ggg050
9	2 36	100541g000000g0	52	2 216	1000504g0010003	95	4 152	g004ggg0g00g00
10	2 40	1101g05000000g0	53	2 220	10000100g300100	96	4 160	g100g40000140g
11	2 44	110gg04g4000000	54	2 224	10000004140ggg0	97	4 162	g0100g001g4040
12	2 48	104gg004000g400	55	2 228	1g000400400010k	98	4 168	h00011g0000410
13	2 52	1045g0010004000	56	2 232	10110g000005040	99	4 170	g00045000000hg
14	2 56	100g400gk00000g	57	2 236	10g40101000010g	100	4 176	g00g10g0040g40
15	2 60	100110001g10040	58	2 240	1000400000hg0h0	101	4 178	g000g01g0004h0
16	2 64	10144g001g00000	59	2 244	10g51000g000g00	102	4 192	g44000g001gg00
17	2 68	100004001l00100	60	2 248	140000g0005g004	103	4 194	g01000g0g10440
18	2 72	10001h00gh00000	61	2 252	100g040k4400000	104	4 200	g01000411040g0
19	2 76	1g0000g040k1000	62	4 16	M0h00000104000	105	4 202	gg00000400030g
20	2 80	104400k01010000	63	4 18	g0k00101110000	106	4 216	g000141g000440
21	2 84	1000001c000g010	64	4 24	k00l0010000100	107	4 218	g000h00g400007
22	2 88	1000000j000400g	65	4 26	k00l0040001000	108	4 224	g400000h000gg4
23	2 92	1h40000000gg004	66	4 32	h000h040g00003	109	4 226	g0001040000ggk
24	2 96	10400g0000g5040	67	4 34	gg004g10000140	110	4 232	g004g10400010g
25	2 100	10g004140000g10	68	4 40	hg0004g00gg000	111	4 234	g041001g001400
26	2 104	14k004g00000400	69	4 42	h040g500400000	112	4 240	g400040h0g1000
27	2 108	1000010hg500000	70	4 48	gc00000h010000	113	4 242	gg004405000010
28	2 112	11000000g400hg0	71	4 50	g10ggg50000000	114	4 248	g0g00g40g44000
29	2 116	101g110g4000000	72	4 56	g540000h000010	115	4 250	l0000040400007
30	2 120	100040k05000g00	73	4 58	g1001004g01010	116	6 16	40M00000001h00
31	2 124	140004100g40004	74	4 64	ggh00001gg0000	117	6 18	c05000001000g0
32	2 128	100014k010000g0	75	4 66	g100001g410400	118	6 32	4g00gg0g000g10
33	2 132	151000004040004	76	4 72	g04100g00k4000	119	6 34	4l005100000000
34	2 136	10gg40000g00440	77	4 74	ggg000001400k0	120	6 40	5400040g000h00
35	2 140	100004000c00gg0	78	4 80	g0h10040410000	121	6 42	410g11g0000040
36	2 144	100010g000g0k10	79	4 82	h04000000gM000	122	6 48	5k004010001000
37	2 148	1000000101g4110	80	4 90	g040441000g010	123	6 50	440014400g0040
38	2 152	10004100g1g0040	81	4 96	g00g0000g11g0g	124	6 56	5000g00gk00003
39	2 156	1gh000000g4000g	82	4 98	g0g101000044g0	125	6 58	4h000005004010
40	2 160	10000g000015440	83	4 104	k00l00g0400000	126	6 64	400g0001k0004g
41	2 164	10040g00000504g	84	4 106	g0500000504400	127	6 66	41011101g00000
42	2 168	1000001400005h0	85	4 112	g1040045000g00	128	6 74	401000401g0g0g
43	2 172	1104g040000gg00	86	4 114	g00g1g0400010g	129	6 80	400g000001hg0g

130	6 82	404400401004g0	173	8 82	1g44001000g040	216	10 130	g110040000g44
131	6 88	4000000400s004	174	8 98	10005000014k00	217	10 132	g400444410000
132	6 96	40g40100001500	175	8 100	140g00g0100k00	218	10 144	k000hh0100000
133	6 98	40g00g0000kk00	176	8 102	1g00ghg0100000	219	10 146	g040400014013
134	6 106	405000g0000k10	177	8 112	1104g00g000h00	220	10 160	kg000000404gg
135	6 112	40g014g00g0g00	178	8 114	1040000g044h00	221	10 162	g04100040k400
136	6 114	41g040g0001100	179	8 116	11041000040050	222	10 164	h00040040g40g
137	6 120	40544010040000	180	8 118	11005000015000	223	10 180	g4g004g001004
138	6 122	5000g000150g00	181	8 128	10g0001gg000k0	224	10 192	g00000k00k00k
139	6 130	40010014g0g040	182	8 130	1g4100000g5000	225	10 194	g1g0000g100k0
140	6 136	4001004140004g	183	8 144	10k40h01000000	226	10 196	g0410000h00gg
141	6 138	4k00k004000100	184	8 146	100000041k1010	227	10 198	g11g0g00g0g00
142	6 144	44000g0g0h0010	185	8 148	10000014k010g0	228	10 210	g050410001004
143	6 146	4000g0140g00h0	186	8 160	101000g4000c00	229	10 212	g10000l010010
144	6 154	40400004h400g0	187	8 162	100101010041g0	230	10 224	g00404h005000
145	6 160	44000104004440	188	8 166	10g0040g0k0040	231	10 226	g0gg045000010
146	6 162	4000000140k04g	189	8 182	10001000g01030	232	10 228	g4g0004000144
147	6 168	4g00044g001400	190	8 192	140g0010g0g0g0	233	10 240	g4g00000hg004
148	6 170	50100050g000g0	191	8 194	101g0004g00410	234	10 244	g0g0g0g40g400
149	6 176	400000g140005g	192	8 196	10100104410400	235	12 16	4g4000000401k
150	6 178	400gg01104g000	193	8 198	10g000g10g000k	236	12 18	4510000440010
151	6 192	4001g0g001g100	194	8 212	10005040054000	237	12 32	400g1k000g100
152	6 194	401400g00h00g0	195	8 224	1004g04100400g	238	12 50	40000l0g0400g
153	6 200	404000001100hg	196	8 226	10010041101004	239	12 54	4000154000g40
154	6 202	50104004100400	197	8 228	1k04000000010k	240	12 66	501000044001g
155	6 216	40001c0g0g0000	198	8 230	1041gg0000010g	241	12 68	5010004h0g000
156	6 218	4000104gg00007	199	8 240	14010g001g000g	242	12 70	5400100l00000
157	6 224	4000g0014g004g	200	8 242	111000g0001014	243	12 84	4h0h040004000
158	6 232	4040k0g0g0000g	201	8 244	10g4000g0000c0	244	12 98	4040040105400
159	6 234	40g0041000h100	202	8 246	1g000010510004	245	12 112	4400010040k03
160	6 240	4g0014110g0000	203	10 16	gggg0000k00g0	246	12 118	400100400kg04
161	6 242	40000M0g000410	204	10 18	g5g1000400004	247	12 128	40440g00000gk
162	6 248	40000g0g404014	205	10 50	g01004g003000	248	12 130	40100004k0050
163	6 250	41g01100004004	206	10 52	l040000h000g0	249	12 132	4011104000140
164	8 20	10144010040004	207	10 64	g00g001h50000	250	12 144	4040k00k01000
165	8 22	10g10g400000gg	208	10 66	h0104g0004003	251	12 148	4144g10040000
166	8 34	10045100014000	209	10 68	Mg00000g400g0	252	12 162	40g0500g04g00
167	8 38	30010g0100000g	210	10 70	g0000h04g400g	253	12 166	40000100014k3
168	8 50	11g00054010000	211	10 84	g00014040g440	254	12 176	400g504400040
169	8 52	14000gg10010g0	212	10 100	g000hg0100g40	255	12 182	4050000440110
170	8 66	11004040500g00	213	10 102	h000hg010g000	256	12 192	4h1h00000g000
171	8 70	11100400440100	214	10 112	g110000000M10	257	12 194	41400400g000k
172	8 80	1g00l000014000	215	10 118	h0g1001040400	258	12 196	500000g01g1g0

