STRUCTURAL PROPERTIES OF HADAMARD DESIGNS

by

ERIC MERCHANT

A DISSERTATION

Presented to the Department of Mathematics
and the Graduate School of the University of Oregon
in partial fulfillment of the requirements
for the degree of
Doctor of Philosophy

June 2005

"Structural properties of Hadamard designs," a dissertation prepared by Eric Merchant in partial fulfillment of the requirements for the Doctor of Philosophy degree in the Department of Mathematics. This dissertation has been approved and accepted by:

Dr. William Kantor, Chair of the Examining Committee

Date

Committee in charge:
Dr. William Kantor, Chair
Dr. Jon Brundan
Dr. Arkady Berenstein
Dr. Hal Sadofsky
Dr. Eugene Luks

Accepted by:

Dean of the Graduate School

An Abstract of the Dissertation of

Eric Merchant for the degree of Doctor of Philosophy

in the Department of Mathematics to be taken June 2005

Title: STRUCTURAL PROPERTIES OF HADAMARD DESIGNS

Approved: _____

Dr. William Kantor

This dissertation focusses on structural properties of Hadamard designs. These are designs obtained from Hadamard matrices, which have been crucial objects of combinatorial study for over 100 years. The structural properties of interest are: lines, colines, good points and good blocks. These properties have a geometric flavor, and allow us to apply ideas from finite geometry. We also closely examine constructions such as the "doubling" construction of Todd and the "tensor product" construction. By combining the geometrical information with properties of these constructions, we prove our two main results:

1. Given the existence of a Hadamard design of order n, we derive an exponential lower bound for the number of non-isomorphic Hadamard designs of order $2n$.

2. Given a finite group G, we construct an infinite family of Hadamard designs with full automorphism group isomorphic to G.

ACKNOWLEDGEMENTS

First and foremost, I want to thank Dr. Bill Kantor for his guidance, and for the wisdom, humour and passion he has brought to the advising process. I've known Bill since he first taught me how to take a determinant 11 years ago, and he has guided me through an assortment of wonderful mathematics ever since.

I owe an unpayable debt of gratitude to my fiancee Stephenie Frank. Without her support and patience, I never would have gotten this far.

To my family and friends (you know who you are), thank you for the love, support and laughter.

CURRICULUM VITA

NAME OF AUTHOR: Eric Merchant

PLACE OF BIRTH: Plymouth, MA, U.S.A.

DATE OF BIRTH: January 16, 1974

GRADUATE AND UNDERGRADUATE SCHOOLS ATTENDED:

University of Oregon

DEGREES AWARDED:

Doctor of Philosophy in Mathematics, 2005, University of Oregon
Master of Science in Mathematics, 2000, University of Oregon
Bachelor of Arts in Mathematics, 1996, University of Oregon

AREAS OF SPECIAL INTEREST:

Combinatorics
Design Theory
Permutation Groups

PROFESSIONAL EXPERIENCE:

Graduate Teaching Assistant, Department of Mathematics, University of Oregon, 1999 - 2005

AWARDS AND HONORS:

Johnson Award, 2002

TABLE OF CONTENTS

CHAPTER I

INTRODUCTION

I.1. Motivation and Background

Design theory occupies a central position in modern combinatorics, as designs relate to many other combinatorial objects. This thesis is concerned with Hadamard designs, related to Hadamard matrices.

Hadamard matrices are ± 1 matrices whose rows are mutually orthogonal. They are called "Hadamard" as they attain the following upper bound established by Hadamard in 1892 [2, p. 59]: For any complex $n \times n$ matrix A with rows $a_1, \ldots, a_n$, $|\det A| \leq |a_1| \cdots |a_n|$. It is elementary to see that the order of a Hadamard matrix is either $1, 2$ or divisible by 4. The Hadamard conjecture states that a Hadamard matrix of order $4n$ exists for every positive integer n. This conjecture has been the subject of much work in the last hundred years, so much so that a recent Mathscinet search on keywords"Hadamard matrix" generates almost 1,000 matches. It has been shown that the set of integers n satisfying the conjecture is of positive density [21]. By contrast, we are concerned with different questions, focusing on the internal *structure* of the combinatorial designs associated with Hadamard matrices. Therefore, although none of the designs constructed in this dissertation have new

parameters, they do possess properties previously unseen among Hadamard designs.

This dissertation is organized as follows: Section II.1 introduces the terminology and objects of study. Section II.2 describes geometrical invariants, namely *lines* and *colines*. Hadamard designs have the nice property that a line through 2 points (or a coline through 2 blocks) has size 2 or 3. When all lines through a point have size 3, the point is *good*, and we define *good* blocks similarly. The number of good points or blocks is an invariant of the design. Utilizing this invariant enables us to quickly rule out isomorphisms between designs, as well as get a handle on the action of the automorphism groups of the designs. The crucial theorems in Section II.2 present relationships between goodness, the automorphism group of a design, and decomposition into sub–designs.

Chapter III analyzes structural properties associated with some constructions of Hadamard designs. Section III.1 deals with a now standard technique for doubling the order of a Hadamard design. Structural properties of the affine version of this construction have been described in [15, 16], and this Section presents much of that analysis for the symmetric designs. Also, we investigate properties which rely on the duality intrinsic to symmetric designs. Crucially, we characterize the automorphism groups of the "doubled" designs, which has a lovely expression in terms of the intersection of conjugacy classes of subgroups of symmetric groups.

Section III.2 deals with the previously unstudied tensor product of designs, which corresponds to the tensor (or Kronecker) product of the associated matrices. Designs

constructed in this manner have a rich line and coline structure, which distinguishes them from many other Hadamard designs, especially those constructed in Section III.1. The Section concludes with a "unique decomposition" theorem III.2.14, essentially a strong "Krull–Schmidt" theorem which shows that, under suitable conditions, a "tensor factorization" must be unique. This uniqueness provides explicit information about the automorphism group of such a design in terms of the "factor" sub–designs.

Chapter IV proves the following:

Theorem IV.0.1 *If a Hadamard design of order n exists, then the number of non-isomorphic Hadamard designs of order $2n$ is at least*

$$\frac{(4n-1)!}{2^{10}n^3(n!)^4} > 2^{8n-16-7\log n}.$$

This is done in a somewhat roundabout way. First, Section IV.1 proves the Theorem in the special case when a Hadamard design of order n *with no good blocks* exists. Then, Section IV.2 uses the doubling procedure of Section III.1 to show that given any Hadamard design of order $n > 2$, there exists a Hadamard design with the same parameters and *no good blocks*, therefore proving Theorem IV.0.1 in its full generality.

Theorem IV.0.1 is reminiscent of results in [14], where it is shown that, given a Hadamard design $\mathcal{D}$ of order n with no good blocks such that $\mathrm{Aut}(\mathcal{D}^+) = 1$, the are at

least $(4n-1)!$ non–isomorphic Hadamard designs of order $2n$. Designs $\mathcal{D}$ with those properties are constructed for $n = 6, 7, 8, 9$ and 10 in Section 4.4 of [14]. Additionally, [14, Theorem 3.10] states that, if $4n-1 = p^f > 11$ is a power of a prime p and n is odd, then the number of non-isomorphic Hadamard $2-(8n-1, 4n-1, 2n-1)$ designs is at least $(4n-1)!/(f(4n-1)(2n-1))^2$. This is an improvement on a previous lower bound, in [13, Theorem 4.1]. Our Theorem is in the same vein as these results, but makes no assumption about the parameter n, other than the existence of a Hadamard design of order n.

Chapter V exploits the information about automorphism groups given in Section III.1. As we shall see, Theorem IV.0.1 motivates the search for Hadamard designs with small automorphism groups. With that in mind, Section V.1 concludes with the proof of a technical but useful result:

Theorem V.1.1 *If a Hadamard design of order $n > 2$ exists, there exist at least $\frac{(16n-2)!}{2^{10}n^3}$ pairwise non–isomorphic, tensor–indecomposable Hadamard designs of order $8n$ with exactly one good block, no good points, and no non–trivial automorphisms.*

Finally, Section V.3 shows that the class of Hadamard designs is "G – universal" in the language of [1], i.e. given any finite group G, we construct a Hadamard design having full automorphism group isomorphic to G. In the case of classical parameters (i.e., when the order n of the design is a power of 2), this resembles [8], which shows

that, for any finite group G, and any $q \geq 3$, for all sufficiently large d there exists a symmetric design with the parameters of $PG(d, q)$ and with full automorphism group isomorphic to G. This paper establishes the corresponding theorem when $q = 2$. In fact, we obtain a significantly stronger result:

Theorem V.3.3 *Given a finite group G and the existence of a Hadamard design of order $n > 2$, then for all $N > 4|G|+2$, there exist at least $\frac{(16n-2)!}{2^{10}n^3}$ non–isomorphic Hadamard designs $\mathcal{D}$ of order $2^{3N+4}n$ with Aut($\mathcal{D}$) $\cong G$.*

CHAPTER II

PRELIMINARIES

II.1. Basic Definitions

A *design* $\mathcal{D}$ with parameters $t-(v,k,\lambda)$ is an incidence structure $(\mathcal{P},\mathcal{B})$ (so elements of $\mathcal{B}$ are subsets of $\mathcal{P}$) satisfying the following conditions:

- $|\mathcal{P}| = v$
- $\forall B \in \mathcal{B}, |B| = k$
- $\forall S \subset \mathcal{P}$ such that $|S| = t, |\{B \in \mathcal{B} : S \subset B\}| = \lambda$.

For any design $\mathcal{D}$, the *automorphism group of* $\mathcal{D}$, denoted by $\mathrm{Aut}(\mathcal{D})$, is the group $\{g \in \mathrm{Sym}(\mathcal{P}) : \mathcal{B}^g = \mathcal{B}\}$.

A design is called *symmetric* if it satisfies the additional equivalent properties (see [2, Cor.II 3.3] for proof of equivalence):

- $|\mathcal{B}| = v$
- $\forall p \in \mathcal{P}, |\{B \in \mathcal{B} : p \in B\}| = k$
- $\forall B_1, B_2 \in \mathcal{B}, |B_1 \cap B_2| = \lambda$.

Thus, $\mathcal{D}$ is symmetric if and only if the *dual design* $\mathcal{D}^* = (\mathcal{B}, \mathcal{P})$ is a design with the same parameters as $\mathcal{D}$. A *Hadamard design of order* n is a symmetric design with parameters $2-(4n-1, 2n-1, n-1)$ for some integer n. For the remainder of this dissertation, $\mathcal{D}$ will denote a Hadamard design, unless otherwise noted.

Given a Hadamard design $\mathcal{D}$, the *affine completion* $\mathcal{D}^+$ of $\mathcal{D}$ is the following *Hadamard* 3*–design*, with parameters $3-(4n, 2n, n-1)$:

- Point-set: $\mathcal{P} \cup \{p_\infty\}$.
- Blocks: $B \cup \{p_\infty\}$ and $B^c = \mathcal{P} - B$ for all $B \in \mathcal{B}$

(where c means "complement"). These designs are affine as every block belongs to a parallel class (in this case $\{B, B^c\}$) of blocks which partitions the points of the design. Note that $\mathrm{Aut}(\mathcal{D}^+)_{p_\infty} = \{g \in \mathrm{Aut}(\mathcal{D}^+) : p_\infty^g = p_\infty\} \cong \mathrm{Aut}(\mathcal{D})$ [4, Cor. 4.6].

This completion procedure is reversible: given $\mathcal{A} = (\mathcal{P}, \mathcal{B})$, an affine $3-(4n, 2n, n-1)$, and $p \in \mathcal{P}$, set $\mathcal{A}_p = (\mathcal{P} - \{p\}, \{B \in \mathcal{B} : p \in B\})$; $\mathcal{A}_p$ is then a Hadamard design of order n. Clearly, $\mathcal{D}^+_{p_\infty} = \mathcal{D}$, but different points of an affine design may produce non-isomorphic designs. In fact, [4, Cor. 4.7] shows

$$\mathcal{A}_p \cong \mathcal{A}_q \;\Leftrightarrow\; \exists f \in \mathrm{Aut}(\mathcal{A}) \text{ s.t. } p^f = q.$$

Given any ordering on the points and blocks of a Hadamard design $\mathcal{D}$, we define the ± 1 incidence matrix, a $4n-1 \times 4n-1$ matrix $A = [a_{i,j}]$ where

$$a_{i,j} = \begin{cases} 1 & \text{if } p_i \in B_j \\ -1 & \text{if } p_i \notin B_j. \end{cases}$$

Given such an incidence matrix, and adding a row and column with all entries equal to 1, one obtains a $4n \times 4n$ matrix with entries ± 1, whose rows are mutually orthogonal. Such a matrix is called a *Hadamard matrix*. This procedure is reversible; given any Hadamard matrix, multiplying a row by -1 results in another (equivalent) Hadamard matrix, similarly with columns. Thus, any Hadamard matrix is equivalent to a Hadamard matrix with the first row and first column being the all 1 vector. Deleting this row and column, one obtains the incidence matrix of a Hadamard design. Therefore, the existence of a Hadamard design of order n is equivalent to the existence of a Hadamard matrix of order $4n$.

The *classical* Hadamard designs are the projective spaces over $\mathbb{F}_2$, the field of size 2. Given a vector space V of dimension $d+1$ over $\mathbb{F}_2$, the points of the design are the one–spaces of V, and the blocks are the hyperplanes, with the obvious incidence relation. This is denoted $\mathcal{PG}(d,2)$, with parameters $2-(2^{d+1}-1, 2^d-1, 2^{d-1}-1)$ and order $n = 2^{d-1}$. The affine completion of this design is the affine space over $\mathbb{F}_2$, with points being the points of V, and blocks the hyperplanes and their complements. This is denoted $\mathcal{AG}(d+1,2)$. Note that $\mathrm{Aut}(\mathcal{PG}(d,2)) = \mathrm{GL}(d+1,2)$ and $\mathrm{Aut}(\mathcal{AG}(d+1,2)) = \mathrm{AGL}(d+1,2) \cong \mathrm{GL}(d+1,2) \ltimes \mathbb{F}_2^{d+1}$.

Given a block $B \in \mathcal{B}$, the *induced design* $\mathcal{D}_{(B)}$ *on* B consists of the points of B, with blocks $C \cap B$ for any block $C \neq B$ (note that different blocks of $\mathcal{D}$ may induce the same block of $\mathcal{D}_{(B)}$). Similarly, given a block $B \in \mathcal{B}$ the *residual design* $\mathcal{D}^B$ *off* B consists of the points of B^c, where blocks are the sets $C \cap B^c$.

II.2. Lines, colines, and goodness

Crucial to the questions of this dissertation is ascertaining whether or not two Hadamard designs are isomorphic. It is in this spirit that we introduce invariants having a geometrical nature. Indeed, as shown below, the more this invariant ("goodness") is present, the more akin a design is to a classical design. Much effort will be spent later in the thesis controlling the number of lines and colines in a design.

