Delsarte Designs in Finite Groups

A Major Qualifying Project (MQP) Report
Submitted to the Faculty of
WORCESTER POLYTECHNIC INSTITUTE
in partial fulfillment of the requirements
for the Degree of Bachelor of Science in

Mathematical Sciences

By:

Sycamore Herlihy

Project Advisor:

William J. Martin

April 2024

Abstract

Let G be a dihedral group and let $\mathcal{T}$ be a collection of irreducible representations of G. In the simplest case, a subset C of G is a Delsarte $\mathcal{T}$-design if, for each representation ρ in $\mathcal{T}$, the matrix $\sum_{g \in C} \rho(g)$ has trace zero. Every finite group gives rise to an association scheme called the conjugacy class scheme of the group. This MQP explores Delsarte $\mathcal{T}$-designs in the context of this association scheme.

Contents

1 Introduction

Association schemes were first introduced by Bose and Shimamoto in 1952. In addition to use in the analysis of incomplete block designs by statisticians, association schemes are used to study combinatorial objects such as highly symmetric graphs, groups and codes [1, p. 343]. In the late 1960s, Philippe Delsarte studied commutative association schemes as a means to connect coding theory and design theory. Association schemes and Delsarte $\mathcal{T}$-designs are well-studied in classical groups like the symmetric and general linear groups (see [2]). However, these groups are quite abstract compared to the dihedral group—in a sense, the dihedral group is the "simplest" non-abelian group we can consider, due to its concrete presentation as the symmetries of an n-gon. Despite this fact, there are currently no results on Delsarte $\mathcal{T}$-designs in the dihedral group.

The remainder of the paper is organized as follows. In the latter half of this section we have a review of and some elaboration on topics from undergraduate mathematics; we hope that this paper can be understood by any student familiar with the standard undergraduate linear and abstract algebra sequences. Section 2 reviews the basic theory of commutative association schemes for any finite set, after which we shift our focus to only the conjugacy class association scheme of a finite group for the remainder of the paper. In Section 3 we give a very brief introduction to representation and character theory, with the goal being to provide just enough information to motivate later results and discussions. Section 4 introduces Delsarte theory, the main focus of the project. This section is broad—we present the theory so that it is applicable for any finite group. We also briefly introduce some topics in coding theory to show a natural duality between codes and designs. Finally in Sections 5 and 6 we focus entirely on the dihedral groups. We first present the structure and construct the conjugacy class association scheme for D_{2n}, then describe the irreducible representations and characters. Then in Section 6 we discuss the Delsarte theory of the dihedral groups, presenting a number of theorems, conjectures, and open questions. Included in these theorems is a complete classification of designs corresponding to the one-dimensional irreducible representations in addition to an interchangibility theorem regarding designs in these same representations. We also characterize some designs that exist in any dihedral group, and make a conjecture about the structure of designs afforded by dihedral subgroups.

As promised, we begin with topics from undergraduate algebra below.

Definition. [3, p. 41] A *group action* of a group G on a set X is a map from $G \times X$ to X (written as $g \cdot x$, for all $g \in G$ and $x \in X$) satisfying the following properties:

1. $g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x$, for all $g_1, g_2 \in G, x \in X$, and
2. $1 \cdot x = x$, for all $x \in X$.

Theorem 1.1. *[3, p. 114] Let G be a group acting on the nonempty set X. The relation on X defined by*

$$y \sim x \text{ if and only if } y = g \cdot x \text{ for some } g \in G$$

is an equivalence relation.

Proof. By axiom 2 of a group action we have $y = 1 \cdot y$ for all $y \in X$, so $\sim$ is reflexive. If $y \sim x$ then $y = g \cdot x$ for some $g \in G$, meaning $g^{-1} \cdot y = g^{-1} \cdot (g \cdot x)$, or $x = g^{-1}y$. Thus $x \sim y$ so $\sim$ is symmetric. If we additionally have $x \sim z$, then $x = g' \cdot z$ for some $g' \in G$ so $y = g \cdot (g' \cdot z) = (gg') \cdot z$. So $\sim$ is also transitive and therefore is an equivalence relation on A. □

In particular we consider the action of G on itself by *conjugation*, where

$$g \cdot x = gxg^{-1} \text{ for all } g \in G, x \in G.$$

We say that two elements x and y of G are *conjugate* in G if there is some $g \in G$ such that $y = gxg^{-1}$ [3, p. 123]. By Theorem 1.1, the orbits of this action partition G into equivalence classes called *conjugacy classes*. We denote these conjugacy classes by $\mathcal{C}_0, \mathcal{C}_1, \cdots, \mathcal{C}_d$, so that $d+1$ gives the number of conjugacy classes.