259	12 198	44040g4g00400	300	16 196	g00014430000	341	24 130	h400g1g1000
260	12 214	4000000040hk3	301	16 200	gg04001040h0	342	24 162	g4g0g0k4000
261	12 224	40000g1010114	302	16 202	gg400410000j	343	24 164	g4100011g0g
262	12 226	44g0444100000	303	16 226	g0g05000g0h0	344	24 166	g0000111g4g
263	12 228	4h0l000000004	304	16 228	k0010hg00004	345	24 168	g10g4400440
264	12 230	5004000h0100g	305	16 232	gggg00000414	346	24 170	gM0100000h0
265	12 240	4h0h0004g0000	306	16 234	g40gg0401004	347	24 234	g1100g01014
266	12 242	4g10g00440010	307	18 32	44g4k4000000	348	24 236	k000g504100
267	14 20	11g0g00040044	308	18 40	404k44000040	349	28 32	cg005000g00
268	14 22	1gg400h0g0000	309	18 44	4040kgg40000	350	28 74	41000h0h010
269	14 38	1100k000041g0	310	18 68	4440g0ggg000	351	28 96	40h0044h000
270	14 66	30000500g0g00	311	18 96	400010001h43	352	28 102	4010l004g00
271	14 86	1000g0400k044	312	18 100	4g1000011g0g	353	28 226	40440500404
272	14 100	100g0110g0k00	313	18 132	40g0044k1000	354	28 236	40000gg0514
273	14 128	100400gk0g0g0	314	18 160	41k0000g4400	355	30 36	31004g0g000
274	14 130	10h41000040g0	315	18 164	414000000g5g	356	30 38	1kg0g010400
275	14 148	1000g141g0g00	316	18 196	401g400101g0	357	30 40	10411010404
276	14 150	10k00401g0400	317	18 200	4000000415g3	358	30 64	1101110g100
277	14 160	100040004040M	318	18 206	403g000000gg	359	30 78	10g40050140
278	14 164	10104001004gg	319	18 226	400040gg0504	360	30 110	1k000100k04
279	14 166	104000g00g4k0	320	18 230	4000hg00401g	361	30 162	105000040M0
280	14 178	140gh00000044	321	18 234	401g040010g4	362	30 174	14510000044
281	14 194	1300400001100	322	18 236	4h00004g4100	363	30 228	1041010000c
282	14 198	1000gg00100k4	323	20 38	101g500g000g	364	32 78	g10015h000
283	14 214	110g4g000g100	324	20 44	1100gkg0g000	365	32 94	k0gg10g100
284	14 224	1s00101000000	325	20 78	1k4110040000	366	32 156	g500k4000g
285	14 226	1004g400h0100	326	20 102	10010004h110	367	32 196	g400150044
286	14 240	1g000104g0h00	327	20 132	1g4g05000003	368	32 216	gk40g10100
287	14 242	1k00000410014	328	20 140	14501004g000	369	34 192	404100g150
288	14 244	10gg00g00g0g4	329	20 162	1g0001404110	370	34 200	40g14g10g0
289	16 38	g00h10g01g00	330	20 164	100040gh004g	371	36 64	140104gk00
290	16 42	g1011k010000	331	20 170	1000g10011k0	372	36 78	1013040400
291	16 70	g0500040hg00	332	20 192	14010g01g00g	373	36 196	1101050500
292	16 74	g00414110010	333	20 202	10010Q00000g	374	36 198	14kg040100
293	16 78	g0040014g01g	334	20 206	100g0410g00j	375	38 68	k00M04g00
294	16 98	g40400g04h00	335	20 230	10010g000g1k	376	40 68	4g0g54g00
295	16 108	gh00kg040000	336	20 234	10g500401004	377	42 76	3000M0003
296	16 110	h0400110g003	337	24 38	g0g10k04100	378	42 78	111140g04
297	16 140	g04000gg0504	338	24 106	g0001gg0504	379	44 64	M10010g4
298	16 164	gg0g0100g00j	339	24 110	g10g0100150	380	44 78	kg0c4000
299	16 166	k40400100050	340	24 128	k400g0h00g0	381	58 128	c0k10g0

CHAPTER 7

THE SOLUTIONS

The first collection of geometric large sets that we found using $A_{2,3}$ was found by the same procedure used by [17], namely, lattice basis reduction. We form our lattice basis in a similar fashion as [17] as well.

7.1 LATTICE BASIS REDUCTION SOLUTIONS

After $A_{2,3}$ is constructed, the lattice basis matrix M is constructed with $\lambda = 21$.

$$M = \begin{bmatrix} I_{381} & \vec{0}_{381} \\ A_{2,3} & -21J \end{bmatrix}$$

The lattice-basis reduction process along with the procedure mentioned earlier eventually yields a column of M which led to a solution u_1 to (3.1), giving us a $2-[2^8, 3, 21]$ geometric design $\mathcal{D}_1$. Once u_1 is found, a new matrix M' is created by using $Q_{2,3}$ and $\lambda = 21$, and the process is repeated to find a second solution u_2 and design, $\mathcal{D}_2$.

$$M' = \begin{bmatrix} I_{254} & \vec{0}_{254} \\ Q_{2,3} & -21J \end{bmatrix}$$

The union of the remaining orbits, obtained by removing the orbits constituting $\mathcal{D}_1$ and $\mathcal{D}_2$ from the 381 G-orbits on $\begin{bmatrix} v \\ 3 \end{bmatrix}$ form a third design, $\mathcal{D}_3$, and together, $\{\mathcal{D}_1, \mathcal{D}_2, \mathcal{D}_3\}$ form a large set of $2-[2^8, 3, 21]$ geometric designs. We found the first 9 large sets of $2-[2^8, 3, 21]$ designs by using the procedures of constructing

M and $M^{'}$ using $A_{2,3}$ and $Q_{2,3}$, respectively, applying the lattice-basis reduction algorithm on M, and $M^{'}$, using the LLL procedure, and permuting the columns of M and $M^{'}$ any time a solution to (3.1) is not found by the the lattice-basis reduction program.

7.1.1 Column permutations

The method of permuting the columns would not change until a solution u was found, and each of the permutation methods (5.3) eventually produces a solution after a bounded number of basis reductions. In the worst case, 9871 permutations followed by LLL reductions were needed.

Since LLL is deterministic, the same initial $A_{2,3}$ or $Q_{2,3}$ matrix would produce the same solution as long as the columns of M were permuted the same way after each basis reduction. Initially 3 solutions u_1, u_2, u_3 were found to equation (3.2) by a rather large number of LLL reductions following basis permutations ($\leq 10,000$). The three designs $\mathcal{D}_1', \mathcal{D}_1'', \mathcal{D}_1'''$ corresponding to the u_i are removed from $A_{2,3}$ to form three matrices $Q_{2,3}', Q_{2,3}'', Q_{2,3}'''$, and by lattice basis reduction on matrices M', M'', M''' corresponding to the $Q_{2,3}$ matrices, we obtain 3 second designs $\mathcal{D}_2', \mathcal{D}_2'', \mathcal{D}_2'''$. Removing these second designs from their $Q_{2,3}$ matrices leaves 3 final designs $\mathcal{D}_3', \mathcal{D}_3'', \mathcal{D}_3'''$. Thus, we obtain 3 large sets $\mathcal{L}_1 = \{\mathcal{D}_1', \mathcal{D}_2', \mathcal{D}_3'\}$, $\mathcal{L}_2 = \{\mathcal{D}_1'', \mathcal{D}_2'', \mathcal{D}_3''\}$, and $\mathcal{L}_3 = \{\mathcal{D}_1''', \mathcal{D}_2''', \mathcal{D}_3'''\}$.

We repeat this process two more times using different column permutations thus generating all together 9 distinct large sets. While LLL produces at most one solution at a time the approach of permuting the basis produces different reduced bases and distinct solutions. The time spent finding a solution using these techniques varied from one solution method to another, though there was no correlation for what permutation method (if any) found a solution to (3.2) with the fewest basis reductions for $A_{2,3}$ and $Q_{2,3}$.

Conjugating the Singer cycle by elements in Θ and simultaneously the

designs in the large sets would yield more large sets, but we are convinced that with a fixed Singer cycle, many more solutions to (3.2) can be found by randomly permuting the columns of M before any basis reductions occur. As a result, the first design found using $A_{2,3}$ always had the second 3-space orbit $\Gamma_2 \in \mathcal{K}$ used, and never had the first orbit $\Gamma_1 \in \mathcal{K}$. The designs within each large set are indexed in lexicographic order based on the orbits within them, so the first design found in each large set is the second design indexed, and was shared among trios of large sets.

Recall the lattice basis reduction method requires removing columns from $A_{2,3}$ to form $Q_{2,3}$ after finding a design. Afterward, we choose one of three methods of permuting the columns of $Q_{2,3}$ after each column reduction. This resulted in the 9 large sets we found consisting of three trios of large sets that all share a design within a trio, the first design found using any of the three permutation methods, which always contained $\Gamma_2 \in \mathcal{K}$.