Three distinct blocks A, B, C of $\mathcal{D}$ form a *coline* if $B \cap C \subset A$, in which case we write $A = B * C$. As a point–set, this implies $B * C = (B \triangle C)^c$, where $\triangle$ denotes the symmetric difference of two sets. Note that $\mathcal{P} = B \cup C \cup (B * C)$, with every point contained in exactly 1, or all 3 blocks of the coline.

Dually, three distinct points p, q, r form a *line* of a Hadamard design if all blocks on both p and q are also on r. Just as with blocks, we denote by $p * q$ the third point collinear with p and q, if such a point exists. This point $p * q$ will be on the blocks containing both p and q, and the blocks containing neither. Thus, every block intersects the line in 1 point, or in all 3, a fact that will be referred to throughout this dissertation. Note that it is impossible for a fourth point to be contained all blocks containing p, q and $p * q$.

A block B is called a *good block* if, given any other block C and any point $p \notin B \cup C$, there exists a block A containing p and $B \cap C$, in which case $A = B * C$. Thus, a block B is good if and only if, for any other block C, $B*C$ exists. B is a good block of a Hadamard design $\mathcal{D}$ of order n if and only if $\mathcal{D}_{(B)}$ is a Hadamard design

of order $n/2$, which is the case if and only if $\mathcal{D}^B$ is an affine Hadamard 3-design of order $n/2$. (For the elementary proof, see [2, Theorem XII.5.3].) Dually, we say p is a *good point* if $p * q$ exists for all other points q, in which case p is a good block of $\mathcal{D}^*$, so $\mathcal{D}^*_{(p)}$ is a Hadamard design, and $(\mathcal{D}^*)^p$ is an affine Hadamard 3-design, both of order $n/2$.

Kimberley [11] provides a careful study of good blocks of affine Hadamard 3–designs. Just as with symmetric Hadamard designs, a block B of such a design is *good* if and only if, for any block $C \notin \{B, B^c\}, (B \triangle C)^c$ is also a block. In that case $(B^c \triangle C)^c = B \triangle C$ is also a block, and therefore B^c is a good block as well. Thus, the good blocks occur in parallel pairs, and we say $\{B, B^c\}$ is a *good parallel class*. Given a Hadamard design $\mathcal{D}$, the good blocks of the 3–design $\mathcal{D}^+$ are the blocks $B \cup \{p_\infty\}$ and B^c, where B is a good block of $\mathcal{D}$. Conversely, for every good parallel class $\{B, B^c\}$ of an affine Hadamard design $\mathcal{A}$, the member of the class containing p will induce a good block of $\mathcal{A}_p$. For, if we have B the member of a good parallel class containing p, then given any other block C which contains p, $(B \triangle C)^c$ is another block *which contains* p, hence another block of $\mathcal{A}_p$. Thus, B is a good block of $\mathcal{A}_p$. Therefore, although different points p and q may induce non-isomorphic designs $\mathcal{A}_p$ and $\mathcal{A}_q$, the number of good blocks of $\mathcal{A}_p$ and of $\mathcal{A}_q$ will equal the number of good parallel classes of $\mathcal{A}$.

Elementary linear algebra shows that in the classical case of $\mathcal{PG}(d, 2)$ all points are good, as the line induced by two 1–spaces is a 2–space, containing three 1–spaces.

Since $\mathcal{PG}(d,2)$ is self–dual, all blocks are good as well. It is a consequence of the Dembowski–Wagner theorem [2, Theorem XII.2.10] that the converse is true, namely any Hadamard design in which all lines (or colines) are of size 3 is isomorphic to a projective space over $\mathbb{F}_2$. The corresponding result for affine designs, namely that an affine design with all good blocks is isomorphic to $\mathcal{AG}(d,2)$ for some d, can be found in [11, Theorem 6].

All lines of an affine Hadamard design have size 2, since they are 3–designs. Thus, lines are not a useful invariant for these designs. However, for an affine Hadamard design $\mathcal{A}$, there is a close relationship between good points of $\mathcal{A}_p$ and automorphisms of $\mathcal{A}$. A *translation* of $\mathcal{A}$ is a non–trivial automorphism f with the property that $B^f = B$ or B^c for all blocks B. Clearly, such an automorphism is fixed-point-free (since for some $B, B^f = B^c$) and of order 2 (as $B^{f^2} = B$ for all blocks B). Also, the subgroup of $\mathrm{Aut}(\mathcal{A})$ generated by the translations (which is just the set of translations together with the identity) forms a normal subgroup, as it is the kernel of the representation of $\mathrm{Aut}(\mathcal{A})$ on its parallel classes. This subgroup is isomorphic to $\mathbb{Z}_2^k$ for some k. These automorphisms can be characterized by:

Lemma II.2.1. *There exists a translation $f \in Aut(\mathcal{A})$ with $p^f = q$ if and only if q is a good point of $\mathcal{A}_p$.*

Proof. $\Leftarrow$ Let q be a good point of $\mathcal{A}_p$, so $q * r$ exists for every point $r \neq q$. Define

a translation f as follows:

$$f : p \leftrightarrow q \text{ and } r \leftrightarrow q * r$$

$$B^f = \begin{cases} B & \text{if } p, q \in B \text{ or } p, q \notin B \\ B^c & \text{else.} \end{cases}$$

To show that f is an automorphism of $\mathcal{A}$, it suffices to show that it preserves incidence on the blocks containing p (i.e., the blocks of $\mathcal{A}_p$), which implies that incidence on the complements of those blocks is also preserved. Clearly, the points p and q are taken care of, as the blocks distinguishing the two are switched, so consider any other point r, and block B containing p and r. There are two cases to consider.

1. $r, p, q \in B$, so $B^f = B$ and $q * r \in B$, as B is one of the blocks on the line $\{q, r, q * r\}$ in the 2-design $\mathcal{A}_p$. So $r^f \in B^f$.

2. $r, p \in B$, but $q \notin B$, so $B^f = B^c$ and $q * r \notin B$ as B is not one of the blocks on the line $\{q, r, q * r\}$, and can therefore be on only 1 of its 3 points, namely r. Thus, $r^f = q * r \in B^c = B^f$.

$\Rightarrow$ Let f be a translation of $\mathcal{A}$ sending p to q. Then the points of $\mathcal{P} - \{p, q\}$ are partitioned into pairs r, r^f. The blocks of $\mathcal{A}_p$ are exactly the blocks of $\mathcal{A}$ containing p. Therefore, to show that $\{r, r^f, q\}$ is a line in $\mathcal{A}_p$, it suffices to show that *any block B of $\mathcal{A}$ containing r, r^f and p also contains q*. Clearly, $r, r^f \in B^f \in \{B, B^c\}$, so $B^f = B$. Since $p \in B$, we have $p^f = q \in B$, which was to be shown. $\square$

Since translations act fixed point freely, this shows that the number of good points

of $\mathcal{A}_p$ is the number of translations in $\mathrm{Aut}(\mathcal{A})$. Thus, the number of good points of $\mathcal{A}_p$ is the same as the number of good points of $\mathcal{A}_q$ for any other point q. Crucial to the second part of the above proof is the fact that any 2 orbits of a translation f form a 4–point *plane* of $\mathcal{A}$, i.e. a set of 4 points such that any block which contains 3 of the points must contain the fourth (cf. [12, Theorem 8]). Thus, a block B intersects such a plane in 0, 2, or 4 points, for if B contained exactly 1 point of the plane, B^c would contain exactly 3 of the points, which is not possible. The 4-point planes of an affine design are related to lines of size 3 in the following lemma.

Lemma II.2.2. *Let $\mathcal{A}$ be an affine Hadamard design of order n. Then $\{q, r, s\}$ is a 3–point line of $\mathcal{A}_p$ if and only if $\{p, q, r, s\}$ is a 4–point plane of $\mathcal{A}$.*

Proof. $\Rightarrow$ Assume $\{q, r, s\}$ is a line of $\mathcal{A}_p$. Let B be a block of $\mathcal{A}$, so that B is either a block of $\mathcal{A}_p$ also containing p, or B is the complement of a block of $\mathcal{A}_p$. If $\{p, q, r\} \subset B$, then B is a block of $\mathcal{A}_p$ containing q and r, hence must contain s. The $n - 1$ blocks on $\{p, q, r\}$ are thus the $n - 1$ blocks on $\{q, r, s\}$.

$\Leftarrow$ If $\{p, q, r, s\}$ is a plane of $\mathcal{A}$ than any block B of $\mathcal{A}_p$ on q and r induces a block $B \cup \{p\}$ of $\mathcal{A}$, containing p, q and r. This block must then contain s.$\square$

Lemma II.2.3. *Let $\mathcal{A}$ be an affine Hadamard design with 2 distinct 4–point planes $\{p, q, r, s\}$ and $\{r, s, t, u\}$. Then $\{p, q, t, u\}$ is a 4–point plane as well.*

Proof. Let B be a block of $\mathcal{A}$ containing p, q and t. We show $u \in B$ as well. There are 2 cases:

1. $r \in B$. Then $s \in B$ as $\{p, q, r, s\}$ is a plane. Then $r, s, t \in B$ implies $u \in B$ as $\{r, s, t, u\}$ is a plane.

2. $r \notin B$. Then $s \notin B$ as B must intersect $\{p, q, r, s\}$ in 2 points. But, $r, s \notin B$ and $t \in B$ implies $u \in B$ as B must intersect $\{r, s, t, u\}$ in 2 points. $\square$

As the above demonstrates, the presence of good blocks or good points in a design gives a lot of information regarding sub-designs and automorphism groups. Even more information about Hadamard designs can be deduced when both good points and good blocks are present. An incident point/block pair $p \in B$ is called a *flag*. If p and B are both good, this is a *good flag*. A non–incident good point/block pair is a *good anti–flag*.

To begin with, we consider a class of designs with a good anti–flag, and then prove that *all* Hadamard designs with a good anti–flag belong to this class. Given a Hadamard design $\mathcal{D} = (\mathcal{P}, \mathcal{B})$, we construct the design $\mathcal{D} \otimes 2$ (this notation is chosen as this is the design obtained from tensoring the Hadamard matrix determined from $\mathcal{D}$ as in Section II.1 and taking the tensor product with the 2×2 matrix $\left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$). Take two copies of the point set, $\mathcal{P}$ and $\mathcal{P}'$, and two copies of the block set, $\mathcal{B}$ and $\mathcal{B}'$, and define $\mathcal{D} \otimes 2$ as follows:

Point-set: $\mathcal{P} \cup \mathcal{P}'$ and an additional point p_∞.

Block-set: $\mathcal{B} \cup \mathcal{B}'$ and an additional block B_∞.

Incidence:

$$\begin{aligned} p \in & \begin{cases} B & \text{if } p \in B \\ B' & \text{if } p \in B \\ B_\infty & \forall\, p \in \mathcal{P} \end{cases} \\ p_\infty \in & \quad B \qquad \forall\, B \in \mathcal{B} \\ p' \in & \begin{cases} B & \text{if } p \in B \\ B' & \text{if } p \notin B. \end{cases} \end{aligned} \tag{II.2.4}$$

This definition enables us to illustrate some properties of $\mathcal{D} \otimes 2$.

Lemma II.2.5. *$p_\infty \notin B_\infty$ is a good anti-flag of $\mathcal{D} \otimes 2$.*

Proof. Clearly B_∞ is a good block, as $(\mathcal{D} \otimes 2)_{B_\infty} = \mathcal{D}$.

Now, consider any point $p \in \mathcal{P}$ and its "copy" $p' \in \mathcal{P}'$. The incidence relations above show that the blocks of $\mathcal{D} \otimes 2$ on both of them are never blocks of $\mathcal{B}'$, and B_∞ is not on p'. Therefore, all blocks on p and p' are the blocks of $\mathcal{B}$ containing p in the original design $\mathcal{D}$. Since p_∞ lies on all blocks of $\mathcal{B}$, the set $\{p, p', p_\infty\}$ is a line. Thus, all lines through p_∞ are of size 3. □

Conversely:

Theorem II.2.6. *Let $\mathcal{D}$ be a Hadamard design containing a good anti-flag $p \notin B$. Then $\mathcal{D} \cong \mathcal{D}_{(B)} \otimes 2$.*

Proof. If $q \neq p$ is any point of $\mathcal{D}$ not on B, then the point $p * q$ is on B, since the line $\{p, q, p * q\}$ must intersect B at a point. Similarly, given any block $C \neq B$ of

$\mathcal{D}$, exactly one of the blocks C or $B * C$ must contain p_∞ (note that C and $B * C$ determine the same block of $\mathcal{D}_{(B)}$, as $C \cap B \subset C * B$ by definition). Define a map $f : \mathcal{D} \to \mathcal{D}_{(B)} \otimes 2$ as follows:

$$q^f = \begin{cases} q & \text{if } q \in B, \\ p_\infty & \text{if } q = p, \\ (p * q)' & \text{else.} \end{cases}$$

$$C^f = \begin{cases} B \cap C & \text{if } p \in C, \\ B_\infty & \text{if } C = B, \\ (B \cap C)' & \text{else.} \end{cases}$$

We show that f is an isomorphism of designs. Clearly f is bijective and preserves all incidences involving p or B. Given any other flag $q \in C$ of $\mathcal{D}$ we refer to (II.2.4) for the following cases:

1. $q \in B$ and $p \in C$. Then $q^f = q \in B \cap C = C^f$.

2. $q \notin B$ and $p \in C$. Then $p * q \in B \cap C$, so $q^f = (p * q)' \in B \cap C = C^f$.

3. $q \in B$ and $p \notin C$. Then $q \in B \cap C$ and hence $q^f = q \in (B \cap C)' = C^f$.

4. $q \notin B$ and $p \notin C$. Then $p * q \notin C$, as C intersects the line $\{p, q, p * q\}$ only at q. Therefore $p * q \notin B \cap C$, which implies $q^f = (p * q)' \in (B \cap C)' = C^f$. $\square$

Thus, given a design with a good anti–flag $p \notin B$, the incidence relations are completely determined by the sub–design $\mathcal{D}_{(B)}$. We now turn our attention to a

design with a good flag. While we do not get as much structural information about such a design, we demonstrate that the existence of a good flag induces an *elation* of the design, that is, an automorphism that, given an incident point/block pair, fixes all the points of a block, and all the blocks on a point.