Example. Let G be an abelian group and let $a, b \in G$. Then $aba^{-1} = aa^{-1}b = b$, so all conjugacy classes have only one element.

We remark that in every group G, every element $b \in Z(G)$ lies in a conjugacy class of size one, since $gbg^{-1} = gg^{-1}b = b$. From here on, our convention is that $\mathcal{C}_0 = \{1_G\}$. We finally have one useful lemma:

Lemma 1.2. *Let $\mathcal{C}_i$ be a conjugacy class of a group G. Then the set $\mathcal{C}_i^{-1} := \{x^{-1} : x \in \mathcal{C}_i\}$ is also a conjugacy class of G.*

Proof. Let $\mathcal{C}_i$ be some conjugacy class of a group G. Then by definition we have that, for all $g \in G$, $g^{-1}\mathcal{C}_i g = \mathcal{C}_i$. Taking inverses gives $g^{-1}\mathcal{C}_i^{-1}g = \mathcal{C}_i^{-1}$, where $\mathcal{C}_i^{-1}$. So $\mathcal{C}_i^{-1}$ is stable under conjugation and thus also a conjugacy class. □

We comment that it is not true in general that $\mathcal{C}_i^{-1} = \mathcal{C}_i$.

Definition. [3, p. 169] For a group G and elements $x, y \in G$, let $[x, y] = xyx^{-1}y^{-1}$. This is known as the *commutator* of x and y and, furthermore, the group $G' = \langle [x, y] \mid x, y \in G \rangle$ is called the *commutator subgroup* of G.

Clearly, the commutator subgroup of an abelian group is simply the identity element 1_G. Let $a \in G'$ and $g \in G$ be given. Then $[g, a] = gag^{-1}a^{-1} \in G'$. Since G' is a subgroup we know $(gag^{-1}a^{-1})a \in G'$, but $(gag^{-1}a^{-1})a = gag^{-1}$. So we have shown that $gG'g^{-1} \subset G'$, meaning G' is normal. With this we also define the *abelianization* of G as the quotient group G/G', called as such because the resulting group is abelian.

Theorem 1.3. *[3, p. 169] For a normal subgroup H of G, G/H is abelian if and only if G' is a subgroup of H.*

The above theorem tells us that G/G' is the "largest" abelian quotient of G.

Definition. [3, p. 342] Let R be a commutative ring with identity. An *R-algebra* is a ring A together with a ring homomorphism $f : R \to A$ such that

1. $f(1_R) = 1_A$
2. $f(r)x = xf(r)$ for all $r \in R$ and $x \in A$

When R is a field, an R-algebra can be viewed as a vector space equipped with a bilinear product. As an example, the matrix algebra $M_n(R)$ is the set of $n \times n$ matrices with entries in the ring R.

We now have a collection of short definitions and a few results from linear algebra taken from [4]. For a matrix A, we denote the conjugate transpose of A by $A^\dagger$. A matrix A is *normal* if it satisfies $A^\dagger A = AA^\dagger$, and a matrix U is *unitary* if $U^\dagger U = UU^\dagger = I$. A matrix P is *idempotent* if $P^2 = P$; we say that two idempotents E, F are *orthogonal* if $EF = 0$ and that an idempotent P is *primitive* if there does not exist two orthogonal idempotents E, F such that $P = E + F$. Finally we present the following two theorems without proof:

Theorem 1.4. *A matrix A is normal if and only if it is unitarily diagonalizable; that is, there exists a unitary matrix P and a diagonal matrix D such that $A = PDP^{-1}$.*

Theorem 1.5. *Let $\{A_1, A_2, \dots, A_n\}$ be a set of diagonalizable matrices such that $A_iA_j = A_jA_i$ for all $1 \leq i, j \leq n$. Then $\{A_1, A_2, \dots, A_n\}$ are simultaneously diagonalizable; that is, there exists an invertible matrix P whose columns are common eigenvectors of $\{A_1, A_2, \dots, A_n\}$ so that $P^{-1}A_iP$ is diagonal for all A_i.*

2 Association Schemes

Let X be a finite set of size $n > 0$ and $\mathcal{R} = \{R_0, R_1, ..., R_d\}$ a set of $d+1$ relations on X. $(X, \mathcal{R})$ is an association scheme when the following conditions are satisfied [5, p. 44]:

(A1) R_0 is the diagonal relation, i.e. $R_0 = \{(x,x) \mid x \in X\}$.

(A2) $\mathcal{R}$ partitions $X \times X$.