7.1.2 Presenting the lattice basis reduction solutions

The combination of the (5.3) permutations used to find each of the large sets we obtained are shown on the table below. The row indicates the first permutation used on M derived from $A_{2,3}$ to find a solution to (3.1), while the column indicates the second permutation used on M derived from $Q_{2,3}$ to find a solution.

	(i)	(ii)	(iii)
(i)	$\mathcal{L}_1$	$\mathcal{L}_8$	$\mathcal{L}_6$
(ii)	$\mathcal{L}_2$	$\mathcal{L}_3$	$\mathcal{L}_9$
(iii)	$\mathcal{L}_5$	$\mathcal{L}_7$	$\mathcal{L}_4$

We display the 9 large sets found by lattice basis reduction on the following two pages in an array along with the large set found in [17]. The indices of the G-orbits Γ_j on 3-spaces, for $1 \leq j \leq 381$ are listed first. Next to the indices are 9 additional columns, each corresponding to one of the large sets we found using

lattice basis reduction. Finally there is one last column separate from the rest that corresponds to the large set found in [17]. Each column for the 9 large sets we found as well as the additional column has 127 1's, 127 2's, and 127 3's, which indicate the orbits contained in $\mathcal{D}_1, \mathcal{D}_2, \mathcal{D}_3$ respectively, for each large set. Our solution display has trios of columns that share the indices in which the number 2 appears. Columns 1, 6, and 8 all share a design and have 2 appear in all the same indices, columns 2, 3, and 9 all have 2 appear in the same indices, and column 4, 5, and 7 all have 2 appear in the same indices.

1	111111111	2	65	322223232	3	129	211332321	2
2	222222222	1	66	122311132	1	130	333221231	2
3	122311132	3	67	133113311	3	131	113113113	2
4	233222223	1	68	222222222	2	132	122133112	1
5	231222223	3	69	131221231	2	133	231222223	1
6	322133312	3	70	311111331	2	134	313223231	2
7	333313311	1	71	313223211	2	135	313333111	3
8	331221233	3	72	311133311	3	136	213222221	2
9	233222223	1	73	222332322	1	137	322331112	3
10	122331312	2	74	211222221	2	138	233222223	1
11	322113132	2	75	322333332	3	139	122131132	3
12	233132321	2	76	133223213	1	140	222222222	1
13	322333312	3	77	311313131	2	141	331131113	3
14	211112121	2	78	113113313	1	142	131223213	1
15	122333132	1	79	131131333	2	143	331223231	2
16	333113131	2	80	222112122	1	144	222112122	1
17	111331313	1	81	222112322	1	145	313311131	3
18	131131331	2	82	122221212	1	146	313221231	2
19	222222222	1	83	111221233	2	147	222312322	1
20	113111113	1	84	111113113	1	148	213312321	1
21	133333313	2	85	122311332	1	149	233132123	3
22	111111331	3	86	331223211	1	150	231312123	1
23	311311131	3	87	222222222	3	151	313313131	2
24	113313333	3	88	233132321	1	152	311131331	1
25	311113333	2	89	222222222	2	153	122333312	1
26	122113312	2	90	331133113	1	154	113223213	1
27	231312123	3	91	331113313	3	155	113331133	2
28	313223213	1	92	133111133	3	156	333223231	3
29	222222222	2	93	213222221	3	157	222332322	2
30	322133332	2	94	211112323	3	158	311113111	3
31	111221211	1	95	111331113	1	159	113111333	2
32	231222221	2	96	231332121	2	160	233312123	1
33	322223232	1	97	331331331	2	161	111111131	3
34	133223211	1	98	311311111	1	162	322113312	2
35	311333131	1	99	233222223	1	163	122311312	2
36	233332321	1	100	311221211	1	164	331311111	2
37	233222223	1	101	133221233	2	165	233222223	3
38	131223213	2	102	122223212	2	166	211222223	2
39	111313133	3	103	233332323	3	167	333113313	2
40	333221213	2	104	122131132	3	168	331221213	3
41	222332122	1	105	313333111	2	169	113223233	1
42	222312122	3	106	222132122	2	170	131133131	2
43	311313113	3	107	113221213	2	171	213222223	1
44	222222222	1	108	222332122	1	172	313333111	3
45	133131111	3	109	322133312	2	173	131313311	1
46	233132323	1	110	233112323	3	174	222312122	3
47	222222222	1	111	233312123	1	175	213222221	1
48	222332322	3	112	333313111	2	176	222332322	2
49	122113112	3	113	113223211	1	177	133111333	3
50	322221232	2	114	313131131	2	178	111331311	3
51	213222221	2	115	222222222	3	179	122131132	2
52	313131133	2	116	131313313	3	180	233222223	1
53	313111333	3	117	331133313	2	181	122313312	3
54	333221211	3	118	122311132	3	182	122131132	3
55	111331333	3	119	322221232	2	183	311333133	2
56	131131111	2	120	122313332	1	184	122133112	3
57	313333131	1	121	231312321	1	185	322221232	2
58	322223232	3	122	111221233	1	186	311131131	3
59	211132323	3	123	131131313	3	187	231312121	1
60	333331331	3	124	233132121	2	188	222312122	1
61	222312322	1	125	222332322	3	189	311131131	2
62	333333333	3	126	111221213	1	190	222132122	2
63	322111112	2	127	233132323	3	191	233312323	3
64	233132321	3	128	213312121	3	192	131133311	2

193	133333331	1	257	222222222	1	321	213222223	3
194	133113331	3	258	231132121	1	322	322113332	3
195	211222221	3	259	222332322	2	323	122331332	1
196	113111113	1	260	231222223	3	324	113221211	1
197	233132121	3	261	133221233	1	325	213332121	1
198	322331312	2	262	131221211	1	326	133221211	2
199	322221212	1	263	222132322	3	327	133311131	3
200	311221211	3	264	122311112	1	328	122113332	1
201	311131331	2	265	322221212	2	329	131111333	2
202	122333332	3	266	122133132	1	330	113113113	1
203	331313331	3	267	113223213	1	331	222112322	2
204	213222223	1	268	113221231	3	332	122113132	3
205	311133311	3	269	122223212	3	333	133333113	3
206	233222223	2	270	311133113	2	334	211332123	2
207	333223231	1	271	311313111	1	335	222222222	1
208	122131312	1	272	222112122	1	336	313113331	3
209	113131313	2	273	213332121	1	337	222222222	1
210	331131111	2	274	313111133	2	338	131313111	3
211	122223212	3	275	211112323	1	339	122223232	3
212	213332121	2	276	111331113	1	340	113113333	2
213	222222222	1	277	131311331	3	341	233222221	2
214	133111111	2	278	113113313	2	342	233332123	2
215	322221232	3	279	331223213	1	343	133223213	3
216	331311133	3	280	133133333	3	344	322311132	3
217	231312321	1	281	331113131	2	345	133113113	1
218	331113131	3	282	222312322	3	346	113113313	1
219	231222223	1	283	331223233	3	347	331313133	2
220	113133113	1	284	113221231	3	348	222332322	2
221	122311312	1	285	122331132	2	349	111311311	3
222	313111333	3	286	333221231	2	350	313133331	2
223	111331133	1	287	222132122	1	351	313311113	3
224	331223231	2	288	113111111	1	352	222222222	3
225	322221232	2	289	231222223	1	353	231112123	3
226	222222222	3	290	222332122	1	354	322221212	1
227	122111332	2	291	231332121	1	355	111313131	3
228	222222222	1	292	113223211	3	356	311333311	3
229	311221213	1	293	322221232	3	357	211222221	2
230	331113311	1	294	122223232	1	358	111221213	3
231	211332123	2	295	231222223	2	359	322111112	1
232	222132122	2	296	222222222	3	360	322133332	2
233	233312123	3	297	311131133	3	361	311331131	3
234	322221232	2	298	311133311	2	362	113221233	2
235	213112123	2	299	333311111	3	363	331333311	2
236	231312323	3	300	331111311	2	364	222222222	2
237	222132122	1	301	211332321	1	365	322221212	1
238	333223233	2	302	122111132	1	366	322223212	1
239	313221233	2	303	111331113	3	367	211132121	1
240	111333313	2	304	322111332	3	368	211222223	3
241	333313311	3	305	122311332	1	369	322313332	2
242	231312321	2	306	333133333	2	370	322331132	3
243	213332121	1	307	322333332	1	371	222132322	3
244	311223231	2	308	233222221	2	372	333133113	2
245	313223233	2	309	222222222	2	373	111333333	2
246	133221233	1	310	113333313	3	374	322111312	1
247	131111113	1	311	311133113	1	375	331113313	3
248	213222221	3	312	113221231	2	376	133331113	2
249	211332323	1	313	131111313	3	377	311113311	1
250	122331112	3	314	222222222	1	378	122333312	3
251	222332322	2	315	322221232	2	379	131313313	3
252	331131331	3	316	111111131	3	380	311113331	3
253	122313312	3	317	131311331	2	381	333131333	2
254	113223231	3	318	331113311	2			
255	233312121	2	319	222222222	2			
256	322313112	1	320	222222222	1			