Theorem II.2.7. *Let $p \in B$ be a good flag of a Hadamard design $\mathcal{D}$. Then there exists an elation f of $\mathcal{D}$ inducing a translation of the affine Hadamard design $\mathcal{D}^B$.*

Proof. We define the map f as follows:

$$q^f = \begin{cases} p * q & \text{if } q \notin B \\ q & \text{if } q \in B \end{cases}$$

$$C^f = \begin{cases} B * C & \text{if } p \notin C \\ C & \text{if } p \in C. \end{cases}$$

This is bijective on points: $q \notin B \Leftrightarrow p * q \notin B$ as the line $\{p, q, p * q\}$ is either contained in B, or intersects B at p. Dually, f is bijective on blocks. To see that f is indeed an automorphism of $\mathcal{D}$, let $q \in C$ and consider the following cases:

1. $q \in B$ and $p \in C$: Then both q and C are fixed, so $q^f \in C^f$.

2. $q \notin B$ and $p \in C$: Then C is on both p and q, hence on the line $\{p, q, p * q\}$, so $q^f = q * p \in C = C^f$.

3. $q \in B$ and $p \notin C$: This is the dual of case 2.

4. $q \notin B$ and $p \notin C$: Then $p * q \notin C$ as C must intersect $\{p, q, p * q\}$ only at q, also $p * q \notin B$ as B must intersect $\{p, q, p * q\}$ only at p. Therefore, $q^f = p * q \in B * C = C^f$, as $B * C = (B \triangle C)^c$ contains all points on neither B nor C.

Given any block $C \neq B, C \cap B^c$ and $(B * C) \cap B^c$ form a parallel class of the affine design $\mathcal{D}^B$. Since f leaves the sets $\{C, B * C\}$ invariant, it must induce a translation of the design $\mathcal{D}^B$. $\square$

CHAPTER III

CONSTRUCTIONS

III.1. Doubling

We begin this section by defining the "doubling" construction first described in [20], and subsequently used by many authors (cf., e.g. [11, 15, 5, 8, 13]). Of particular interest are the good blocks and points which arise from this construction. We will see that in most cases we can rule out any good points and all but one good block.

Let $\mathcal{D}_1 = (\mathcal{P}_1, \mathcal{B}_1)$ be a Hadamard $2-(4n-1, 2n-1, n-1)$ design, and $\mathcal{A}_2 = (\mathcal{P}_2, \mathcal{B}_2)$ be a Hadamard $3-(4n, 2n, n-1)$ design. Then $\mathcal{A}_2$ has $4n-1 = |\mathcal{B}_1|$ parallel classes of blocks. Let σ be any bijection from the parallel classes of $\mathcal{A}_2$ to $\mathcal{B}_1$. Denote by $\overline{B_2}$ the parallel class containing B_2. Define the $2-(8n-1, 4n-1, 2n-1)$ Hadamard design $\mathcal{D}_1\sigma\mathcal{A}_2$ as follows:

- Points: $\mathcal{P}_1 \cup \mathcal{P}_2$
- Blocks: $B_\infty = \mathcal{P}_1$ and $\overline{B_2}^\sigma \cup B_2$ for all $B \in \mathcal{B}_2$.

Note that B_∞ is a good block of $\mathcal{D}_1\sigma\mathcal{A}_2$, as $((\overline{B_2}^\sigma \cup B_2) \triangle B_\infty)^c = \overline{B_2}^\sigma \cup B_2^c$ is a block for all $B_2 \in \mathcal{B}_2$ (clearly $\overline{B_2} = \overline{B_2^c}$). Clearly

$$(\mathcal{D}_1\sigma\mathcal{A}_2)_{(B_\infty)} \cong \mathcal{D}_1, \tag{III.1.1}$$

and

$$(\mathcal{D}_1\sigma\mathcal{A}_2)^{B_\infty} \cong \mathcal{A}_2. \tag{III.1.2}$$

The existence of other good blocks of $\mathcal{D}_1\sigma\mathcal{A}_2$ is a function of $\mathcal{D}_1, \mathcal{A}_2$ and σ. Given two blocks of the form $\overline{B_2}^\sigma \cup B_2$ and $\overline{C_2}^\sigma \cup C_2$, with $C_2 \notin \{B_2, B_2^c\}$, we have

$$\big((\overline{B_2}^\sigma \cup B_2)\triangle(\overline{C_2}^\sigma \cup C_2)\big)^c = \big(\mathcal{P}_1 - (\overline{B_2}^\sigma \triangle \overline{C_2}^\sigma)\big) \cup \big(\mathcal{P}_2 - (B_2 \triangle C_2)\big). \tag{III.1.3}$$

Thus, $\overline{B_2}^\sigma \cup B_2$ is good if and only if the following 2 conditions are met (see [16, Lemma 1] for the analogous proof for affine Hadamard designs):

1. Both B_2 and $\overline{B_2}^\sigma$ are good, so that $\mathcal{P}_2 - (B_2 \triangle C_2)$ and $\mathcal{P}_1 - (\overline{B_2}^\sigma \triangle \overline{C_2}^\sigma)$ are blocks of $\mathcal{B}_2$ and $\mathcal{B}_1$, respectively, for all blocks $C_2 \neq B_2$.

2. $\overline{(\mathcal{P}_2 - (B_2 \triangle C_2))}^\sigma = \mathcal{P}_1 - (\overline{B_2}^\sigma \triangle \overline{C_2}^\sigma)$ for all blocks $C_2 \neq B_2$, so that in (III.1.3), the set on the right is indeed a block of $\mathcal{D}_1\sigma\mathcal{A}_2$.

Although it is nice to have these explicit criteria for good blocks in $\mathcal{D}_1\sigma\mathcal{A}_2$, for most applications in this dissertation, the following suffices:

Observation III.1.4. *If either $\mathcal{D}_1$ or $\mathcal{A}_2$ has no good blocks, then B_∞ is the unique good block of $\mathcal{D}_1\sigma\mathcal{A}_2$.*

Before we discuss the good points that result from the doubling construction, we first characterize the lines of size 3 that intersect B_∞ in 1 point.

Lemma III.1.5. *Let p be a point of $\mathcal{D}_1$ and q, r be points of $\mathcal{A}_2$. Then $\{p, q, r\}$ is a line of $\mathcal{D}_1\sigma\mathcal{A}_2$ if and only if, for the $2n-1$ blocks B of $\mathcal{A}_2$ with $q, r \in B$, we have $p \in \overline{B}^\sigma$.*

Proof. $\Rightarrow$ If $\{p, q, r\}$ is a line of $\mathcal{D}_1\sigma\mathcal{A}_2$, then every time $p, q \in \overline{B}^\sigma \cup B$, we have $r \in \overline{B}^\sigma \cup B$, so $q, r \in B$ and $p \in \overline{B}^\sigma$.

$\Leftarrow$ Given such a σ, if $q, r \in \overline{B}^\sigma \cup B$ then $p, \in \overline{B}^\sigma \cup B$. Thus, $\{p, q, r\}$ forms a line of $\mathcal{D}_1\sigma\mathcal{A}_2$.$\square$

Corollary III.1.6. *Let $\mathcal{D}_1$ be a Hadamard design of order $n > 2$, and $\mathcal{A}_2$ an affine Hadamard design of order n. Then there exists a σ such that $\mathcal{D}_1\sigma\mathcal{A}_2$ has at least* 1 *point on no lines of size* 3.

Proof. By above, given a point p of $\mathcal{D}_1$ and q, r points of $\mathcal{A}_2$, there are $(2n-1)!2n!$ choices of σ for which $\mathcal{D}_1\sigma\mathcal{A}_2$ has $\{p, q, r\}$ as a line. Fixing q, but letting p and r vary, we see that there are $(4n-1)! - (4n-1)^2(2n-1)!(2n)!$ choices of σ for which $\mathcal{D}_1\sigma\mathcal{A}_2$ has no lines of size 3 through q. $\square$

In the case where B_∞ is the only good block of $\mathcal{D}_1\sigma\mathcal{A}_2$, the automorphism group can be nicely described. Let $G_1 = \mathrm{Aut}(\mathcal{D}_1)$ in its permutation representation on blocks, $G_2 = \mathrm{Aut}(\mathcal{A}_2)$ in its permutation representation on blocks, and $\overline{G_2} = \mathrm{Aut}(\mathcal{A}_2)$ in its permutation representation on *parallel classes* of blocks.

Lemma III.1.7. *Let $\mathcal{D}_1\sigma\mathcal{A}_2$ have B_∞ as its only good block, and $g \in Aut(\mathcal{D}_1\sigma\mathcal{A}_2)$. Then g induces a $g_1 \in G_1$ on B_∞ and a $g_2 \in G_2$ off B_∞ satisfying $g_1 = \overline{g_2}^\sigma$.*

Conversely, given such g_1 and g_2 satisfying $g_1 = \overline{g_2}^\sigma$, there exists a $g \in Aut(\mathcal{D}_1\sigma\mathcal{A}_2)$ inducing g_1 and g_2 on and off B_∞, respectively.[1]

[1] Similar ideas appear in [8, 15].

Proof. $\Rightarrow$ Since B_∞ is the unique good block, $B_\infty^g = B_\infty$. Therefore, g induces an automorphism $g_1 \in G_1$ acting on B_∞, and a $g_2 \in G_2$ acting off B_∞. Then, for any other block:

$$(\overline{B_2}^\sigma \cup B_2)^g = \overline{B_1}^{\sigma g_1} \cup B_2^{g_2} = \overline{B_2}^{\overline{g_2}\sigma} \cup B_2$$

which implies

$$\sigma g_1 = \overline{g_2}\sigma.$$

$\Leftarrow$ Suppose $g_1 = \overline{g_2}^\sigma$ for $g_1 \in G_1, g_2 \in \overline{G_2}$. We then define an automorphism g acting as g_1 on B_∞ and as an arbitrary pre–image of $\overline{g_2}$ off B_∞ as follows:

$$(\overline{B_2}^\sigma \cup B_2)^g = \overline{B_2}^{\sigma g_1} \cup B_2^{g_2} = \overline{B_2}^{\sigma\sigma^{-1}\overline{g_2}\sigma} \cup B_2^{g_2} = \overline{B_2}^{g_2\sigma} \cup B_2^{g_2}.$$

This is a block of $\mathcal{D}_1\sigma\mathcal{A}_2$, proving that g induces an automorphism.$\square$

Corollary III.1.8. *Let $\mathcal{D}_1\sigma\mathcal{A}_2$ have B_∞ as its only good block. If $Aut(\mathcal{A}_2)$ contains no translations, then:*

$$Aut(\mathcal{D}_1\sigma\mathcal{A}_2) \cong G_1 \cap \overline{G_2}^\sigma.$$

Proof. Since G_2 contains no translations, the homomorphism $G_2 \to \overline{G_2}$ is an isomorphism. Thus, Lemma III.1.7 provides the bijection between $\mathrm{Aut}(\mathcal{D}_1\sigma\mathcal{A}_2)$ and $G_1 \cap \overline{G_2}^\sigma$. $\square$

Notation III.1.9. *One special case of the doubling procedure deserves mention. Since every block B of a Hadamard design $\mathcal{D}$ determines a unique parallel class $\{B \cup \{p_\infty\}, B^c\}$. Denote by σ_0 the inverse mapping from parallel classes of $\mathcal{D}^+$ to*

blocks of $\mathcal{D}$*, i.e.* $\{B \cup \{p_\infty\}, B^c\}^{\sigma_0} = B$*. It is easily checked that the resulting design* $\mathcal{D}\sigma_0\mathcal{D}^+$ *is in fact the design* $\mathcal{D} \otimes 2$ *described in II.2.4.*

III.2. The Tensor Product

It is common knowledge that the tensor or Kronecker product of 2 Hadamard matrices is again a Hadmard matrix (see e.g. [2, Lemma I 9.6]). Given the relationship between Hadamard matrices and Hadamard designs (see section II.1), there is a corresponding notion of a tensor product of designs. Namely, if 2 Hadamard matrices have their first row and column being the all–one vectors, their tensor product has the same property, so the sub–matrix obtained by removing the first row and column is the incidence matrix of a Hadamard design. In this section, we present a matrix–free description of this product, and show that under certain circumstances (when the design has no good points), the product decomposition is unique, and thus determines the automorphism group in terms of the sub–designs.

If $\mathcal{D}_1 = (\mathcal{P}_1, \mathcal{B}_1)$ and $\mathcal{D}_2 = (\mathcal{P}_2, \mathcal{B}_2)$ are Hadamard designs of order n_1 and n_2 respectively, we denote by $\mathcal{D}_1 \otimes \mathcal{D}_2$ the Hadamard design of order $4n_1n_2$ with point–set $\mathcal{P}_1 \cup \mathcal{P}_2 \cup (\mathcal{P}_1 \times \mathcal{P}_2)$, and blocks of the following form:

$$B_1^* = B_1 \cup \mathcal{P}_2 \cup (B_1 \times \mathcal{P}_2) \tag{III.2.1}$$

$$B_2^* = \mathcal{P}_1 \cup B_2 \cup (\mathcal{P}_1 \times B_2) \tag{III.2.2}$$

$$(B_1, B_2) = (B_1^* \triangle B_2^*)^c. \tag{III.2.3}$$

We will need the line structure of the design (colines are described similarly).

Observation III.2.4. *The lines of size 3 in the design $\mathcal{D} = \mathcal{D}_1 \otimes \mathcal{D}_2$ are of the following types, where $\{x_i, y_i, z_i\}$ is a line of $\mathcal{D}_i$ of size 3 and p_i is an arbitrary point of $\mathcal{D}_i$:*

i. $\{x_i, y_i, z_i\}$

ii. $\{(x_1, x_2), (y_1, y_2), (z_1, z_2)\}$

iii. $\{(x_1, p_2), (y_1, p_2), z_1\}$ *or* $\{(p_1, x_2), (p_1, y_2), z_2\}$

iv. $\{p_1, p_2, (p_1, p_2)\}$

Two special cases are worth mentioning. The trivial case of an "empty" Hadamard design $\mathcal{E}$ with no points or blocks. Clearly, $\mathcal{D} \otimes \mathcal{E} = \mathcal{D}$ (just as taking a Kroenecker product with the matrix [1] leaves the original matrix) and this case shall hereafter be ignored. More interesting is the tensor product with the design consisting of one point and block which are non-incident. As mentioned above, this construction corresponds to the doubled design $\mathcal{D}\sigma_0\mathcal{D}^+$ mentioned above, or $\mathcal{D} \otimes 2$ defined in II.2.