(A3) For any $i \in \{0, 1, \ldots, d\}$ the relation $R_i^{-1} := \{(y,x) \mid (x,y) \in R_i\}$ also belongs to $\mathcal{R}$.

(A4) For all $i, j, k \in \{0, 1, \ldots, d\}$ and for all $(x,y) \in R_k$, the number

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

depends only on the choices of i, j, k.

If $(x,y) \in R_i$ we say that x and y are i^{th} *associates.* An association scheme is *symmetric* if $R_l = R_l^{-1}$ for all $0 \leq l \leq d$ and *commutative* if $p_{ij}^k = p_{ji}^k$ for all i, j, k. For our purposes, we will deal only with commutative association schemes. Later, we will display the intersection numbers with matrices L_i for $i = 0, \ldots, d$ so that the kj entry of L_i is equal to p_{ij}^k.

We can also describe an association scheme in terms of matrices. Build the 01-matrix A_i for $i \in \{0, 1, \cdots, d\}$ to be the $n \times n$ matrix with xy entry equal to 1 if $(x,y) \in R_i$, and 0 otherwise. So if we have a set of 01-matrices $\mathcal{A} = \{A_0, A_1, \ldots, A_d\}$, $(X, \mathcal{A})$ is an association scheme if [5, p. 45]

(B1) $A_0 = I$.

(B2) $\sum_{i=0}^d A_i = J$ where J is the matrix of all ones.

(B3) for any $i \in \{0, 1, \ldots, d\}$, $A_i^T \in \mathcal{A}$.

(B4) for all $i, j \in \{0, 1, \ldots, d\}$, $A_i A_j = \sum_{k=0}^d p_{ij}^k A_k$ for some scalars p_{ij}^k $(0 \leq i, j, k \leq d)$.

We call these the *adjacency matrices* of the scheme, and it is quickly seen that these criteria are equivalent to the conditions (A1)-(A4) above. Since $\mathcal{A}$ is a set of $d+1$ linearly independent matrices, the set $\{A_0, A_1, \ldots, A_d\}$ forms a basis for a $(d+1)$-dimensional subalgebra of $M_n(\mathbb{C})$ called the *Bose-Mesner algebra*, which we denote by $\mathbb{A}$. [6, p. 52]. We present some facts about $\mathcal{A}$.

Lemma 2.1. *Let $\mathcal{A} = \{A_0, A_1, \ldots, A_d\}$ be the adjacency matrices of a commutative association scheme. Then the matrices $A_0, A_1, \ldots, A_d$ are normal and pairwise commutative.*

Proof. That the matrices commute follows from property (B4) and the assumption of a commutative association scheme: $A_i A_j = \sum_{k=0}^d p_{ij}^k A_k = \sum_{k=0}^d p_{ji}^k A_k = A_j A_i$, so the matrices commute. Then we know from property (B3) that, for all $0 \leq i \leq d$, there exists $0 \leq j \leq d$ so that $A_i^T = A_j$. Thus $A_i^T A_i = A_j A_i = A_i A_j = A_i A_i^T$. So the matrices are normal. □

We now construct an additional basis for $\mathbb{A}$ following that of Bannai and Ito in [6]. Since the adjacency matrices A_i are normal and commute with each other, they are simultaneously diagonalizable by a unitary matrix. Let $B = \{u_0, \dots, u_{n-1}\}$ be an orthonormal basis of $\mathbb{C}^n$ where $A_i u_j = \lambda_{ij} u_j$ for all i, j and define the relation $\sim$ on B so that $u_j \sim u_k$ if $\lambda_{ij} = \lambda_{ik}$ for all $i = 0, 1, \dots, d$. It is immediately clear that $\sim$ is an equivalence relation. Denote the equivalence classes of this relation by $S_0, S_1, \dots, S_r$. Since the eigenspace of $J = \sum_{i=0}^{d} A_i$ corresponding to the eigenvalue n is equal to span$\{(1, 1, \dots, 1)\}$, without loss of generality we can set $S_0 = \{u_0\} = \{\frac{1}{\sqrt{n}}\mathbb{1}\}$.

We now define the matrices E_j by

$$E_j = \sum_{u_k \in S_j} u_k u_k^\dagger$$

for all $j = 0, \dots, r$ and for a matrix P set $P_{ji} = \lambda_{ik}$ for $u_k \in S_j$ so that $A_i = \sum_{j=0}^{r} P_{ji} E_j$ for all $i = 0, \dots, d$. We will use without proof that $r = d$, giving the following theorem from [6, p. 59–60].