7.2 LINEAR PROGRAMMING SOLUTION METHOD

The process of selecting the proper columns of $A_{2,3}$ to get a constant λ row sum can also be seen as a linear programming problem where the objective function accumulates 3-subspace orbits. Our objective equation in (5.4) was meant to generate a collection of 3-subspace orbits, the maximum number of 3-subspace orbits that can be collected, while ensuring that every 2-subspace was contained in this collection 21 times each.

$$\begin{array}{lll} \text{(i)} & \text{maximize} & f(x) = J \cdot x \\ \text{(ii)} & \text{subject to} & A_{2,3}x^T + s = 21, \\ \text{(iii)} & \text{where} & s = 0, \\ \text{(iv)} & \text{and} & x \in \{0,1\}^n \end{array} \tag{7.1}$$

The non-zero x_i designate the indices of the k-space orbits used to create our collection, which would also be our geometric design, with $u = (x_1, x_2, \ldots, x_{\rho(k)})$ as our solution to (3.1).

7.2.1 Variables for different solutions

GUROBI is deterministic like LLL, and stops once it finds a solution, but if the program is run again with all settings unchanged, the same solution is returned. Settings that can be changed include $A_{2,3}$, the number of threads used, the objective and objective equation, and the types of values that can be used for x_j. For example, the objective can very easily be changed to minimizing the number of 3-subspaces instead. Likewise, the objective equation can changed to count the total number of times any of the 2-subspace orbit representatives in $\begin{bmatrix} V \\ 2 \end{bmatrix}$ appear in a given orbit $\Gamma_i \in \mathcal{K}$. The objective can be concerned with accumulating the lengths of the $\Gamma_j \in \mathcal{K}$. Every Γ_j orbit we use in $A_{2,3}$ is of the same length, but in general not every orbit of k-subspaces used to find geometric designs or large sets need to have the same length. Any of these alterations to the ILP have been confirmed to yield geometric large sets from $A_{2,3}$, as does changing the number of threads used by GUROBI to check nodes, and even just randomly permuting the columns of $A_{2,3}$.

7.2.2 Presenting the linear programming solutions

The two solutions found and expressed on the following page were both found using the format of equation (7.1). The solutions are shown in a similar format to the solutions found by lattice basis reduction. The second solution we found by randomly permuting the columns of $A_{2,3}$, so the solutions found by GUROBI lack the symmetry found in the earlier solutions.

1	11	44	22	87	23	130	23	173	22	216	32	259	21	302	13	345	21
2	21	45	22	88	32	131	33	174	21	217	33	260	32	303	31	346	33
3	32	46	33	89	22	132	11	175	32	218	13	261	33	304	11	347	23
4	21	47	23	90	22	133	21	176	22	219	22	262	22	305	32	348	12
5	22	48	32	91	31	134	31	177	32	220	31	263	13	306	13	349	23
6	13	49	22	92	33	135	31	178	33	221	33	264	11	307	11	350	21
7	21	50	32	93	21	136	23	179	31	222	13	265	33	308	22	351	23
8	23	51	23	94	13	137	32	180	13	223	31	266	33	309	23	352	21
9	11	52	13	95	33	138	21	181	23	224	23	267	32	310	33	353	12
10	31	53	32	96	32	139	31	182	32	225	11	268	32	311	33	354	33
11	21	54	22	97	13	140	23	183	12	226	22	269	21	312	31	355	12
12	32	55	21	98	12	141	12	184	33	227	21	270	13	313	12	356	31
13	12	56	21	99	22	142	21	185	21	228	11	271	22	314	22	357	13
14	32	57	23	100	13	143	11	186	13	229	33	272	13	315	12	358	22
15	21	58	32	101	22	144	11	187	33	230	32	273	13	316	13	359	21
16	32	59	13	102	12	145	32	188	12	231	22	274	13	317	12	360	23
17	12	60	23	103	22	146	32	189	32	232	12	275	21	318	23	361	33
18	32	61	11	104	11	147	22	190	11	233	13	276	31	319	33	362	12
19	32	62	13	105	31	148	12	191	12	234	11	277	22	320	11	363	31
20	33	63	32	106	33	149	22	192	21	235	32	278	23	321	12	364	13
21	13	64	23	107	12	150	21	193	32	236	31	279	12	322	32	365	12
22	21	65	31	108	13	151	12	194	33	237	11	280	21	323	33	366	12
23	23	66	13	109	21	152	12	195	13	238	22	281	22	324	13	367	31
24	23	67	13	110	13	153	21	196	21	239	33	282	12	325	22	368	33
25	12	68	31	111	31	154	12	197	32	240	11	283	31	326	31	369	21
26	13	69	21	112	13	155	32	198	11	241	21	284	23	327	33	370	31
27	33	70	21	113	21	156	21	199	23	242	31	285	12	328	13	371	31
28	12	71	31	114	22	157	12	200	23	243	12	286	12	329	13	372	31
29	32	72	13	115	31	158	33	201	33	244	21	287	21	330	11	373	22
30	11	73	12	116	23	159	13	202	21	245	12	288	21	331	31	374	22
31	31	74	12	117	33	160	12	203	21	246	12	289	23	332	31	375	32
32	33	75	33	118	11	161	12	204	33	247	13	290	32	333	21	376	21
33	13	76	12	119	32	162	32	205	12	248	23	291	31	334	33	377	21
34	11	77	12	120	23	163	11	206	32	249	31	292	13	335	13	378	12
35	21	78	22	121	23	164	32	207	33	250	21	293	12	336	12	379	23
36	11	79	22	122	31	165	32	208	11	251	22	294	11	337	32	380	11
37	11	80	23	123	11	166	13	209	23	252	23	295	23	338	22	381	33
38	13	81	31	124	23	167	11	210	31	253	22	296	21	339	21		
39	33	82	31	125	23	168	33	211	13	254	33	297	21	340	31		
40	33	83	32	126	13	169	12	212	31	255	13	298	31	341	23		
41	11	84	21	127	12	170	32	213	32	256	31	299	21	342	21		
42	33	85	31	128	33	171	23	214	23	257	21	300	12	343	12		
43	32	86	21	129	12	172	21	215	11	258	21	301	13	344	13		

CHAPTER 8

PROVING NON-ISOMORPHISM

Upon finding our 11 large sets, we easily establish that they, together with the large set found in [17] are all distinct. Let $\Lambda = \{\mathcal{L}_0, \mathcal{L}_1, \ldots, \mathcal{L}_{11}\}$ be the 12 large sets discussed above. We now take the time to establish that these 12 large sets are non-isomorphic to each other.

8.1 SINGER SUBGROUPS ARE CONJUGATE IN $GL_8(2)$

Let Θ be the general linear group $GL_8(2)$. Establishing the pairwise non-isomorphism of these large sets requires obtaining the normalizer of our group G in Θ:

$$N_\Theta(G) = \{x \in \Theta \mid xG = Gx\}$$

The normalizer of $G = \langle\alpha\rangle$ in $GL_n(q)$ has order equal to $n(q^n - 1)$ and is the extension of $\langle\alpha\rangle$ by the Frobenius automorphism ζ. The element $\zeta \in \Theta$ can be expressed by the matrix seen below:

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

Checking the list of maximal subgroups of Θ shows that $N = N_\Theta(G)$ is not maximal in Θ. Let $\Phi_8 = \langle\zeta\rangle \leq N$, where $\zeta : \alpha \to \alpha^2$ is the Frobenius subgroup normalizing G. We have checked that Φ_8 does not fix any of the 12 large sets, and does not move any one of the 12 large sets to any other.

The order of a Sylow 17-subgroup in $\Theta = GL_8(2)$ is 17. Thus, since $17|255$, a singer subgroup $S \leq \Theta$ contains a Sylow 17-sugroup P, in fact a unique such subgroup. Since S centralizes P, the order of the centralizer of P in Θ is at least 255. Direct computation with MAGMA, [66], shows that the order of the centralizer of a Sylow 17-subgroup is exactly 255. Thus $C_\Theta(P) = S$.