Corollary III.2.5. *If $\mathcal{D} \cong \mathcal{D}_1 \otimes \mathcal{D}_2$, then every point of $\mathcal{D}$ is on at least one line of size 3.*

Proof. Lines of the form $\{p_1, p_2, (p_1, p_2)\}$ cover all points. □

For any Hadamard design $\mathcal{D}$ and point p, define:

$$p^\perp = \{p\} \cup \{q | p * q \text{ exists}\},$$

and for any set of points X:

$$X^{\perp} = \bigcap_{p \in X} p^{\perp}.$$

Lemma III.2.6. *Let p_1 be a point of $\mathcal{D}_1 \otimes \mathcal{D}_2$, and let $\perp_1$ denote the perp structure of $\mathcal{D}_1$. Then*

$$p_1^{\perp} = p_1^{\perp_1} \cup \mathcal{P}_2 \cup (p_1^{\perp_1} \times \mathcal{P}_2).$$

Proof. Lines of type *i* give $p_1^{\perp} \cap \mathcal{P}_1 = p_1^{\perp_1}$. All points of $\mathcal{P}_2$ are contained in $p_1^{\perp}$ courtesy of lines of type *iv*. Finally, $p_1^{\perp} \cap (\mathcal{P}_1 \times \mathcal{P}_2) = p_1^{\perp_1} \times \mathcal{P}_2$ as lines of type *iii* connect p_1 and a point of the form (q_1, p_2) if and only if $q_1 \in p_1^{\perp_1}$.□

Of course, we can similarly characterize $p_2^{\perp}$.

Lemma III.2.7. *Let (p_1, p_2) be a point of $\mathcal{D}_1 \otimes \mathcal{D}_2$. Then*

$$(p_1, p_2)^{\perp} = p_1^{\perp} \cap p_2^{\perp} = p_1^{\perp_1} \cup p_2^{\perp_2} \cup (p_1^{\perp_1} \times p_2^{\perp_2}).$$

Proof. $p_1^{\perp_1} \subseteq (p_1, p_2)^{\perp}$ as lines of type *iii* will exist whenever the corresponding line exists in $\mathcal{D}_1$. Also, $p_1 \in (p_1, p_2)^{\perp}$ via the unique line of type *iv* through (p_1, p_2). Similarly for $p_2^{\perp_2} \subseteq (p_1, p_2)^{\perp}$. Finally, lines of type *ii* show that $(p_1, p_2)^{\perp} \cap (\mathcal{P}_1 \times \mathcal{P}_2) = p_1^{\perp_1} \times p_2^{\perp_2}$. □

Lemma III.2.8. *The good points of $\mathcal{D}_1 \otimes \mathcal{D}_2$ are all of the form p_1, p_2, or (p_1, p_2) where p_i is a good point of $\mathcal{D}_i$.*

Proof. Lemma III.2.6 shows that p_1 is good if and only if $p_1^{\perp_1} = \mathcal{P}_1$, i.e., if and only if p_1 is a good point of $\mathcal{D}_1$. Similarly, p_2 is good if and only if $p_2^{\perp_2} = \mathcal{P}_2$. For a

point of the form (p_1, p_2) to be good, lemma III.2.7 shows that both p_1 and p_2 will necessarily be good as well. □

Corollary III.2.9. *Let $\mathcal{D} = \mathcal{D}_1 \otimes \mathcal{D}_2$ where $\mathcal{D}_2$ has no good points. If p is a point of $\mathcal{D}$, then $p^\perp \supseteq \mathcal{P}_2$ if and only if $p \in \mathcal{P}_1$.*

Lemma III.2.10. *Let $\mathcal{D}_1 \otimes \mathcal{D}_2$ have a point–transitive automorphism group. Then $\mathcal{D}_1 \otimes \mathcal{D}_2$ is isomorphic to a projective space over $\mathbb{F}_2$.*

Proof. For any $p_1 \in \mathcal{P}_1$ and $p_2 \in \mathcal{P}_2$, there exists an automorphism $g \in \mathrm{Aut}(\mathcal{D}_1 \otimes \mathcal{D}_2)$ so $p_1^g = (p_1, p_2)$. Therefore, $|p_1^\perp| = |(p_1, p_2)^\perp|$, which implies by Lemma III.2.7 $p_1^\perp \subseteq p_2^\perp$. Thus, $\mathcal{P}_2 \subseteq p_2^\perp$, so p_2 is a good point of $\mathcal{D}_2$ and hence of $\mathcal{D}_1 \otimes \mathcal{D}_2$ by Lemma III.2.8. Since $\mathrm{Aut}(\mathcal{D}_1 \otimes \mathcal{D}_2)$ is transitive, all points of $\mathcal{D}_1 \otimes \mathcal{D}_2$ are good. This implies that $\mathcal{D}_1 \otimes \mathcal{D}_2$ is a projective space by the Dembowski–Wagner Theorem [2, Theorem XII.2.10]. □

Dually, Lemma III.2.10 implies that a tensor product design with a block–transitive automorphism group is classical as well.

Theorem III.2.11. *Given a Hadamard design $\mathcal{D}$, we have $\mathcal{D} \cong \mathcal{D}_1 \otimes \mathcal{D}_2$ where $\mathcal{D}_i = (\mathcal{P}_i, \mathcal{B}_i)$ if and only if the point set and the block set of $\mathcal{D}$ can be partitioned as $\mathcal{P} = \mathcal{P}_1 \cup \mathcal{P}_2 \cup (\mathcal{P}_1 \times \mathcal{P}_2)$ and $\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2 \cup (\mathcal{B}_1 \times \mathcal{B}_2)$ satisfying the following properties:*

1. *The incidence structures $(\mathcal{P}_i, \mathcal{B}_i)$ are both induced 2-designs of $\mathcal{D}$.*[2]

[2] By conventional abuse of notation, $(\mathcal{P}_i, \mathcal{B}_i)$ is the design consisting of the point set $\mathcal{P}_i$ and blocks being the intersection of $\mathcal{B}_i$ with the point set. Note that $(\mathcal{P}_i, \mathcal{B}_i)$ may be the trivial Hadamard design on a single point, with a single block being the empty set.

2. *For all* $p_1 \in \mathcal{P}_1$ *and* $B_2 \in \mathcal{B}_2$ *we have* $p_1 \in B_2$ *and for all* $p_2 \in \mathcal{P}_2$ *and* $B_1 \in \mathcal{B}_1$ *we have* $p_2 \in B_1$

3. *For every* $(p_1, p_2) \in \mathcal{P}_1 \times \mathcal{P}_2, (p_1, p_2) = p_1 * p_2$. *Dually, every block* $(B_1, B_2) \in \mathcal{B}_1 \times \mathcal{B}_2$ *lies on a coline of size 3 with* B_1 *and* B_2.

Proof. The forward implication is immediate, by the definition of $\mathcal{D}_1 \otimes \mathcal{D}_2$. For the converse, first we note that if such sub-designs of $\mathcal{D}$ exist, they must themselves be symmetric designs. The existence of the partitions shows:

$$v_1 + v_2 + v_1 v_2 = v = b = b_1 + b_2 + b_1 b_2.$$

Combined with Fisher's Inequality: $v_i \leq b_i$ for any 2-design gives $v_i = b_i$, implying that both induced sub-designs are symmetric. To see that both designs are Hadamard, consider any block $B_1 \in \mathcal{B}_1$. Since $\{p_1, p_2, (p_1, p_2)\}$ forms a line by condition *3*, and we are given $p_2 \in B_1$ by condition *2*, we have $(p_1, p_2) \in B_1$ if and only if $p_1 \in B_1$. Set $|B_1 \cap \mathcal{P}_1| = k_1, |\mathcal{P}_1| = v_1$, and $|\mathcal{P}_2| = v_2$. Since $\mathcal{D}$ is Hadamard, we have:

$$|B_1| = k_1 + v_2 + k_1 v_2 = \frac{1}{2}(v + 1) - 1 = \frac{1}{2}(v_1 + v_2 + v_1 v_2 + 1) - 1.$$

Which gives:

$$k_1 + 1 = \frac{1}{2}(v_1 + 1),$$

which shows that $\mathcal{D}_1$ is Hadamard. Similarly, so is $\mathcal{D}_2$.

As we saw above, $(p_1, p_2) \in B_1$ if and only if $p_1 \in B_1$. This ensures that the points in B_1 correspond to the points of B_1^* given in equation (III.2.1). Similarly, a

block $B_2 \in \mathcal{B}_2$ satisfies equation (III.2.2). Finally, the colines of condition *3* ensure that the blocks of the form (B_1, B_2) satisfy equation (III.2.3). $\square$

If $\mathcal{D}$ contains subdesigns $\mathcal{D}_1$ and $\mathcal{D}_2$ satisfying the conditions of Theorem III.2.11, then we say $\mathcal{D} = \mathcal{D}_1 \otimes \mathcal{D}_2$ as a *internal* tensor product. The associativity of this product follows from the corresponding statement about matrices.

Lemma III.2.12. *For Hadamard designs $\mathcal{D}_1, \mathcal{D}_2$ and $\mathcal{D}_3$,*

$$(\mathcal{D}_1 \otimes \mathcal{D}_2) \otimes \mathcal{D}_3 = \mathcal{D}_1 \otimes (\mathcal{D}_2 \otimes \mathcal{D}_3).$$

Proof. The design on the left has points:

$$(\mathcal{P}_1 \cup \mathcal{P}_2 \cup (\mathcal{P}_1 \times \mathcal{P}_2)) \cup \mathcal{P}_3 \cup (\mathcal{P}_3 \times (\mathcal{P}_1 \cup \mathcal{P}_2 \cup (\mathcal{P}_1 \times \mathcal{P}_2)))$$

and blocks similarly. The subdesigns $(\mathcal{P}_1, \mathcal{B}_1) = \mathcal{D}_1$ and $(\mathcal{P}_2 \cup \mathcal{P}_3 \cup (\mathcal{P}_2 \times \mathcal{P}_3), \mathcal{B}_2 \cup \mathcal{B}_3 \cup (\mathcal{B}_2 \times \mathcal{B}_3)) = \mathcal{D}_2 \otimes \mathcal{D}_3$ satisfy the conditions of Theorem III.2.11. $\square$

Theorem III.2.13. *If $\mathcal{D} = \mathcal{D}_1 \otimes \mathcal{D}_2 = \mathcal{D}'_1 \otimes \mathcal{D}'_2$ and $\mathcal{D}$ contains no good points, then:*

$$\mathcal{D} = (\mathcal{D}_1 \cap \mathcal{D}'_1) \otimes (\mathcal{D}_1 \cap \mathcal{D}'_2) \otimes (\mathcal{D}_2 \cap \mathcal{D}'_1) \otimes (\mathcal{D}_2 \cap \mathcal{D}'_2)$$

where $(\mathcal{D}_i \cap \mathcal{D}'_j)$ is the induced subdesign on $(\mathcal{P}_i \cap \mathcal{P}'_j, \mathcal{B}_i \cap \mathcal{B}'_j)$.[3]

Proof. It suffices to show that $\mathcal{D}_1 = (\mathcal{D}_1 \cap \mathcal{D}'_1) \otimes (\mathcal{D}_1 \cap \mathcal{D}'_2)$, as $\mathcal{D}_2$ will decompose similarly. To begin with, we have:

$$\mathcal{P}_1 = (\mathcal{P}_1 \cap \mathcal{P}'_1) \cup (\mathcal{P}_1 \cap \mathcal{P}'_2) \cup (\mathcal{P}_1 \cap (\mathcal{P}'_1 \times \mathcal{P}'_2))$$

[3]Note that the $\mathcal{D}_i \cap \mathcal{D}_j$ may be trivial, or even empty.

which is a partition of $\mathcal{P}_1$. We first show that this partition satisfies property *3* of Theorem III.2.11. Let $p_1 = (p_1', p_2')$, so $p_1 = p_1' * p_2'$. We need to show that $p_1', p_2' \in \mathcal{P}_1$. By lemmas III.2.6 and III.2.7, we have:

$$\mathcal{P}_2 \subseteq p_1^{\perp} = (p_1', p_2')^{\perp} = {p_1}'^{\perp} \cap {p_2}'^{\perp}.$$

Thus, $\mathcal{P}_2 \subseteq {p_1}'^{\perp}$, so ${p_1}'^{\perp} \in \mathcal{P}_1$ by Lemma III.2.9 (Note that since $\mathcal{D}$ has no good points, neither does $\mathcal{D}_2$, by Lemma III.2.8). Clearly, the same argument shows that $p_2' \in \mathcal{P}_1$, so we have satisfied property *3* for the points of $\mathcal{P}_1$. For the dual condition, suppose $B_1 = (B_1', B_2') \in \mathcal{B}_1$. We need to show ${B_1}'^*, {B_2}'^* \in \mathcal{B}_1$. It suffices to show that $\mathcal{P}_2 \subset {B_1'}^*$ as the blocks of $\mathcal{B}_1$ are the only blocks which contain all points of $\mathcal{P}_2$, and we already have $\mathcal{P}_2 \subset B_1^* = (B_1', B_2')$. Let $q_2 \in \mathcal{P}_2$, and we consider the following 3 cases:

1. $q_2 = q_1' \in \mathcal{P}_2 \cap \mathcal{P}_1'$. But, $q_1' \in (B_1', B_2')$ implies $q_1' \in {B_1}'^*$.

2. $q_2 = q_2' \in \mathcal{P}_2 \cap \mathcal{P}_2'$. Then $q_2' \in {B_1}'^*$ is immediate.

3. $q_2 = (q_1', q_2') \in \mathcal{P}_2 \cap (\mathcal{P}_1' \times \mathcal{P}_2')$. By the argument above, this means $q_1', q_2' \in \mathcal{P}_2 \subset (B_1', B_2')$, so $q_1' \in {B_1'}^*$, implying $(q_1', q_2') \in {B_1'}^*$.

The same argument shows $B_2' \in \mathcal{B}_1$, completing the proof of property *3.*

Property *2* of Theorem III.2.11 is immediate, as any point of $\mathcal{P}_1 \cap \mathcal{P}_1'$ is contained in every block of $\mathcal{B}_1 \cap \mathcal{B}_2'$ simply by the incidence relations of $\mathcal{D}_1' \otimes \mathcal{D}_2'$.

For property *1,* first note $\mathcal{D}_1$ is a 2–design. Given any two points $p, q \in \mathcal{P}_1 \cap \mathcal{P}_1'$, they lie on λ_1 blocks of $\mathcal{B}_1$. But, $\mathcal{B}_1 = (\mathcal{B}_1 \cap \mathcal{B}_1') \cup (\mathcal{B}_1 \cap \mathcal{B}_2') \cup (\mathcal{B}_1 \cap (\mathcal{B}_1' \times \mathcal{B}_2'))$.

Suppose p and q lie on λ_{pq} blocks of $\mathcal{B}_1 \cap \mathcal{B}'_1$. Then they lie on every block of $\mathcal{B}_1 \cap \mathcal{B}'_2$ by property *2* (say this set has size β), and property *3* gives us that the blocks of $\mathcal{B}_1 \cap (\mathcal{B}'_1 \times \mathcal{B}'_2)$ are on unique colines with a block from each of the first two sets, so p and q must lie on $\lambda_{pq}\beta$ blocks of that type. Therefore:

$$\lambda_1 = \lambda_{pq} + \beta + \lambda_{pq}\beta$$

Since λ_1 and β are both independent of the choice of p and q, λ_{pq} must be too. In other words, $(\mathcal{P}_1 \cap \mathcal{P}'_1, \mathcal{B}_1 \cap \mathcal{B}'_1)$ is an induced 2–design of $\mathcal{D}_1$. The same argument gives $(\mathcal{P}_1 \cap \mathcal{P}'_2, \mathcal{B}_1 \cap \mathcal{B}'_2)$ a 2–design, completing the proof.□

In the above theorem, "no good points" can be replaced with the hypothesis "no good blocks" by duality.

If $\mathcal{D} \neq \mathcal{D}_1 \otimes \mathcal{D}_2$ for any non–empty $\mathcal{D}_1, \mathcal{D}_2$, we say $\mathcal{D}$ is *tensor–indecomposable*. The following corollary demonstrates that, in the absence of good points, a design decomposes into unique tensor factors. This is in contrast to the classical case of $\mathcal{PG}(d, 2)$, which can be decomposed into complementary subspaces in many ways.

Corollary III.2.14. *Let*

$$\mathcal{D} = \bigotimes_{i=1}^{n} \mathcal{D}_i = \bigotimes_{i=1}^{m} \mathcal{D}'_i$$

where the $\mathcal{D}_i$ and $\mathcal{D}'_i$ are tensor-indecomposable, and $\mathcal{D}$ has no good points.

Then there exists a bijection $f : \{1, ..., n\} \to \{1, ..., m\}$ satisfying $\mathcal{D}_{if} \cong \mathcal{D}'_i$

We have:

$$\mathcal{D} = \mathcal{D}_1 \otimes \bigotimes_{i=2}^{n} \mathcal{D}_i = \mathcal{D}'_1 \otimes \bigotimes_{i=2}^{m} \mathcal{D}'_i.$$

If $\mathcal{D}_1 = \mathcal{D}_1'$, we are done by induction. Otherwise, Theorem III.2.13 gives:

$$\mathcal{D}_1 = (\mathcal{D}_1 \cap \mathcal{D}_1') \otimes \mathcal{D}_1 \cap \bigotimes_{i=2}^{m} \mathcal{D}_i'.$$

Since $\mathcal{D}_1$ is tensor–indecomposable, we must have $\mathcal{D}_1 = \mathcal{D}_1 \cap \bigotimes_{i=2}^{m} \mathcal{D}_i'$. Another application of III.2.13 yields:

$$\bigotimes_{i=2}^{m} \mathcal{D}_i' = (\mathcal{D}_1 \cap \bigotimes_{i=2}^{m} \mathcal{D}_i') \otimes (\bigotimes_{i=2}^{n} \mathcal{D}_i \cap \bigotimes_{i=2}^{m} \mathcal{D}_i') = \mathcal{D}_1 \otimes (\bigotimes_{i=2}^{n} \mathcal{D}_i \cap \bigotimes_{i=2}^{m} \mathcal{D}_i').$$

By induction, this decomposition is unique, so $m - 1 = n - 1$, and for some j, we have $\mathcal{D}_j' = \mathcal{D}_1$. □

Corollary III.2.15. *Let $\mathcal{D} = \mathcal{D}_1 \otimes \mathcal{D}_2$ where both $\mathcal{D}_1$ and $\mathcal{D}_2$ are tensor–indecomposable, and $\mathcal{D}$ has no good points. Then $Aut(\mathcal{D})$ is isomorphic to*

- *$Aut(\mathcal{D}_1) \times Aut(\mathcal{D}_2)$ if $\mathcal{D}_1 \ncong \mathcal{D}_2$.*
- *$(Aut(\mathcal{D}_1) \times Aut(\mathcal{D}_2)) \rtimes \mathbb{Z}_2$ if $\mathcal{D}_1 \cong \mathcal{D}_2$.*

Proof. Clearly $\mathrm{Aut}(\mathcal{D}) \geq \mathrm{Aut}(\mathcal{D}_1) \times \mathrm{Aut}(\mathcal{D}_2)$, stabilizing the point-sets $\mathcal{P}_1$ and $\mathcal{P}_2$. Any image of the subdesigns $(\mathcal{P}_1, \mathcal{B}_1)$ and $(\mathcal{P}_2, \mathcal{B}_2)$ must give another decomposition. By Theorem III.2.13, the present decomposition is unique. Thus, any automorphism must leave these subdesigns fixed, if they are not isomorphic, or potentially switch them if they are. □

Generalizing this, we show that determining a factorization yields the following information regarding the automorphism group.

Corollary III.2.16. *Let $\mathcal{D}$ have no good points and*

$$\mathcal{D} = \bigotimes_{i=1}^{n_1} \mathcal{D}_1 \otimes \bigotimes_{i=1}^{n_2} \mathcal{D}_2 \otimes \cdots \otimes \bigotimes_{i=1}^{n_m} \mathcal{D}_m$$

for tensor–indecomposable designs $\mathcal{D}_i$. Then:

$$Aut(\mathcal{D}) \cong Aut(\mathcal{D}_1) \wr S_{n_1} \times Aut(\mathcal{D}_2) \wr S_{n_2} \times \cdots \times Aut(\mathcal{D}_m) \wr S_{n_m}$$

Proof. Any automorphism of $\mathcal{D}$ maps a tensor decomposition to a tensor decomposition, but Theorem III.2.14 ensures that this decomposition is unique. Thus, the above group is the only possibility. □

The corollary of the following Lemma gives a necessary condition for designs of the form $\mathcal{D}_1 \sigma \mathcal{A}_2$ to be tensor-decomposable. Recall the definition of a block B^* from equation III.2.1.

Lemma III.2.17. *Let $\mathcal{D} = \mathcal{D}_1 \otimes \mathcal{D}_2$ and let B be a good block of $\mathcal{D}_1$. Then $\mathcal{D}_{(B^*)} = \mathcal{D}_{1(B)} \otimes \mathcal{D}_2$.*

Proof. The points of $\mathcal{D}_{(B^*)}$ are: $B \cup \mathcal{P}_2 \cup B \times \mathcal{P}_2$, which is also the point set of $\mathcal{D}_{1(B)} \otimes \mathcal{D}_2$. For blocks, $(B_1, B_2) \cap B^* = (B_1 \cap B, B_2)$.□

Corollary III.2.18. *Let $\mathcal{D} = \mathcal{D}_1 \sigma \mathcal{A}_2$ have a unique good block, and no good points. If $\mathcal{D}_1$ is tensor–indecomposable, so is $\mathcal{D}$.*

Suppose $\mathcal{D} \cong \mathcal{D}_3 \otimes \mathcal{D}_4$. By the dual of lemma III.2.8, the unique good block of $\mathcal{D}$ must be a block of $\mathcal{D}_3$ or $\mathcal{D}_4$. Assume it is a block of $\mathcal{D}_3$. By lemma III.2.17 above, $\mathcal{D}_{(B^*)} \cong \mathcal{D}_{3(B)} \otimes \mathcal{D}_4$. However, by equation III.1.1 we have $\mathcal{D}_{(B)} \cong \mathcal{D}_1$, which is tensor–indecomposable by assumption. □

CHAPTER IV

LOWER BOUNDS

In this Chapter, we prove the following Theorem:

Theorem IV.0.1. *If a* $2-(4n-1,2n-1,n-1)$ *design exists, then the number of non-isomorphic* $2-(8n-1,4n-1,2n-1)$ *designs is at least*

$$\frac{(4n-1)!}{2^{10}n^3(n!)^4} > 2^{8n-16-7\log n}.$$

This is first proved in Section IV.1 with the additional hypothesis that a Hadamard design of order n *with no good blocks* exists. Then, in Section IV.2, we show that if a Hadamard design of order $n > 2$ exists, then a Hadamard design of the same order exists with no good blocks, completing the proof of Theorem IV.0.1. The Section concludes with corollary IV.2.4, which shows how the lower bound of Theorem IV.0.1 also gives lower bounds for other types of combinatorial objects.

IV.1. Exponentially Many Hadamard Designs

Let $\mathcal{D}_1$ be a Hadamard design of order n and $\mathcal{A}_2$ be an affine Hadamard design of order n. Set $G_1 = \mathrm{Aut}(\mathcal{D}_1)$, and let $\overline{G_2}$ denote $\mathrm{Aut}(\mathcal{A}_2)$ in its permutation representation on the set of parallel classes of $\mathcal{A}_2$. We begin with a general observation about isomorphisms among designs of the form $\mathcal{D}_1\sigma\mathcal{A}_2$:

Lemma IV.1.1. *Let $\mathcal{D}_1\sigma\mathcal{A}_2$ and $\mathcal{D}_1\tau\mathcal{A}_2$ have B_∞ as their only good block. Then $\mathcal{D}_1\sigma\mathcal{A}_2 \cong \mathcal{D}\tau\mathcal{A}_2$ if and only if $\sigma \in \overline{G_2}\tau G_1$.*

Proof.[1]

$\Rightarrow$ Since B_∞ is the only good block of both $\mathcal{D}_1\sigma\mathcal{A}_2$ and $\mathcal{D}\tau\mathcal{A}_2$, any isomorphism $f : \mathcal{D}_1\sigma\mathcal{A}_2 \to \mathcal{D}_1\tau\mathcal{A}_2$ must satisfy $B_\infty^f = B_\infty$. Therefore, f must induce $f_1 \in G_1$ acting on B_∞, and $f_2 \in \mathrm{Aut}(\mathcal{A}_2)$ acting off B_∞. As before, denote by $\overline{B_2}$ the parallel class of a block B_2 of $\mathcal{A}_2$ and by $\overline{f_2}$ the permutation of parallel classes induced by f_2. Let $B_1 \cup B_2$ be a block of $\mathcal{D}_1\sigma\mathcal{A}_2$, so that $\overline{B_2}^\sigma = B_1$. Then $(B_1 \cup B_2)^f = B_1^{f_1} \cup B_2^{f_2}$ must be a block of $\mathcal{D}_1\tau\mathcal{A}_2$, implying that $\overline{B_2}^{\overline{f_2}\tau} = B_1^{f_1} = (\overline{B_2}^\sigma)^{f_1}$. This must be true for all $\overline{B_2}$, and therefore $\sigma f_1 = \overline{f_2}\tau$, so that $\sigma = \overline{f_2}\tau f_1^{-1} \in \overline{G_2}\tau G_1$, which was to be shown.

$\Leftarrow$ Given $\sigma \in \overline{G_2}\tau G_1$, choose $\overline{f_2} \in \overline{G_2}$ and $f_1 \in G_1$ so that $\sigma = \overline{f_2}\tau f_1^{-1}$. Choose any $f_2 \in \mathrm{Aut}(\mathcal{A}_2)$ so that f_2 induces $\overline{f_2}$ in its action on parallel classes. Define a function $f : \mathcal{D}_1\sigma\mathcal{A}_2 \to \mathcal{D}_1\tau\mathcal{A}_2$ acting as the identity on points, and $B_\infty^f = B_\infty$. For the other blocks, set $(B_1 \cup B_2)^f = B_1^{f_1} \cup B_2^{f_2}$. Since $B_1 = \overline{B_2}^\sigma$, we have:

$$(B_1 \cup B_2)^f = \overline{B_2}^{\sigma f_1} \cup B_2^{f_2} = \overline{B_2}^{\overline{f_2}\tau} \cup B_2^{f_2} = \overline{B_2^{f_2}}^\tau \cup B_2^{f_2},$$

which is a block of $\mathcal{D}_1\tau\mathcal{A}_2$, completing the proof. $\square$

Corollary IV.1.2. *If either $\mathcal{D}_1$ or $\mathcal{A}_2$ has no good blocks, then the number of non–isomorphic designs of the form $\mathcal{D}_1\sigma\mathcal{A}_2$ is at least* $\dfrac{(4n-1)!}{|G_1||\overline{G_2}|}$.

[1] For an analogous proof in the affine case, see [15, Theorem 1]. Similar ideas also appear in [8, Theorem 3.1] and [5, Lemma 2.1].

Proof.[2] There are $(4n-1)!$ choices for σ, and Lemma IV.1.1 states that any given $\mathcal{D}_1\sigma\mathcal{A}_2$ can be isomorphic to only $|G_1\sigma\overline{G_2}| \leq |G_1||\overline{G_2}|$ other designs of this form. $\square$

Next we bound the sizes of the above groups, first appealing to a well–known fact regarding automorphisms of Hadamard designs.

Fact IV.1.3. *Let $\mathcal{D}$ be a $2-(4n-1, 2n-1, n-1)$ Hadamard design and $1 \neq g \in Aut(\mathcal{D})$. Then g fixes at most $2n-1$ points and at most $2n-1$ blocks.*

Proof. Choose a block B such that $B^g = C \neq B$. Therefore $h : B \cap C^c \to B^c \cap C$, and $|B \cap C^c| = |B^c \cap C| = n$, so the support of g contains at least $2n$ points. Thus, *g fixes at most $4n-1-2n = 2n-1$ points.* Dually, g fixes at most $2n-1$ blocks. $\square$

Lemma IV.1.4. *For a Hadamard design $\mathcal{D}$ of order n, set $G = Aut(\mathcal{D})$ and $\overline{G} = Aut(\mathcal{D}^+)$ in its representation on parallel classes of blocks. Then $|G| < 16n(n!)^2$ and $|\overline{G}| < 64n^2(n!)^2$.*

Proof. Define $G_{B,C} = \{g \in \text{Aut } \mathcal{D} | B^g = B, C^g = C\}$. Note that $G_{B,C}$ leaves the sets $B^c \cap C$ and $B \cap C^c$ invariant, so we get a homomorphism

$$\phi : G_{B,C} \to \text{Sym}(B^c \cap C) \times \text{Sym}(B \cap C^c).$$

Anything in the kernel of ϕ fixes $|B \triangle C| = 2n$ points, hence ϕ is injective, by Fact IV.1.3. Thus,

$$|G| \leq (4n-1)(4n-2)|G_{B,C}| \leq (4n-1)(4n-2)(n!)^2 < 16n(n!)^2.$$

[2]The same bound can be found in [14, Corollary 3.7] using different counting methods.