Lemma 8.1.1. *A Singer subgroup in $GL_n(q)$, is self-centralizing in $GL_n(q)$.*

Proof. $GL_n(q)$ acts faithfully on the $q^n - 1$ non-zero vectors of V. Thus, there is an isomorphic embedding $\phi : GL_n(q) \to \mathcal{S}_{q^n-1}$. Now,

$$\langle\alpha\rangle \;\leq\; C_{GL_n(q)}(\langle\alpha\rangle) \;\leq\; C_{\mathcal{S}_{q^n-1}}(\langle\alpha\rangle) \;=\; \langle\alpha\rangle$$

However, it is known that the centralizer of a cycle of length m in S_m is of order m. Thus, a Singer subgroup in $GL_n(q)$ is self-centralizing. □

Given this information, the following theorem is now established.

Theorem 8.1.1. *All Singer subgroups are conjugate in $\Theta = GL_8(2)$.*

Proof. The order of the centralizer of a Sylow 17-subgroup in Θ is exactly 255. That can be obtained directly from computation with MAGMA. By proposition (2.7.1), since all the Sylow 17-subgroups are conjugate in Θ, so are their centralizers in Θ, thus all Singer subgroups are conjugate. □

It is also known that in general, Singer subgroups in $GL_n(q)$ are conjugate to each other according to statements of various researchers, [38, 30], that the book of B. Huppert, [44] would contain a proof. We could not find an explicit proof of this general fact, though our proof still works for any $GL_n(q)$ with similar conditions related to the factorization of $q^n - 1$.

8.2 AUTOMORPHISM GROUPS OF $\mathcal{L} \in \Lambda$

In this section we establish that the automorphism group of each $\mathcal{L} \in \Lambda$ is the Singer subgroup G.

Lemma 8.2.1. *Θ is not the full automorphism group of any $\mathcal{L} \in \Lambda$.*

Proof. Otherwise, every element of Θ would fix $\mathcal{L}$, contrary to the fact that for each $\mathcal{L} \in \Lambda$ there are elements of $\Theta - G$ that do not fix $\mathcal{L}$. □

Corollary 8.2.1. *For any large set $\mathcal{L} \in \Lambda$, Aut($\mathcal{L}$) must be contained in a maximal subgroup of Θ, containing G.*

Lemma 8.2.2. *For any large set $\mathcal{L} \in \Lambda$, Aut($\mathcal{L}$) is contained in a maximal subgroup of $M \leq \Theta$, where $|M| = 5,922,201,600 = 2^{13}3^{5}5^{2}7^{1}17^{1}$.*

Proof. There are in all 10 conjugacy classes of maximal subgroups of Θ. By order consideration, only 2 of these classes can be of subgroups containing G, namely conjugacy class $\mathcal{M}_2$ consisting of subgroups of order 5,922,201,600, or conjugacy class $\mathcal{M}_3$ consisting of subgroups of order 47,377,612,800. The Sylow 17-subgroups in a maximal subgroup H of class M_3 is self-centralizing in H, while the Sylow 17-subgroups in a maximal subgroup K of class M_2 is centralized by a group of order 255. Therefore, any Singer subgroup is contained in a maximal subgroup of class $\mathcal{M}_2$. □

We presently describe our method of finding a maximal subgroup $H \in \mathcal{M}_2$ containing our Singer cycle α. By using MAGMA we obtain a generic subgroup $Q \in \mathcal{M}_2$. We select a Sylow 17-subgroup $T \leq Q$ and compute the centralizer C of T in Q. We then ask MAGMA to find an element $x \in \Theta$ such that $G^x = C$, then $C^{x^{-1}} = G$, and $Q^{x^{-1}} \supseteq G$. $H = Q^{x^{-1}}$ is a maximal subgroup of Θ containing G.

We exhibit below the generators of H:

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

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

The maximal subgroup H can be proven to be the unique maximal subgroup of Θ that contains G, as ζ is contained in H as well.

Lemma 8.2.3. *Let $M \in \mathcal{M}_2$, and P be a Sylow 17-subgroup of M. Then $C_M(P)$ is a Singer subgroup of order 255, and $|N_M(P)| = 2040$, therefore, there is a unique maximal subgroup $M \in \mathcal{M}_2$ containing G.*

Proof. Let $M \in \mathcal{M}_2$ and P be a Sylow 17-subgroup of M. Then, $C_M(P)$ is a Singer cycle S, and $N_M(P) = N_M(S) = N_\Theta(S) = S \cdot \Phi_8$. Let G be our particular Singer subgroup, and let $M, M' \in \mathcal{M}_2$ containing G. Then there exists $g \in \Theta$ such that $G^g = G$ and $M^g = M'$. Hence, $g \in N_\Theta(G) \leq M$, therefore $M' = M^g = M$. □

If $t \in H$ is an automorphism of $\mathcal{L} \in \Lambda$, then the complete coset tG consists of automorphisms of $\mathcal{L}$, so the full automorphism group of $\mathcal{L}$ is a union of cosets of G in H. To determine the full automorphism group of $\mathcal{L}$, it suffices to run through a set of left coset representatives of G in H.

Lemma 8.2.4. *Let $\mathbb{D}$ be the collection of all designs that appear in the 12 large sets. For each $\mathcal{D} \in \mathbb{D}$ we have that* $\mathrm{Aut}(\mathcal{D}) = G$.

Proof. The maximal subgroup H containing G acts transitively on the 255 non-zero vectors of V because G is transitive on the nonzero vectors. Let H_1 be the stabilizer in H of vector 1, then $|H_1| = |H|/255$. Note that since G is *regular* on the 255 non-zero vectors, $H_1 \cap G = \{1\}$, and we have:

$$|H_1 G| = \frac{|H_1| \cdot |G|}{|H_1 \cap G|} = (\frac{|H|}{255} \cdot 255)/1 = |H|,$$

Therefore the elements of H_1 constitute a collection of left coset representatives of G in H. Running computationally through all elements of $H_1 - \{1\}$ we verify that none of these elements is an automorphism of any $\mathcal{D} \in \mathbb{D}$. □

Lemma 8.2.5. *If $\mathcal{L} \in \Lambda$ and Q is the full group of automorphisms of $\mathcal{L}$, then Q fixes the designs of $\mathcal{L}$ and $Q = G$.*

Proof. Let $\mathcal{L} = \{\mathcal{D}_1, \mathcal{D}_2, \mathcal{D}_3\}$, and $Q_{[L]}$ be the subgroup of Q that fixes each of the designs $\{\mathcal{D}_1, \mathcal{D}_2, \mathcal{D}_3\}$. Then $G = Q_{[L]} \trianglelefteq Q$ and $Q/Q_{[L]}$ is a subgroup $T \leq \mathcal{S}_3$. In fact, Q is a split extension of $Q_{[L]}$ by T, because clearly $Q_{[L]} \cap T = \{1\}$. But an element of order 2 in T would have to fix one of the three designs, which is a contradiction because 2 does not divide the order of G. Also, an element of order 3 in T cannot normalize $Q_{[L]}$ as the only elements of order 3 in $N_\Theta(G) = \langle\alpha\rangle \cdot \langle\zeta\rangle$ are in $G = \langle\alpha\rangle$, which fix each design. □

8.3 PROVING NON-ISOMORPHISM

An important theorem of A. Betten, R. Laue, and A. Wassermann in [9] was eventually used to aid us in determining whether the large sets we found were isomorphic to one another.

Theorem 8.3.1. *Let G be a finite group acting on a set X. Suppose that $x_1, x_2 \in X$ and $g \in G$ such that $x_1^g = x_2$. Moreover, suppose that a Sylow p-subgroup P of G is contained in both stabilizers G_{x_1} and G_{x_2}. Then $x_1^n = x_2$ for some $n \in N_G(P)$.*

Proof. Suppose that for $x_1, x_2 \in X$, and $g \in G$, $x_1^g = x_2$. Recall that by lemma (2.7.1), $G_{x_2} = G_{x_1^g} = (G_{x_1})^g$. By the hypothesis, P is a Sylow p-subgroup of both G_{x_1} and G_{x_2}. Since P is a Sylow p-subgroup of G_{x_1}, P^g is a Sylow p-subgroup of $(G_{x_1})^g = G_{x_2}$. Since P and P^g are both Sylow p-subgroups of G_{x_2}, they are conjugate in G_{x_2}. Thus, there exists some $h \in G_{x_2}$ such that $P^h = P^g$. This is equivalent to $P = P^{gh^{-1}}$, but this in turn implies that $gh^{-1} \in N_G(P)$. Now, let $n = gh^{-1}$, then, since $x_1^g = x_2$ and $h^{-1} \in G_{x_2}$, we have
$x_1^n = x_1^{gh^{-1}} = (x_1^g)^{h^{-1}} = x_2^{h^{-1}} = x_2$, with $n \in N_G(P)$. □

The above theorem is clearly a variant of Frattini's argument. From this theorem we can immediately prove that the 12 large sets in Λ are non-isomorphic, where $\mathcal{L}_0$ is the large set found by [17]. Recall that we have verified using APL that no element in the Frobenius automorphism $\Phi_8 = \langle\zeta\rangle$ maps any of the 12 large sets to any other or to themselves.