Also, $\mathrm{Aut}(\mathcal{D}^+)_{p_\infty} = G$, and $|\overline{G}| \leq |\mathrm{Aut}(\mathcal{D}^+)|$ (as $\overline{G}$ is a homomorphic image of $\mathrm{Aut}(\mathcal{D}^+)$), so

$$|\overline{G}| \leq 4n|G| < 64n^2(n!)^2.\square$$

Corollary IV.1.5. *Theorem IV.0.1 holds if there exists a Hadamard design of order n without good blocks.*

Proof. Combining Lemmas IV.1.2 and IV.1.4, we see that the number of non-isomorphic designs of the form $\mathcal{D}\sigma\mathcal{D}^+$ is greater than

$$\frac{(4n-1)!}{|G||\overline{G}|} > \frac{(4n-1)!}{2^{10}n^3(n!)^4} > 2^{8n-16-7\log n}. \tag{IV.1.6}$$

The second inequality in (IV.1.6) follows from the inequalities[3]

$$2^{4n} = \sum_{i=0}^{4n}\binom{4n}{i} < 1 + \sum_{1}^{4n-1}\binom{4n}{2n} + 1 < 4n\binom{4n}{2n},$$

from which we deduce $\binom{4n}{2n} > \frac{2^{4n}}{4n}$. Similarly, $\binom{2n}{n} > \frac{2^{2n}}{2n}$. Thus,

$$\frac{(4n)!}{(n!)^4} = \binom{4n}{2n}\binom{2n}{n}\binom{2n}{n} > \frac{2^{4n}}{4n}\left(\frac{2^{2n}}{2n}\right)^2 = \frac{2^{8n}}{2^4n^3},$$

as required in (IV.1.6) .

IV.2. Eliminating Goodness

Theorem IV.2.1. *Given a $2-(4n-1, 2n-1, n-1)$ Hadamard design with $n > 2$, there exists a Hadamard design with the same parameters having no good blocks, and at most one good point.*

[3]The author is grateful to Àkos Seress for his help with these bounds.

The proof relies on the next two lemmas.

Lemma IV.2.2. *Let $\mathcal{D}$ be a Hadamard design of order $n > 4$. Then there exists a Hadamard design $\mathcal{D}'$ of order $n' = n/2^h$ with neither good points nor good blocks, for some h.*

Proof. Assume first that n is not a power of 2. If $\mathcal{D}$ has a good block B, then $\mathcal{D}_{(B)}$ is a Hadamard design of order $n/2$. If $\mathcal{D}_{(B)}$ has a good block, we can repeatedly look at induced designs, each of half the order of the previous design. Similarly, a good point p of $\mathcal{D}$ is a good block of $\mathcal{D}^*$, hence there exists an induced design $\mathcal{D}^*_{(p)}$ with order $n/2$. Since n is not a power of 2, after some sequence of induced designs we must obtain a design $\mathcal{D}'$ with no good blocks or points.

If n is a power of 2, let $\mathcal{D}'$ be the Paley design on 31 points (see [17] for the relevant definition). $\mathcal{D}'$ is a Hadamard design of order 2^3 . Since $\mathcal{D}'$ has a (point and block) transitive automorphism group, either all points/blocks are good, or none are. If all points were good, we would have $\mathcal{D}'$ isomorphic to a projective space of dimension 4 over the field of size 2 by the Dembowski-Wagner Theorem [2, Theorem XII.2.10]. This is not the case, by [7].

Lemma IV.2.3. *Let n have the property that there exists a Hadamard design of order n with no good blocks and at most one good point. Then $2n$ has that property as well.*

Proof. Let $\mathcal{D}$ be a Hadamard design of order n with no good blocks and at most one good point (note that $n > 2$ as the projective plane over $\mathbb{F}_2$ is the unique Hadamard

design of order 2). Set $\mathcal{D}_1 = \mathcal{D}\sigma(\mathcal{D}^*)^+$, where σ is chosen so that $\mathcal{D}_1 \ncong \mathcal{D}\sigma_0\mathcal{D}^+$. Such a σ exists, as for $n \geq 3$, the middle term of (IV.1.6) guarantees the existence of more than one Hadamard design of order $2n$, up to isomorphism. Note that $\mathcal{D}_1$ has B_∞ as its unique good block by Observation III.1.4, as $\mathcal{D}$ has no good blocks.

We claim $\mathcal{D}_1$ *has no good points.* For, a good point off B_∞ would yield a good anti-flag, giving $\mathcal{D}_1 \cong \mathcal{D}\sigma_0\mathcal{D}^+$ by Lemma II.2.6. This contradicts our choice of σ.

On the other hand, a good point on B_∞ would yield a good flag, inducing an elation through B_∞ by Lemma II.2.7. This would, in turn, induce a translation of $(\mathcal{D}^*)^+$, implying that $\mathcal{D}^*$ has a good point, by Lemma II.2.1. This is impossible as good points of $\mathcal{D}^*$ correspond to good blocks of $\mathcal{D}$, which don't exist.

Since $\mathcal{D}_1$ has no good points and a unique good block, $\mathcal{D}_1^*$ is a Hadamard design of order $2n$ with no good blocks, and a unique good point. □

Proof of Theorem IV.2.1 For $n \neq 4$, find $n' = n/2^h$ as in lemma IV.2.2, then apply lemma IV.2.3 h times. For $n = 4$, [16, page 339] cites the existence of a Hadamard design (denoted A^8C^7) on 15 points with no good blocks, whose affine completion has a unique translation. Thus, A^8C^7 must have a unique good point, by Lemma II.2.1. □

Proof of Theorem IV.0.1 This now follows from Theorem IV.2.1 and Corollary IV.1.5.□

We conclude this Chapter with a corollary of Theorem IV.0.1 which shows that the exponential lower bound on non–isomorphic Hadamard designs immediately im-

plies a similar bound for non–isomorphic Hadamard 3 designs, and a lower bound for inequivalent Hadamard matrices.

Corollary IV.2.4. *If a* $2-(4n-1,2n-1,n-1)$ *design exists, then the number of non-isomorphic affine* $3-(8n,4n,2n-1)$ *designs is at least*

$$\frac{(4n-1)!}{2^{13}n^4(n!)^4} > 2^{8n-19-8\log n},$$

and the number of inequivalent Hadamard matrices of size $8n$ *is at least*

$$\frac{(4n-1)!}{2^{16}n^5(n!)^4} > 2^{8n-22-9\log n}.$$

Proof. Any of the Hadamard designs constructed in Theorem IV.0.1 can be completed to an affine design. However, these affine designs may be isomorphic. Given any point p of a $3-(8n,4n,2n-1)$ affine Hadamard design $\mathcal{A}$ we get a unique $2-(8n-1,4n-1,2n-1)$ Hadamard design on the remaining points, using the blocks containing p. Distinct points p potentially induce non-isomorphic 2–designs. However, since there are only $8n$ points, we see that $\mathcal{A}$ can be associated with at most $8n$ distinct 2–designs. This proves the first assertion.

Hadamard matrices H and H' are *equivalent* if there exist monomial $\{\pm 1\}$ matrices P and Q such that $PHQ = H'$. Let H be a Hadamard matrix of order $8n$. Fix a column of H, set P equal to the diagonal matrix with entries of the fixed column, and let Q be the identity matrix. We then obtain an equivalent matrix $H' = PHQ$ with a column of all 1's. Denote by $\widehat{H}$ the $8n$ by $8n-1$ matrix obtained by removing the all one column from H'. Then $(\widehat{H}, -\widehat{H})$ is the $\{\pm 1\}$ incidence matrix

of a Hadamard 3–design. As above, different columns potentially determine non-isomorphic 3–designs. Since there are $8n$ choices of columns, a given matrix can be associated with at most $8n$ distinct 3–designs. This proves the second assertion. □

CHAPTER V

AUTOMORPHISM GROUPS

In this chapter we accomplish two things. First, we show that by applying the doubling procedure (cf. III.1) 3 times to an arbitrary Hadamard design, we can construct many non–isomorphic Hadamard designs with no non–trivial automorphisms. Section V.2 describes a class of designs which have classical parameters (i.e. the order n is a power of 2), but smaller automorphism groups than the corresponding classical designs. Also, these designs have properties that make them more tractable when applying the doubling procedure. In Section V.3, we show that given an arbitrary group G, we can construct a Hadamard design with classical parameters whose full automorphism group is isomorphic to G. Finally, taking a tensor product with a rigid design from Section V.1 gives a proof of Theorem V.3.3.

V.1. Rigidity

We begin this section by constructing Hadamard designs with no non–trivial automorphisms, which also have tractable properties in view of the constructions of Chapter III.

Theorem V.1.1. *If a Hadamard design of order $n > 2$ exists, there exist at least $\frac{(16n-2)!}{2^{10}n^3}$ pairwise non–isomorphic, tensor–indecomposable Hadamard designs of*

order $8n$ with exactly one good block, no good points, and no non–trivial automorphisms.

Proof. By Theorem IV.2.1, we may assume $\mathcal{D}$ has no good blocks. Set $\mathcal{D}_1 = \mathcal{D}\sigma(\mathcal{D}^*)^+$, where σ is chosen as in corollary III.1.6 so there exists a point q of $\mathcal{D}_1$ which is on no lines of size 3. We list some properties of $\mathcal{D}_1$.

1.1 *$\mathcal{D}_1$ has a unique good block, B_∞.* For, $\mathcal{D}$ has no good blocks, so equation (III.1.3) rules out any other good blocks.

1.2 *$\mathcal{D}_1$ has no good points.* For, a good point would be on a line of size 3 with q, which is ruled out.

1.3 *Any automorphism inducing the identity on B_∞ is the identity.* For, any such automorphism would fix the parallel classes of $D_1^{B_\infty} = (\mathcal{D}^*)^+$, hence induce a translation of that affine design. However, $\mathcal{D}$ has no good blocks, so $\mathcal{D}^*$ has no good points. Therefore, Lemma II.2.1 implies $(\mathcal{D}^*)^+$ has no translations.

1.4 *$\mathcal{D}_1$ is tensor–indecomposable.* For, the point q is on no lines of size 3, hence use corollary III.2.5.

We now define $\mathcal{D}_2 = \mathcal{D}_1\tau\mathcal{D}_1^+$ for a carefully chosen τ. Let $\hat{B}$ denote the unique good block of $\mathcal{D}_1$ (this notation is used so as not to confuse it with the new block B_∞ of $\mathcal{D}_2$). Fix a point of $p \in \hat{B}$, so that p is on $2n-1$ blocks of $\mathcal{D}_{1(\hat{B})} = \mathcal{D}$. These blocks are of the form $B_i \cap \hat{B}$, where $B_i \neq \hat{B}$ is a block of $\mathcal{D}_1$ containing p. So, let $B_1, B_2, \ldots, B_{2n-1}$ be $2n-1$ blocks inducing those blocks of $\mathcal{D}_{1(\hat{B})}$ (note that we have

2 choices for each block). Let C be an arbitrary block not containing p. Set $\tau = \sigma_0 t$ where σ_0 is as in note III.1.9 and t is the following element of the symmetric group on the blocks of $\mathcal{D}_1$.

$$t = (\hat{B}, B_1, B_2, \ldots, B_{2n-2}, C).$$

Properties of $\mathcal{D}_2$:

2.1 *B_∞ is the unique good block of $\mathcal{D}_2$.* Recall that equation (III.1.3) shows that any other good block must arise as the union of a good block of $\mathcal{D}_1^+$ and a good block of $\mathcal{D}_1$. Since $\hat{B} \in \mathrm{supp}(t)$, this does not happen, as although $\hat{B}$ is good, $\hat{B}^t = B_1$ is not.

2.2 *$\mathcal{D}_2$ has no good points on B_∞.* Otherwise, the elation given by Theorem II.2.7 would induce a translation of $\mathcal{D}_2^{B_\infty} = \mathcal{D}_1^+$, which is impossible by Lemma II.2.1 since $\mathcal{D}_1$ has no good points, by property 1.2 of $\mathcal{D}_1$.

2.3 *$\mathcal{D}_2$ has no good points off B_∞.* For, such a good point would imply that $\mathcal{D}_2 \cong \mathcal{D}_1 \sigma_0 \mathcal{D}_1^+$ by Theorem II.2.6. Setting $G_1 = \mathrm{Aut}(\mathcal{D}_1)$ in its permutation representation on the blocks of $\mathcal{D}_1$ and $\overline{G_1} = \mathrm{Aut}(\mathcal{D}_1^+)$ in its representation on the parallel classes of blocks of $\mathcal{D}_1^+$, the assumed isomorphism and lemma IV.1.1 give $\tau \in \overline{G_1}\sigma_0 G_1$.

On the other hand, $\overline{G_1}$ fixes $\overline{\hat{B}}$, since it is the unique good parallel class of $\mathcal{D}_1^+$, and G_1 fixes $\hat{B}$, since it is the unique good block of $\mathcal{D}_1$. Thus, any element of $\overline{G_1}\sigma_0 G_1$ sends $\overline{\hat{B}}$ to $\hat{B}$. However, $\overline{\hat{B}}^\tau = B_1$, so no isomorphism is possible.

2.4 $\mathcal{D}_2$ *is tensor–indecomposable* by corollary III.2.18, as $\mathcal{D}_1$ is indecomposable, by property 1.4.

2.5 $\mathcal{D}_2$ *has a point moved by any non–trivial automorphism.*

Proof. We'll show p_∞ behaves as stated: if $g \in \mathrm{Aut}(\mathcal{D}_2)$ fixes p_∞, we will show $g = 1$.

By Corollary III.1.8, g induces a $g_1 \in G_1$ and a $g_2 \in \mathrm{Aut}(\mathcal{D}^+)$ which induces a $\overline{g_2} \in \overline{G_1}$ on parallel classes (G_1 and $\overline{G_1}$ as in property 2.3 above), with $g_1 = \overline{g_2}^\tau$. Since g fixes p_∞, so does g_2. Thus, g_2 fixes (as a set) the blocks on p_∞, and restricted to those blocks g_2 induces an automorphism g_2^* of $(\mathcal{D}_1^+)_{p_\infty} = \mathcal{D}_1$. Since one member of each parallel class contains p_∞, the action of g_2^* on those blocks can be deduced from the action of $\overline{g_2}$ on parallel classes. In fact, since σ_0 associates to each parallel class of $\mathcal{D}_1^+$ the member of the parallel class containing p_∞, we see $g_2^* = \overline{g_2}^{\sigma_0}$ in its representation on blocks of $\mathcal{D}_1$.