Corollary 8.3.1. *The 12 large sets in Λ are pairwise non-isomorphic.*

Proof. Let X be the collection of all large sets of type $LS[3][2, 3, 2^8]$, and $G = \langle\alpha\rangle$ be the Singer subgroup defined earlier. Θ acts on X, and for any $\lambda \in X$ the stabilizer Θ_λ is the full automorphism group of λ. For each $\lambda \in \Lambda$ we have that $P < G \leq \Theta_\lambda$ where P is the Sylow-17 subgroup of G. Let $\lambda, \mu \in \Lambda$, $\lambda \neq \mu$, and suppose there is $g \in \Theta$ such that $\lambda^g = \mu$. Then by Theorem (8.3.1), there must exist an element $n \in N_\Theta(P) = N_\Theta(G)$ such that $\lambda^n = \mu$. However, $N_\Theta(G) = \langle\alpha\rangle \cdot \langle\zeta\rangle$, so $n = \alpha^i \cdot \zeta^j$, and $\lambda^n = \lambda^{\alpha^i \cdot \zeta^j} = \lambda^{\zeta^j}$. But this is a contradiction since we know that no element of Φ_8 sends any large set of Λ to any other. □

Since all Singer cycles are conjugate in Θ, any other Singer cycle would yield completely analogous and equivalent results.

CHAPTER 9

FUTURE PROBLEMS

Lattice basis reduction and ILP are both methods of finding geometric designs that can be used on other sets of feasible parameters. Creation of the $A_{t,k}$ matrix for the purposes of finding geometric designs has variations as well that can aid in finding other geometric designs and large sets. The use of a different G by use of the entire normalizer of a given Singer subgroup or even any subgroup of the normalizer can yield different $A_{t,k}$ matrices. It has also been proven that if $n \leq 3$ and q are prime, then any nontrivial q-Steiner systems that contain the normalizer of a Singer subgroup in $GL_n(q)$ are nonisomorphic, [15]. $2-[2^n, 3, \lambda]$ geometric designs have been found for various λ for $n = 6, 7, 8, 9, 10$, as well as $2-[2^n, 4, \lambda]$ designs for $n = 8, 9$, and $2-[3^n, 3, \lambda]$ for $n = 6, 7, 8$, [18]. In particular, geometric designs with $t > 2$ were found with parameters $3-[2^9, 4, 11]$ and $3-[2^9, 4, 15]$, [18], all of these found with lattice basis reduction using Singer subgroups for G, or using subgroups of the normalizer of Singer subgroups.

We present a series of tables for fixed values of q, t, and N that indicate whether an $LS[N][t, k, q^n]$ large set is admissible and can exist (as indicated by a question mark), is realizable and have been proven to exist (as indicated by a value of k), or cannot exist (as indicated by a dash), with each row representing a different value for n. Admissible geometric large set parameters satisfy the necessary divisibility conditions for the constituent designs to exist, each of which have $\lambda = \begin{bmatrix} n-t \\ k-t \end{bmatrix} / N = \lambda_{max}/N$. Kiermaier and Laue's recursive combinations for large sets of the same t, [48], can explain the recursive admissibility of these parameters. A recursive relation appears on these tables due to the fact that when the

parameters for an $LS[N][t, k, q^n]$ and $LS[N][t, k+1, q^n]$ large set satisfy the necessary conditions to exist, then the admissibility of its constituent designs imply the admissibility of the constituent designs of an $LS[N][t, k+1, q^{n+1}]$ as well. These tables include parameters that belong to a family of geometric large sets that have been proven to exist by recursive combinations such as those found in the work of Braun et al., [16]. The tables can be found in the appendix.

Geometric designs were discovered by computer construction in [18] using group actions on various $G \leq \langle \alpha, \zeta \rangle$. α, ζ represent Singer cycles and Frobenius automorphisms respectively on various dimensions. Using (3.2.1), $A_{2,4}$ was created from $A_{2,3}$ and $A_{3,4}$ using the same Singer subgroup $\langle \alpha \rangle$ for group action orbits, though GUROBI has returned no solutions to (3.1).

We have found a number of the confirmed geometric designs found by [18], including a solution to (3.1) for $A_{2,4}$ where $\lambda = 105$, and where G was the normalizer of α in $GL_8(2)$. We have not yet found large sets with the dimensions $LS[N][2, 4, 2^8]$, and unfortunately 105 does not divide the maximum value of $\lambda = 651$. Thus the geometric design we have found cannot be a constituent design of a large set with these parameters. Other geometric designs have been found that may or may not be constituent designs for large sets. We have also found 2-$[2^6, 3, 6]$ and 2-$[2^6, 3, 3]$ designs, which GUROBI has deemed are not constituent designs of large sets. All geometric designs of 2-subspaces in 3-subspaces must have λ divisible by 3, and all $LS[N][2, 3, 2^6]$ large sets have constituent designs with λ dividing 15. 6 does not divide 15, and despite the fact that 3 does, GUROBI has still deemed that it is infeasible to find $LS[5][2, 3, 2^6]$ using $\langle \alpha^7 \rangle$. We are still in the process of trying to find large sets with other G in these dimensions.

GUROBI and lattice basis reduction have also been used to try to prove the existence of $LS[3][3, 4, 2^9]$ large sets. Exhaustive search with GUROBI has not returned any solutions to (3.1) where $\lambda = 21$. Other recursive methods for finding

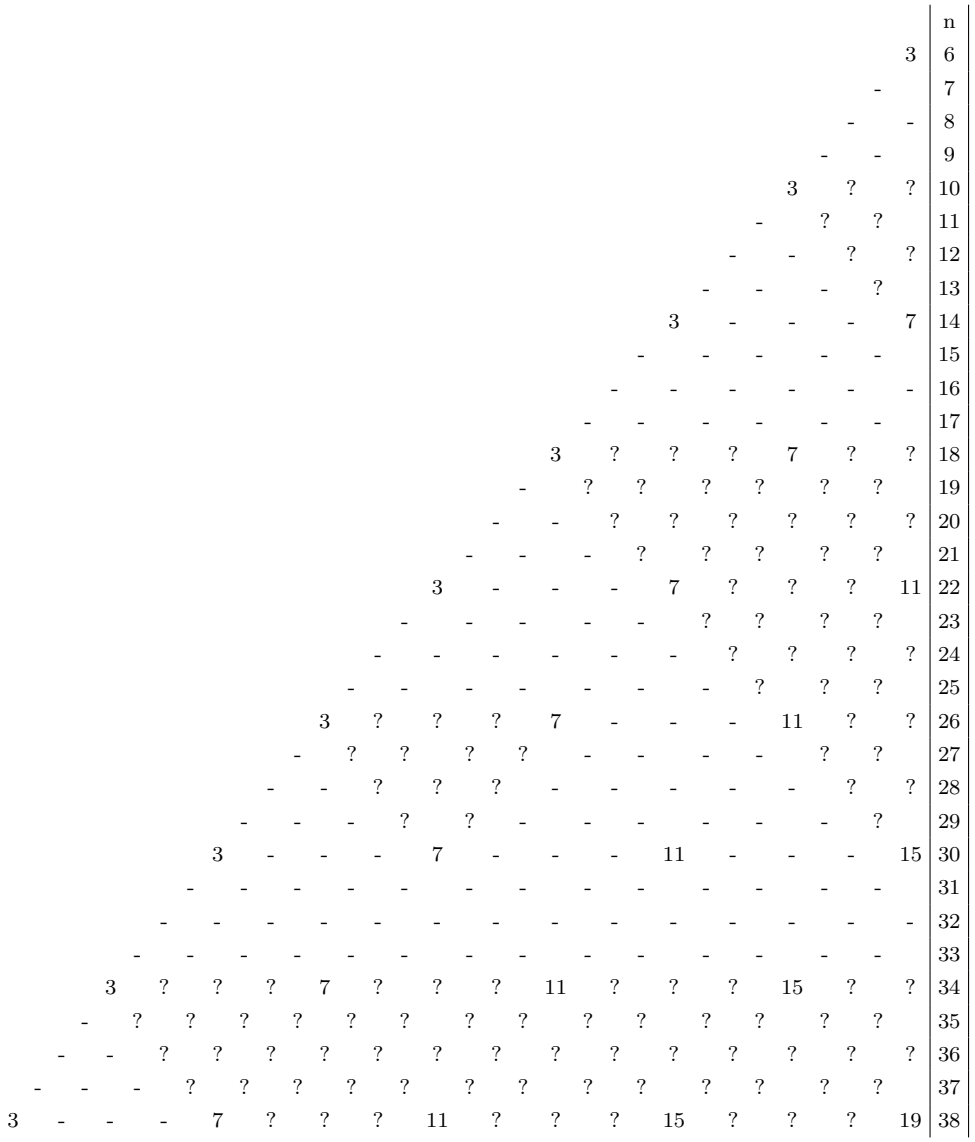
designs are also being explored and used, such as the recent methods of Trang Van Trung, [78]. Designs in a v-set V can be found by partitioning V into two sets of v_1 and v_2 elements, and searching for $t-(v_1, s, \lambda_s)$ and $t-(v_2, k-s, \lambda_{k-s})$ designs within each subset for $0 \leq s \leq k$. After the designs are found, blocks within designs for each pair of designs $t-(v_1, s, \lambda_s)$ and $t-(v_2, k-s, \lambda_{k-s})$ are adjoined together and are verified to be designs by whether or not the resulting adjoining of blocks result in the same λ for every pair of designs.