Since $g_1 = \overline{g_2}^\tau = \overline{g_2}^{\sigma_0 t} = (g_2^*)^t$, we have:

$$g_1(g_2^*)^{-1} = \overline{g_2}^\tau (g_2^*)^{-1} = t^{-1}\overline{g_2}^{\sigma_0} t (g_2^*)^{-1} = t^{-1} t^{(g_2^*)^{-1}}.$$

A priori, the support of $g_1(g_2^*)^{-1} = t^{-1}t^{(g_2^*)^{-1}}$ is at most twice the size of the support of t. However, *both of the automorphisms* $(g_2^*)^{-1}$ *and* $g_1(g_2^*)^{-1}$ must fix $\hat{B}$. Thus,

$$\hat{B}^{g_1(g_2^*)^{-1}} = \hat{B}^{t^{-1}g_2^* t^{-1}(g_2^*)^{-1}} = \hat{B}$$

implies:

$$\hat{B}^{t^{-1}} = C = \hat{B}^{g_2^* t^{-1} (g_2^*)^{-1}} = C^{(g_2^*)^{-1}},$$

so g_2^* fixes C. Therefore,

$$|\mathrm{supp}(g_1 (g_2^*)^{-1})| \leq 2(|\mathrm{supp}(t)| - 1) = 4n - 2.$$

Thus, $g_1 (g_2^*)^{-1}$ fixes at least $4n + 1$ blocks, implying $g_1 (g_2^*)^{-1} = 1$, by fact IV.1.3 since $\mathcal{D}_1$ is of order $2n$. So, $g_1 = g_2^*$ and g_1 commutes with t. Since g_1 centralizes t and fixes $\hat{B}$, g_1 must fix all elements of $\mathrm{supp}(t)$. Thus, g_1 induces an automorphism g_1^* of $\mathcal{D}_{1(\hat{B})}$ fixing *all but at most one block on* p, so g_1^* must fix *all* blocks on p (since $\lambda < k - 1$ for any Hadamard design). Additionally, g_1^* fixes the block $C \cap \hat{B}$ of $\mathcal{D}_{1(\hat{B})}$ which means g_1^* fixes at least $2n$ blocks of $\mathcal{D}_{1(\hat{B})}$. Thus, by fact IV.1.3, g_1^* is the identity, as $\mathcal{D}_{1(\hat{B})} = \mathcal{D}$ is of order n. Thus, g_1 induces the identity on $\mathcal{D}_{1(\hat{B})}$ and thus g_1 is the identity on $\mathcal{D}_1$ by property 1.3 of $\mathcal{D}_1$. Since g_1 is the identity on blocks, $\overline{g_2} = g_1^{\gamma^{-1}}$ is the identity on parallel classes, meaning g_2 is the identity, or a translation. Since g_2 fixes p_∞, it must be the identity (recall that translations are fixed point free). Thus, any $g \in \mathrm{Aut}(\mathcal{D}_2)$ which fixes the point p_∞ must be the identity.

2.6 $|\mathrm{Aut}(\mathcal{D}_2)| \leq 8n$ and $|\mathrm{Aut}(\mathcal{D}_2^+)| \leq 16n(8n)$. Since p_∞ is fixed by no non–trivial automorphism, $|\mathrm{Aut}(\mathcal{D}_2)|$ is equal to the size of the orbit of p_∞, which is at most $8n$, since p_∞ is off the unique good block of $\mathcal{D}_2$. $\mathrm{Aut}(D_2^+)$ is bounded as in Lemma IV.1.4, as $\mathcal{D}_2^+$ is formed by adding another point, whose orbit size

is at most $16n$.

Since $\mathcal{D}_2$ has a point not fixed by any non-trivial automorphism, $\mathcal{D}_2^*$ has a block with that property, call this block $\tilde{B}$. Also, $\mathcal{D}_2$ has a unique good block we'll call C_2 (again, so as not to confuse it with the new B_∞ in the following construction) which induces the unique good parallel class $\overline{C_2}$ of $\mathcal{D}_2^+$. Set $\mathcal{D}_3 = \mathcal{D}_2^*\gamma\mathcal{D}_2^+$ where $\overline{C_2}^\gamma = \tilde{B}$, and γ is otherwise arbitrary. Note that there are $(16n-2)!$ choices for γ, as $\mathcal{D}_2$ is of order $4n$.

$\mathcal{D}_3$ has the following properties:

3.1 $\mathcal{D}_3$ *has only one good block.* For, since $\mathcal{D}_2$ has no good points by 2.2 and 2.3, $\mathcal{D}_2^*$ has no good blocks, so again, equation (III.1.3) ensures that B_∞ is the only good block of $\mathcal{D}_3$.

3.2 $\mathcal{D}_3$ *has no good points on* B_∞. For, just as with the construction of $\mathcal{D}_2$, such a good point would induce an elation by Theorem II.2.7, which would induce a translation of $\mathcal{D}_3^{B_\infty} = \mathcal{D}_2^+$. This is impossible by Lemma II.2.1, since $\mathcal{D}_2$ has no good points, again by 2.2 and 2.3.

3.3 $\mathcal{D}_3$ *has no good points off* B_∞. Otherwise by Theorem II.2.7, we would have $\mathcal{D}_3 \cong \mathcal{D}_2^*\sigma_0\mathcal{D}_2^{*+}$, which would imply $(\mathcal{D}_3)_{B_\infty} = \mathcal{D}_2^+ \cong \mathcal{D}_2^{*+}$. But, $\mathcal{D}_2^+$ has a good parallel class, $\overline{C_2}$. However, $\mathcal{D}_2$ has no good points, by properties 2.2 and 2.3, so $\mathcal{D}_2^*$ has no good blocks, so $\mathcal{D}_2^{*+}$ has no good parallel classes. Thus, $\mathcal{D}_2^{*+} \ncong \mathcal{D}_2^+$.

3.4 $\mathcal{D}_3$ *is tensor–indecomposable* by Corollary III.2.18, as $\mathcal{D}_2$ is, by 2.4.

3.5 $\mathrm{Aut}(\mathcal{D}_3) = 1$. For, any $g \in \mathrm{Aut}(\mathcal{D}_3)$ induces a $g_2 \in \mathrm{Aut}(\mathcal{D}_2^+)$, acting as $\overline{g_2}$ on parallel classes, which must fix $\overline{C_2}$ (as $\overline{C_2}$ is the unique good parallel class of $\mathcal{D}_2^+$), and a $g_1 \in \mathrm{Aut}(\mathcal{D}_2^*)$. By lemma III.1.7: $g_1 = \overline{g_2}^\gamma$, and since $\overline{C}^\gamma = \tilde{B}$, g_1 must fix $\tilde{B}$, implying that g_1 is the identity (because $\tilde{B}$ was chosen to be the block moved by any non–trivial automorphism). Thus, $\overline{g_2}$ is the identity on parallel classes of blocks. Since $\mathcal{D}_2^+$ does not admit translations (again by Lemma II.2.1 and the fact $\mathcal{D}_2$ has no good points, by 2.2 and 2.3), g_2 must be the identity. Thus, g fixes all blocks of $\mathcal{D}_3$, so must be the identity.

3.6 *There are at least* $\dfrac{(16n-2)!}{2^{10}n^3}$ *non–isomorphic choices for* $\mathcal{D}_3$. Since $\mathcal{D}_2^*$ has no good blocks, we may adapt the proof of corollary IV.1.2, taking into account our restriction for γ, and our upper bounds on $|\mathrm{Aut}(\mathcal{D}_2^*)| = |\mathrm{Aut}(\mathcal{D}_2)|$ and $|\mathrm{Aut}(\mathcal{D}_2^+)|$ given in 2.6. □

V.2. GMW Designs

This Section describes a family of Hadamard designs with classical parameters whose automorphism groups have been completely determined. Applying the doubling procedure to these designs will yield designs with classical parameters and arbitrary automorphism groups in Section V.3.

GMW designs are symmetric designs arising from certain difference sets, and have the same parameters as projective spaces. For a definition and basic properties, see [2, Section VI, 17]. Additionally, [9, Theorem 1] gives the full automorphism group of

such designs, as well as determining when they are isomorphic. This is also proven in [3, Theorem 1.2], without the use of the classification of finite simple groups. We will not need the full generality of the theorems in those papers, but use the following:

Fact V.2.1. *For any integer $N > 1$, there exists a Hadamard GMW design $\mathcal{D}$ with parameters $2-(2^{3N}-1, 2^{3N-1}-1, 2^{3N-2}-1)$, such that $Aut(\mathcal{D}) \cong \Gamma\mathrm{L}(N, 8)$ in its natural action on non-zero vectors of $\mathbb{F}_8^N$.*

The field size 8 here is entirely arbitrary, any power of 2 greater than 4 will do. Note that while the designs in question have the same parameters as a projective space of dimension $3N-1$ over $\mathbb{F}_2$, they are not isomorphic to projective spaces, as their automorphism groups are too small. Other differences are also apparent:

Observation V.2.2. *The designs of fact V.2.1 have no good points or blocks, and are tensor–indecomposable.*

Proof. Since the automorphism group is point/block transitive, one good point/block would imply that all points/blocks are good, contradicting the Dembowski-Wagner Theorem [2, Theorem XII.2.10], as these designs are not projective spaces. Also, the transitive automorphism group ensures that these designs are tensor–indecomposable by Lemma III.2.10. □

Lemma V.2.3. *Let $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ be a GMW design as given in fact V.2.1. Then $Aut(\mathcal{D}^+) = Aut(\mathcal{D})$.*

Proof. Set $G = \mathrm{Aut}(\mathcal{D}^+)$. We need to show that G fixes the point p_∞. Assume that p_∞ is moved. Then G is 2–transitive on points, as the subgroup fixing p_∞ is already known to be transitive on the remaining points.

Claim: $G \cong \mathrm{A\Gamma L}(N, 8)$. By V.2.1, we have $G_{p_\infty} = \mathrm{Aut}(\mathcal{D}) \cong \Gamma\mathrm{L}(N, 8)$. Consider the subgroup $T < G_{p_\infty}$ consisting of transvections fixing a common hyperplane (see [19, Ch. 4] for relevant definitions). $|T| = 8^{N-1}$, T fixes 8^{N-1} points (including p_∞), and any other such subgroup of $G_{p_\infty} \cong \Gamma\mathrm{L}(N, 8)$ is conjugate to T in G_{p_∞}. Set $H = \mathrm{Fix}(T) \subset \mathcal{P} \cup \{p_\infty\}$ and consider the incidence structure $\mathcal{D}' = (\mathcal{P} \cup \{p_\infty\}, H^G)$. Since G is 2–transitive, this is a design. Some properties of $\mathcal{D}'$:

1. If $g \in G$ and $p_\infty \in H^g$, then $H^g \in H^{G_{p_\infty}}$ as $H^g = \mathrm{Fix}(T^g)$, so T and T^g are G_{p_∞} conjugate.

2. Thus, the number of blocks of $\mathcal{D}'$ on p_∞ is the number of conjugates of T in G_{p_∞}, which in turn is the number of hyperplanes of a vector space of dimension N over $\mathbb{F}_8$, which is $\dfrac{8^N - 1}{7}$. Thus, $\mathcal{D}'$ has parameters $v = 8^N, k = |H| = 8^{N-1}$, and $r = \dfrac{8^N - 1}{7}$. Therefore, the parameters of $\mathcal{D}'$ are the same as $\mathcal{AG}(N, 8)$. However, we do not yet know that the $\mathcal{D}'$ is, in fact, classical.

3. Let $H_1 \neq H_2 \in H^G$ with $H_1 \cap H_2 \neq \phi$. By transitivity of $\mathrm{Aut}(\mathcal{D}')$, we may assume $p_\infty \in H_1 \cap H_2$. The remaining points of $H_1 \cap H_2$ are those points fixed by 2 distinct conjugates of T in G_{p_∞}. But these are just the non–zero points contained in the intersection of 2 hyperplanes of $\mathbb{F}_8^N$. Thus, $|H_1 \cap H_2| = 8^{N-2}$.

Furthermore, there are exactly 9 conjugates of T pointwise fixing $H_1 \cap H_2$, so there are exactly 9 blocks containing $H_1 \cap H_2$. Since these 9 blocks cannot pairwise intersect outside of $H_1 \cap H_2$, they partition $\mathcal{P} \cup \{p_\infty\} - (H_1 \cap H_2)$.

By [6, Thm. 1], the above 3 properties imply $\mathcal{D}' \cong \mathcal{AG}(N, 8)$, proving the claim that $G \cong A\Gamma\mathrm{L}(N, 8)$. Therefore, $G \cong G_{p_\infty} \ltimes V$, where $V = \mathbb{F}_8^N$.

Finally, we return to the original design $\mathcal{D}^+$ by considering the (point–transitive, hence point–regular) action of $V = \mathbb{F}_8^N$ on the blocks of $\mathcal{D}^+$. Since there are $2^{3N-1}-1$ parallel classes in $\mathcal{D}^+, V$ must fix at least one: $\{B, B^c\}$. Then, V has a subgroup W of index 2 fixing B, hence acting regularly on the points of B. Thus, B can be identified with W, a hyperplane of $\mathcal{AG}(V)$, so by transitivity, all blocks can be identified with hyperplanes. Therefore, $\mathcal{D}^+ \cong \mathcal{AG}(3n, 2)$, which in turn implies that $\mathcal{D} \cong \mathcal{PG}(3N-1, 2)$, and $\mathrm{Aut}(\mathcal{D}) \cong GL(3N, 2)$ contradicting fact V.2.1 . □

Note that this proof can also be done by simply citing [18, Thm. 1.1], which classifies *all* affine designs admitting a 2–transitive action on points. However, the above proof is included for completeness, and does not require the classification of finite simple groups.

V.3. Arbitrary Automorphism Groups

In light of Theorem III.1.8, we now show that any group is isomorphic to the intersection of two conjugate copies of $\Gamma\mathrm{L}(N, 8)$ within the symmetric group $\mathbf{S}_{8^N-1}$ for suitably chosen N. The lemma below is adapted from [9]. A similar argument

can be found in [8, Lemma 10.3].

Lemma V.3.1. *Let G be a finite group, with $N > 4|G| + 2$. There exists $\sigma \in \mathbf{S}_{8^N-1}$ such that $G \cong \Gamma\mathrm{L}(N,8) \cap \Gamma\mathrm{L}(N,8)^\sigma$.*

Proof. Throughout, we will be considering the action of the groups $\mathbf{S}_{8^N-1}, G$ and $\Gamma\mathrm{L}(N,8)$ on non-zero vectors of $\mathbb{F}_8^N$, so notation involving span and direct sum will always be assumed to have the zero vector removed. Let $K = \mathbb{F}_{8^2}$ and set

$$\mathbb{F}_8^N = (\oplus_g Kx_g) \oplus Ku \oplus \langle Y \rangle,$$

where Y is some set of more than $2|G|$ linearly independent vectors. G acts on $\mathbb{F}_8^N$ via $(Kx_g)^h = Kx_{gh}$ while pointwise fixing Ku and $\langle Y \rangle$. Fix $y_0 \in Y_0 \subseteq Y$ where $|Y_0| = 2|G|$.

Now, set π to be the product of 2 disjoint cycles π_1 and π_2, both pointwise fixing Kx_1 and Ku, with π_1 a 6–cycle permuting all but 1 non–zero vector of a 1–space of $Kx_1 \oplus Ku$, and π_2 a $(8^4 - 2(8^2) - 5)$–cycle acting on the remaining non–zero vectors of $Kx_1 \oplus Ku$. Set π' to be the product of 2 disjoint cycles π_1' and π_2', both pointwise fixing Kx_1 and Ky_0, with π_1' a 6–cycle permuting all but 1 non–zero vector of a 1–space of $Kx_1 \oplus Ky_0$ and π_2' a $(8^4 - 2(8^2) - 6)$-cycle on $Kx_1 \oplus Ky_0$, whose support contains the remaining non–zero vector of the 1–space spanned by the support of π_1'. Set π_* to be the product of 2 disjoint cycles π_{1*} and π_{2*}, both pointwise fixing Ku and $\langle Y \rangle$, where π_{1*} is a 6–cycle on all but 1 non–zero vector of a 1–space, and π_{2*} a $(8^{2+|Y|} - 8^{|Y|} - 8^2 - 5)$–cycle on the remaining non–zero vectors of $Ku \oplus \langle Y \rangle$. Whenever

$1 \neq g \in G$ let π_g denote the product of 2 disjoint cycles, both pointwise fixing $Kx_1 \oplus \langle x_g \rangle$ and $Kx_1 \oplus \langle Y_0 \rangle$, π_{1g} is a 6–cycle permuting all but 1 non–zero vector of a 1–space, and π_{2g} a cycle of length greater than $8^{2+|Y_0|}$ whose support spans exactly $Kx_1 \oplus \langle x_g \rangle \oplus \langle Y_0 \rangle$. Furthermore, choose π_{2g} in such a way that the length of the cycle differs for distinct g. This is possible, as $|G| < 8^{3+|Y_0|} - (8^3 + 8^{|Y_0|} + 8^{2+|Y_0|} + 6)$. For all $h \in G$ define σ to be

- π^h on $(Kx_1 \oplus Ku)^h = Kx_h \oplus Ku$,
- π'^h on $(Kx_1 \oplus Ky_0)^h = Kx_h \oplus Ky_0$,
- π_g^h on $(Kx_1 \oplus \langle x_g \rangle \oplus \langle Y_0 \rangle)^h = Kx_h \oplus \langle x_{gh} \rangle \oplus \langle Y_0 \rangle$ whenever $g \neq 1$, and
- π_* on $Ku \oplus \langle Y \rangle$.

Then: $G \leq \Gamma\mathrm{L}(N,8) \cap \Gamma\mathrm{L}(N,8)^\sigma$, as all elements of G commute with σ; we are going to prove equality here.

Now, suppose we have $\alpha, \beta \in \Gamma\mathrm{L}(N,8)$ such that $\alpha = \beta^\sigma$. Then we have $\alpha^{-1}\beta = \sigma^{-1}\sigma^\beta \in \Gamma\mathrm{L}(N,8)$. But the support of $\sigma^{-1}\sigma^\beta$ has size at most:

$$2|\mathrm{supp}(\sigma)| \leq 2(8^4 2|G| + 8^{3+|Y_0|}|G|(|G|-1) + 8^{2+|Y|}) < 8^N - 8^{N-1}$$

and therefore $\alpha^{-1}\beta$ is the identity, as no non-trivial element of $\Gamma\mathrm{L}(N,8)$ can fix more than 8^{N-1} non–zero vectors of $\mathbb{F}_8^N$. Thus, σ centralizes α. Then α permutes the cycles of σ. Since $8^{2+|Y|} - 8^{|Y|} > 8^{3+|Y_0|} - 8^{2+|Y_0|}$, π_{2*} is a longer cycle than any of the π_{2g}, and hence is the longest cycle of σ. Thus, α must stabilize the support of π_{2*}. Also, α

permutes the 6–cycles of σ, hence must permute the 1–spaces they determine. Thus, α must fix the single vector in the intersection of those 1–spaces and the support of π_{2*}. Since α fixes this vector and commutes with π_{2*}, it must fix all vectors in the support of π_{2*}. This set contains a basis for $Ku \oplus \langle Y \rangle$, so α must be the identity on this subspace. In particular, α is linear.

If $(Kx_1 \oplus Ku)^\alpha = Kx_h \oplus Ku$ then we may replace α with αh^{-1} and assume $Kx_1 \oplus Ku$ is left invariant by α. This means that α commutes with π, hence must stabilize the support of π_2. Again, this support intersects the 1–spaces determined by all the 6–cycles of σ in a single vector, implying that α pointwise fixes the support of π_2. Again, this set contains a basis of $Kx_1 \oplus Ku$, so α induces the identity on $Kx_1 \oplus Ku$. Note that if $|G| = 1$ we are finished, as in that case $\mathbb{F}_8^N = Kx_1 \oplus Ku \oplus \langle Y \rangle$, so we have shown that α is the identity. Therefore, we may assume $|G| > 1$.

α must permute the cycles of length $8^4 - 2(8^2) - 5$, as well as the cycles of length $8^4 - 2(8^2) - 6$. Thus, for all $h \in G$, there exists $h^*, \overline{h} \in G$ satisfying $(Kx_h \oplus Ku)^\alpha = Kx_{\overline{h}} \oplus Ku$ and $(Kx_h \oplus Ky_0)^\alpha = Kx_{h^*} \oplus Ky_0$. Then $(Kx_h)^\alpha \subseteq (Kx_{\overline{h}} \oplus Ku) \cap (Kx_{h^*} \oplus Ky_0)$ implies that $(Kx_h)^\alpha = Kx_{h^*} = Kx_{\overline{h}}$, since Ku and Ky_0 are fixed by α. Thus, the "basic" subspaces Kx_h are permuted by α.

Let $g \neq 1$. Then the cycles π_{2g} are of distinct length for different g. α must permute these cycles, so for each h there is some h' such that

$$(Kx_h \oplus \langle x_{gh} \rangle \oplus \langle Y_0 \rangle)^\alpha = Kx_{h'} \oplus \langle x_{gh'} \rangle \oplus \langle Y_0 \rangle.$$

Then $Kx_{h^*} \oplus \langle x_{gh} \rangle^\alpha \subset Kx_{h'} \oplus \langle x_{gh'} \rangle \oplus \langle Y_0 \rangle$ so that $h' = h^*$, since $Kx_{h'}$ is the only

"basic" subspace of $Kx_{h'} \oplus \langle x_{gh'} \rangle \oplus \langle Y_0 \rangle$. This in turn implies that $\langle x_{gh} \rangle^\alpha = \langle x_{gh'} \rangle$. Since $\langle x_{gh} \rangle^\alpha \subset (Kx_{gh})^\alpha = Kx_{(gh)^*}$, it follows that $(gh)^* = gh' = gh^*$ for all $g \neq 1$ and h. Since 1^* is already known to be 1, setting $h = 1$, we see $g^* = g$, so that α stabilizes each Kx_g. Thus, $(Kx_g \oplus Ku)^\alpha = Kx_g \oplus Ku$, since $\alpha = 1$ on Ku. As before, this means that α must centralize π_2^h, and fix the vector it has in common with the 1–spaces determined by the 6–cycles, so α must pointwise fix the support of π_2^h. Again, this support contains a basis for $Kx_h \oplus Ku$, and therefore $\alpha = 1$ on this subspace. Thus, α is the identity, and we have shown $G = \Gamma\mathrm{L}(N, 8) \cap \Gamma\mathrm{L}(N, 8)^\sigma$. □

Corollary V.3.2. *For any finite group G and $N > 4|G| + 2$, there exists a tensor–indecomposable Hadamard design on $v = 2^{3N+1} - 1$ points with automorphism group isomorphic to G, a unique good block and no good points.*

Proof. Let $\mathcal{D}$ be a GMW design on $2^{3N} - 1$ points with $\mathrm{Aut}(\mathcal{D}) \cong \Gamma\mathrm{L}(N, 8)$, as in fact V.2.1. Since $\mathcal{D}$ is an abelian difference set design, it is self–dual. Thus, the permutation σ definined in lemma V.3.1, which acts on the points of $\mathcal{D}$, can be dualized to a permutation σ^* which acts on blocks of $\mathcal{D}$. Form $\mathcal{D}_G = \mathcal{D}\hat{\sigma}\mathcal{D}^+$, where $\hat{\sigma} = \sigma_0\sigma^*$. $\mathcal{D}_G$ has $2^{3N+1} - 1$ points. Since $\mathcal{D}$ has no good blocks by observation V.2.2, B_∞ is the unique good block of $\mathcal{D}\sigma\mathcal{D}^+$ by equation (III.1.3). Thus, corollary III.1.8 gives $\mathrm{Aut}(\mathcal{D}\sigma\mathcal{D}^+) \cong G$ as $\mathrm{Aut}(\mathcal{D}) = \mathrm{Aut}(\mathcal{D}^+)$ by lemma V.2.3. A good point off B_∞ would yield $\mathcal{D}_G \cong \mathcal{D}\sigma_0\mathcal{D}^+$ by fact II.2.6. However, $\Gamma\mathrm{L}(N, 8) \leq \mathrm{Aut}(\mathcal{D}\sigma_0\mathcal{D}^+)$, stabilizing B_∞, by corollary III.1.8 and $\Gamma\mathrm{L}(N, 8)$ is much larger than G. A good point on B_∞ would induce an elation by Theorem II.2.7 which in turn would induce

a translation of $\mathcal{D}^+$, contradicting fact II.2.1 and observation V.2.2. Since $\mathcal{D}$ is tensor–indecomposable by observation V.2.2, so is $\mathcal{D}_G$ by corollary III.2.18. □

Theorem V.3.3. *Given a finite group G and the existence of a Hadamard design of order n, then for all $N > 4|G| + 2$, there exist at least $\frac{(16n-2)!}{2^{10}n^3}$ non–isomorphic Hadamard designs $\mathcal{D}$ of order $2^{3N+4}n$ with $Aut(\mathcal{D}) \cong G$.*

Proof. Given a Hadamard design $\mathcal{D}$ of order n, form $\mathcal{D}_3$ of order $8n$ with $\mathrm{Aut}(\mathcal{D}_3) = 1$ as in Theorem V.1.1. Given G, form $\mathcal{D}_G$ of order 2^{3N-1} with $\mathrm{Aut}(\mathcal{D}_G) \cong G$ as in corollary V.3.2. Since neither $\mathcal{D}_3$ nor $\mathcal{D}_G$ has good points, we have $\mathrm{Aut}(\mathcal{D}_G \otimes \mathcal{D}_3) \cong G$ by corollary III.2.15. $\mathcal{D}_G \otimes \mathcal{D}_3$ is a Hadamard design of order $2^{3N+4}n$. There are $\frac{(16n-2)!}{2^{10}n^3}$ non–isomorphic choices for $\mathcal{D}_3$, inducing non–isomorphic designs $\mathcal{D}_3 \otimes \mathcal{D}_G$ by the unique factorization of corollary III.2.14. □

CHAPTER VI

FURTHER QUESTIONS

We conclude the thesis with a survey of some questions for further study.

- Theorem V.1.1 constructs rigid Hadamard designs by applying the doubling procedure 3 times to a Hadamard design with no good blocks. Can this be done more efficiently? In other words, given that a Hadamard design of order n exists, can it be shown that a rigid design of order $2n$ or even n exists? This is conjectured in [14].

- The rigid Hadamard designs constructed in Theorem V.1.1 may or may not have rigid affine completions. More troublesome is the fact that the corresponding matrices do admit non–trivial automorphisms, namely the "dual translations" induced by the good blocks of the designs. Can the proof be adapted so as to guarantee rigid matrices?

- Theorem IV.2.1 shows that if a Hadamard design of order n exists, a design with the same parameters, no good blocks and *at most one good point* exists. Can one construct a design with those parameters with *neither* good points nor blocks? This would require $n > 4$.

- The bound in Theorem IV.0.1 relies on the crude upper bound on the size of

the automorphism groups obtained in Lemma IV.1.4. A better bound would improve the Theorem proportionally. Does there exist a constant c such that, if $\mathcal{D}$ is a $2-(4n-1, 2n-1, n-1)$, then $|\mathrm{Aut}(\mathcal{D})| < c^n$?

- Theorem II.2.7 shows that a good flag induces an elation through the flag. However, this does not characterize elations of a Hadamard design. Indeed, one can construct (via the doubling procedure) a design admitting an elation through a flag with a good block, but non–good point. Can one construct a design admitting an elation through a flag where *neither* the point nor the block is good?

BIBLIOGRAPHY

[1] L. Babai, On the abstract group of automorphisms. *Combinatorics, proc. Eighth British Comb. Conf.* (ed. H.N.V. Temperley), Cambridge U. Press, Cambridge, (1981) 1–40.

[2] T. Beth, D. Jungnickel, H. Lenz, *Design Theory.* Cambridge University Press, Cambridge, 1999.

[3] U. Dempwolff, W.M. Kantor, Distorting symmetric designs. *in preparation*

[4] D.R. Hughes, F.C. Piper, *Design theory.* Cambridge University Press, Cambridge, 1985.

[5] D. Jungnickel, The number of designs with classical parameters grows exponentially. *Geometriae Dedicata* **16** (1984) 167–178.

[6] W.M. Kantor, Characterizations of finite projective and affine spaces. *Can. J. Math.* **21** (1969) 64-75.

[7] W. M. Kantor, Automorphism groups of Hadamard matrices. *J. Comb. Theory* **6** (1969), 279–281.

[8] W.M. Kantor, Automorphisms and isomorphisms of symmetric and affine designs. *J. Alg. Comb.* **3** (1994) 301–338.

[9] W.M. Kantor, Note on GMW Designs. *Europ. J. Comb.* **22** (2001) 63–69.

[10] W.M. Kantor, unpublished manuscript.

[11] Marion E. Kimberley, On the construction of certain Hadamard designs, *Math Z.* **119** (1971), 41–59

[12] M. E. Kimberley, On collineations of Hadamard designs. *J. Lond. Math. Soc.* **2** 6 (1973) 713–724.

[13] C. Lam, S. Lam, V.D. Tonchev, Bounds on the number of affine, symmetric and Hadamard designs and matrices. *JCT(A)* **92** (2000) 186–196.

[14] C. Lam, S. Lam, V.D. Tonchev, Bounds on the number of Hadamard designs of even order. *J. Comb. Designs* **9** (2001) 363–378.

[15] C. W. Norman, Hadamard designs with no non-trivial automorphisms. *Geom. Ded.* **2** (1976) 201–204.

[16] C. W. Norman, Non–isomorphic Hadamard designs. *JCT(A)* **21** (1976) 336–344.

[17] R. E. A. C. Paley, On orthogonal matrices. *J. Math. Phys.* **12** (1933), 311–320

[18] O. Pfaff, The classification of doubly transitive affine designs. *Des., Codes, Cryptogr.* **1** (1991) 207–217.

[19] D. E. Taylor, *T*he Geometry of the Classical Groups. Heldermann Verlag, Berlin, 1992

[20] J. A. Todd, A combinatorial problem. *J. Math. Phys.* **12** (1933), 321–333.

[21] J. Seberry Wallis, On the existence of Hadamard matrices. *J. Combinatorial Theory Ser. A* **21** (1976), no. 2, 188–195.