CHAPTER 10

APPENDIX

Admissibility and Realizability of $LS[3][2, k, 2^n]$

																																			n
																																		-	6
																																	-		7
																																3		?	8
																															-		?		9
																														-		-		?	10
																													-		-		-		11
																												-		-		-		-	12
																											-		-		-		-		13
																										?		?		?		-		-	14
																									-		?		?		-		-		15
																								-		-		?		-		-		-	16
																							-		-		-		-		-		-		17
																						-		-		-		-		-		-		-	18
																					-		-		-		-		-		-		-		19
																				?		?		?		?		?		?		?		?	20
																			-		?		?		?		?		?		?		?		21
																		-		-		?		?		?		?		?		?		?	22
																	-		-		-		?		?		?		?		?		?		23
																-		-		-		-		?		?		?		?		?		?	24
															-		-		-		-		-		?		?		?		?		?		25
														?		?		?		-		-		-		?		?		?		?		?	26
													-		?		?		-		-		-		-		?		?		?		?		27
												-		-		?		-		-		-		-		-		?		?		?		?	28
											-		-		-		-		-		-		-		-		-		?		?		?		29
										-		-		-		-		-		-		-		-		-		-		?		?		?	30
									-		-		-		-		-		-		-		-		-		-		-		?		?		31
								?		?		?		-		-		-		?		?		?		-		-		-		?		?	32
							-		?		?		-		-		-		-		?		?		-		-		-		-		?		33
						-		-		?		-		-		-		-		-		?		-		-		-		-		-		?	34
					-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		35
				-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-	36
			-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		-		37
		?		?		?		?		?		?		?		?		?		?		?		?		?		?		?		-		-	38
	-		?		?		?		?		?		?		?		?		?		?		?		?		?		?		-		-		39
-		-		?		?		?		?		?		?		?		?		?		?		?		?		?		-		-		-	40


n
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38

Admissibility and Realizability of $LS[3][3, k, 2^n]$

															n
														-	8
												?			9
										-			?		10
								-			-				11
						-			-						12
				-			-			-					13
		-			-			-							14
	?			?			?			?					15
-			?			?			?			-			16

Admissibility and Realizability of $LS[5][2, k, 3^n]$

															n
														?	6
										-					7
								-			-				8
						-			-						9
				?			?			-					10
		-			?			-							11
	-			-			-			-					12

BIBLIOGRAPHY

[1] R. Ahlswede, H. K. Aydinian, and L. H. Khachatrian, *On Perfect Codes and Related Concepts*, Designs, Codes Crypto., 22 (2001), pp. 221-237.

[2] S. Ajoodani-Namini and G.B. Khosrovshahi, *Combining t-Designs*, J. Comb. Th., 58 (1991), pp. 26-34.

[3] S. Ajoodani-Namini, *Extending Large Sets of t-Designs*, J. Comb. Th., A 76, (1996), pp. 139-144.

[4] W.O. Alltop, *An infinite class of 4-designs*, J. Comb. Th., A 6 (1969), pp. 320-322.

[5] W.O. Alltop, *An infinite class of 5-designs*, J. Comb. Th., A 12 (1972), pp. 390-395.

[6] W. O. Alltop, *Extending t-Designs*, J. Comb. Th., A 18, (1975), pp. 177-186.

[7] R. D. Baker, *Partitioning the Planes of $AG_{2m}(2)$ into 2-Designs*, Discrete Mathematics, 15 (1976), pp. 35-40.

[8] J. A. Barrau, *Over drietalstelsels, in het bijzonder die van dertien elementen*, Kon. Akad. Wetensch. Amst. Verslag Wis-en Natuurk. Afd., 17, (1908) pp. 274-279.

[9] A. Betten, R. Laue, A. Wassermann, *Simple 7-designs with Small Parameters*, J. Comb. Designs, 7 (1999), pp. 79-94.

[10] A. Beutelspacher, On Parallelisms of Finite Projective Spaces, Geometriae Dedicata, 3 (1974), pp. 35-40.

[11] R. C. Bose and S. S. Shrikhande, *On the Falsity of Euler's Conjecture about the Non-Existence of Two Orthogonal Latin Squares of Order 4t+2*, Proc. Nat. Acad. Sci. U.S.A., 45 (1959), pp. 734-737.

[12] R.C. Bose, and D. M. Mesner, *On linear associative algebras corresponding to association schemes of partially balanced designs*, Ann. Math. Stat. **30** (1959), pp 21-38.

[13] R. C. Bose, S. S. Shrikhande, and E. T. Parker, *Further Results on the Construction of Mutualy Orthogonal Latin Squares and the Falsity of Euler's Conjecture*, Canad. J. Math., 12 (1960), pp. 189-203.

[14] V. Boyer, M. Elkihel, D. El Baz, *Heuristics for the 0-1 multidimensional knapsack problem*, European Journal of Operational Research, 199 (2009), pp. 658-664.

[15] M. Braun, T. Etzion, P. J. R. Östergard, A. Vardy, and A. Wassermann, *Existence of q-Analogs of Steiner Systems*, submitted 2013.

[16] M. Braun, M. Kiermaier, A. Kohnert, and R. Laue, *Large Sets of Subspace Designs*, arXiv:1411.7181, 2014.

[17] M. Braun, A. Kohnert, P. Östergard, A. Wassermann, *Large Sets of t-Designs over Finite Fields*, JCTA 124 (2014), pp. 195-202.

[18] M. Braun, A. Kerber, and R.Laue, *Systemic Construction of q-Analogs of Designs*. Designs, Codes, and Cryptography, 34 (2005), pp. 55-70.

[19] P.J. Cameron, *Generalization of Fisher's Inequality to Fields with More than One Element*, in T. McDonough and V. Mavron, Eds., Combinatorics, London Math. Soc. LNS, 13 (1974), pp. 9-13.

[20] P. J. Cameron, *Locally Symmetric Designs*, Geometriae Dedicata, 3 (1974), pp. 65-76.

[21] Y. M. Chee and S. S. Magliveras, *A Few More Large Sets of t-Designs*, J. Comb. Designs, 6 (1998), pp. 293-308.

[22] C.J. Colbourn, J.H. Dinitz, D.R. Stinson, *Applications of Combinatorial Designs to Communications, Cryptography, and Networking*, (1999), pp. 1-63.

[23] J. H. Conway, *A Perfect Group of Order 8,315,553,613,086,720,000 and the Sporadic Simple Groups*, Proceedings of the National Academy of Sciences of the United States of America, 61 (2) (1968), pp. 398-400.

[24] C. Cusack, S. Magliveras, *Semiregular Large Sets*, Designs, Codes, and Cryptography, 18, (1999), pp. 81-87

[25] P. Delsarte, *Association Schemes and t-Designs in Regular Semilattices*, JCTA 20 (1976), pp. 230-243.

[26] R. H. F. Denniston, *Some New 5-Designs*, Bull. London Math. Soc., 8 (1976), pp. 263-267.

[27] R. H. F. Denniston, *On Biplanes with 56 Points*, Ars Combin., 9 (1980), pp. 167-179.

[28] T. Etzion and A. Vardy, *Error-correcting codes in projective space*, IEEE Trans. Inform. Theory 57 (2011), pp. 1165-1173.

[29] A. Fazeli, Sh. Lovett, and A. Vardy, *Nontrivial t-designs over finite fields exist for all t*, arXiv:1306.2088v1, June (2013), pp. 1-12

[30] S. R. Ghorpade, S. U. Hasani and M. Kumari, *Primitive Polynomials, Singer Cycles and Word-Oriented Linear Feedback Shift Registers*, Designs, Codes and Cryptography, 58 (2), (2011), pp. 123-134.

[31] L. Gilman and A. Rose, *A.P.L.: Interactive Approach, Third Edition*, (1983)

[32] N.A. Gordon, T.M. Jarvis, and R. Shaw, *Some Aspects of the Linear Groups GL(n,q)*, (2003), pp. 1-30. Available at http://www.hull.ac.uk/maths/people/rs/staffdetails.html.

[33] gurobi Optimization Inc., gurobi *Optimizer Reference Manual*, 2015, http://www.gurobi.com.

[34] H. Hanani, *On Quadruple Systems*, Can. J. Math., 12 (1960), pp. 145-157.

[35] H. Hanani, *The Existence and Construction of Balanced Incomplete Block Designs*, Ann. Math. Stat., 32 (1961), pp. 361-386.

[36] H. Hanani, A. Hartman and E. S. Kramer, *On three-designs of small order*, Discrete Math, 45 (1983), pp.75-97.

[37] A. Hedayat, S. Kageyama, *The family of t-designs- part I*, Journal of Statistical Planning and Inference, 4 (2), (1980), pp. 173-212.

[38] M. D. Hestenes, *Singer Groups*, Canadian Journal of Mathematics, 22 (3), (1970), pp. 492-513.

[39] D. G. Higman, *Finite permutation groups of rank 3*, Math. Z. **86** (1964), pp. 145-156.

[40] D. G. Higman, *Intersection matrices for finite permutation groups*, J. Algebra **6** (1967), pp. 22-42.

[41] D. G. Higman, *Coherent algebras*, Linear Algebra Appl. **93** (1987), pp. 209-239.

[42] X. Hubaut, *Two New Families of 4-Designs*, Discrete Math., 9 (1974), pp. 247-249.

[43] D. Hughes, *On t-designs and groups*, Amer. J. Math. 87 (1965) pp. 761-778.

[44] B. Huppert, *Endliche Gruppen I*, Springer-Berlag, (1967).

[45] T. Itoh, *A New Family of 2-Designs over GF(q) Admitting* $SL_m(q^l)$, Geometriae Dedicata, 69 (1998), pp. 261-286.

[46] K. Iverson, *A Programming Language*, Wiley, (1962)

[47] P. Keevash, *The Existence of Designs*, arXiv:1401.3665.

[48] M.L Kiermaier and R. Laue, *Derived and Residual Subspace Designs*, Advances in Mathematics of Communication, 9 (2015), pp. 105-115

[49] T. P. Kirkman, *Query VI*, Lady's and Gentlemen's Diary, (1850) 48.

[50] T. P. Kirkman, *On the Triads Made with Fifteen Things*, London, Edinburgh and Dublin Philo. Mag. and J. Sci., 37 (1850) pp. 169-171.

[51] M. H. Klin, *On some classes of permutation groups, preserving relations*, Ph.D. thesis, under Prof. L.A. Kaluznin, Kiev State Univ., 1975.

[52] R. Koetter and F. Kschischang, *Coding for Errors and Erasures in Random Network Coding*, IEEE Transactions on Information Theory, 54 (2008), pp. 3579-3591.

[53] E. Kramer and D. Mesner, *t-Designs on Hypergraphs*, Discr. Math. 15 (3) (1976), pp. 263-296.

[54] E. Kramer, D. Leavitt and S. Magliveras, *Construction Procedures for t-designs and the Existence of New Simple t-designs*, Annals of Discr. Math. 26 (1985), pp. 247-274.

[55] D. L. Kreher and S. P. Radziszowski, *The Existence of Simple 6-(14,7,4) Designs*, J. Combin. Theory, A 43 (1986), pp. 237-243.

[56] D. L. Kreher, *t-Designs, $t \geq 3$, the CRC Handbook of Combinatorial Designs, Ed. C.J. Colbourn & J.H. Dinitz*, CRC Press (1995) pp. 47 - 66.

[57] D. L. Kreher and D. R. Stinson, *Combinatorial Algorithms: generation, enumeration and search*, CRC Press (1999) pp.viii - 329.

[58] G. Kuperberg, S. Lovett and R. Peled, *Probabilistic existence of regular combinatorial structures*, arXiv:1302.4295v2, October (2013), pp. 1-44.

[59] R. Laue, S. S. Magliveras, A. Wassermann, *New Large Sets of t-Designs*, JCD 9 (2001), pp. 40-59.

[60] J. Leech, *Notes on Sphere Packings*, Canadian Journal of Mathematics, 19 (1967), pp. 251-267

[61] A. K. Lenstra, H. W. Lenstra Jr., and L. Lovász, *Factoring Polynomials with Rational Coefficients*, Mathematische Annalen, 261 (1982), pp. 515-534.

[62] G. Lunardon, On Regular Parallelisms in $PG(3, q)$, Discrete Mathematics, 51 (1984), pp. 229-235.

[63] S. S. Magliveras, *The maximal subgroups of the Higman-Sims simple group*, Ph.D. thesis, under Prof. D. L. Livingstone, University of Birngham, England, 1970.

[64] S. S. Magliveras and D. W. Leavitt, *Simple 6-(33,8,36) Designs from $P\Gamma L_2(32)$, Computat. Group Theory, Proceedings of the London Math. Soc. Symposium on Computational Group Theory*, Academic Press, (1984), pp. 337-352.

[65] S. S. Magliveras and T.E. Plambeck, *New infinite families of simple 5-designs*, J. Combin. Theory, A 44, (1987), pp. 1-5.

[66] J. Cannon and C. Playoust, magma: A new computer algebra system, Euromath Bull., 2 (1996), pp. 113-144.

[67] M. Miyakawa, A. Munemasa, and S. Yoshiara, *On a Class of Small 2-Designs over GF(q)*. J. of Combinatorial Designs, 3 (1995) 61-77.

[68] T. Penttila and B. Williams, Regular Packings of $PG(3, q)$, European Journal of Combinatorics, 19 (1998), pp. 713-720.

[69] J. Plücker, *System der analytisechen Geometrie: Auf neue Betrachtungsweisen gegründet, und insbesondere eine ausführliche Theorie der Curven dritter Ordnung enthaltend*, Duncker and Humblot, Berlin, 1835.

[70] J. Plücker, *Theorie der algebraischen Curven: Gegründet auf eine neue Behandlungsweise der analytischen Geometrie*, Marcus, Bonn, 1839.

[71] D. K. Ray Chaudhuri and E. J. Schram, *A Large Set of Designs on Vector Spaces*, Journal of Number Theory, 47 (1994) 247-272.

[72] F. S. Roberts, *Applied Combinatorics*, Prentice-Hall, 1984.

[73] H. Suzuki, *2-Designs over GF(q)*, Graphs and Combinatorics, 8 (1992), pp. 381-389.

[74] L. Teirlinck, *Non-Trivial t-Designs without Repeated Blocks Exist for All t*, Discrete Mathematics, 65 (1987), pp. 301-311.

[75] L. Teirlinck, *Locally Trivial t-Designs and t-Designs without Repeated Blocks*, Discrete Mathematics, 77 (1989), pp. 345-356.

[76] S. Thomas, *Designs over Finite Fields*, Geometriae Dedicata, 24 (1987), pp. 237-242.

[77] T. V. Trung, *On the existence of an infinite family of simple 5-designs*, Math. Zeitschr. 187 (1984), pp. 285-287.

[78] T. V. Trung, *Simple t-designs: A recursive construction for arbitrary t*, Design Codes and Cryptography, February 2016.

[79] F. Wettl, *On Parallelisms of Odd-Dimensional Finite Projective Spaces*, Proceedings of the Second International Mathematical Miniconference part II (Budapest, 1988), Period Polytech, Transportation Energy, 19 (1-2) (1991), pp. 111-116.

[80] R. M. Wilson, *The necessary conditions for t-designs are sufficient for something*, Utilitas Mathematica 4 (1973), pp. 207-215.

[81] E. Witt, *Uber steinersche systeme*, Abh. Math. Sem. Univ. Hamburg, 12 (1938), pp. 265-275.

[82] E. Witt, *Die 5-fach transitiven gruppen von Mathieu*, Abh. Math. Sem. Univ. Hamburg, 12 (1938), pp. 256-265.

[83] Q. R. Wu, *A Note on Extending t-Designs*, Australas. J. Combin., 4 (1991), pp. 229-235.