Theorem 2.2. *The following properties hold:*

(i) $E_0 = \frac{1}{n} J$

(ii) $\sum_{i=0}^{d} E_i = I$

(iii) $E_i E_j = \delta_{ij} E_i$

(iv) $E_0, \dots, E_r$ *are linearly independent*

(v) each $E_j \in \text{span}\{A_0, \dots, A_d\}$

(vi) $r = d$

(vii) $E_i^\dagger = E_i$

Proof. (i) is easily seen since we defined $E_0 = u_0 u_0^\dagger = (1/n)\mathbb{1}\mathbb{1}^\dagger = (1/n)J$. Then we have $A_i = \sum_{j=0}^{d} P_{ji} E_j$, so $I = A_0 = \sum_{j=0}^{d} P_{j0} E_j = \sum_{j=0}^{d} E_j$, since $P_{j0} = 1$ for all j. So (ii) is proved. By definition

$$E_i E_j = (\sum_{u_k \in S_i} u_k u_k^\dagger)(\sum_{u_l \in S_j} u_l u_l^\dagger);$$

but $u_k^\dagger u_l = \delta_{kl} u_k$ since they are an orthonormal set. So $E_i E_j = \delta_{ij} E_i$ and (iii) is proved. That the E_j are linearly independent then follows from (iii), and (v) follows from (iv) and (vi) since we have a set of linearly independent matrices that span a space of dimension d. Finally $E_i^\dagger = (\sum_{u_j \in S_i} u_j u_j^\dagger)^\dagger = \sum_{u_j \in S_i} u_j u_j^\dagger = E_i$, so (vii) holds. □

Since $\{A_0, A_1, \dots, A_d\}$ and $\{E_0, E_1, \dots, E_d\}$ are both bases of $\mathbb{A}$, we can also express each E_i as a linear combination of the $A_j's$. Define the matrix Q such that

$$E_i = \frac{1}{n} \sum_{j=0}^{d} Q_{ji} A_j.$$

Then P and Q are referred to as the *first and second eigenmatrices* of the association scheme respectively [6, p. 60]. We note that $PQ = nI$.

Now we consider the entry-wise multiplication of matrices, so that for two matrices A, B of the same size we have $(A \circ B)_{ij} = A_{ij}B_{ij}$. This operation is also known as the *Hadamard product* of matrices. We first want to show that $\mathbb{A}$ is closed under the Hadamard product. Since the relations in our association scheme are disjoint and each A_i is a 01-matrix, we can see that

$$A_i \circ A_j = \delta_{ij} A_i.$$

So for $C, D \in \mathbb{A}$ with $C = c_0A_0 + \cdots + c_dA_d$ and $D = c_0A_0 + \cdots + c_dA_d$ we have

$$C \circ D = (c_0A_0 + \cdots + c_dA_d) \circ (c_0A_0 + \cdots + c_dA_d) = c_0d_0A_0 + \cdots + c_dd_dA_d.$$

So closure is proved. We can then write

$$E_i \circ E_j = \frac{1}{n}\sum_{k=0}^{d} q_{ij}^k E_k,$$

where we call the coefficients q_{ij}^k the *Krein parameters* of the scheme. We finish this discussion by observing a duality between $\{A_0, A_1, \ldots, A_d\}$ and $\{E_0, E_1, \ldots, E_d\}$:

$$\begin{array}{ll}
\sum A_i = J & \sum E_i = I \\
A_0 = I & E_0 = \frac{1}{n}J \\
A_iA_j = \sum p_{ij}^k A_k & E_i \circ E_j = \frac{1}{n}\sum_{k=0}^{d} q_{ij}^k E_k \\
A_i \circ A_j = \delta_{ij}A_i & E_iE_j = \delta_{ij}E_i \\
A_i = \sum P_{ji}E_j & E_j = \sum Q_{ji}A_j
\end{array}$$

In this paper, we apply this theory to study a particular association scheme on finite groups. Given a finite group G of size n, the *conjugacy class association scheme* with $X = G$ has the relations $\mathcal{R} = \{R_0, R_1, \ldots, R_d\}$ where $R_i = \{(x, y) \mid x^{-1}y \in \mathcal{C}_i\}$. We must prove that this does in fact satisfy the requirements of an association scheme. Consider $(x, y) \in R_0$. Then we have that $x^{-1}y \in \mathcal{C}_0$. Recalling that $\mathcal{C}_0 = \{1_G\}$ then gives $x = y$, showing that R_0 is the diagonal relation. Axiom (A2) follows from the fact that the conjugacy classes partition G. Next suppose we have x, y so that $x^{-1}y \in \mathcal{C}_i$. Given any $g \in G$ we then know that $g^{-1}x^{-1}yg \in \mathcal{C}_i$. Taking the inverse of both sides gives $g^{-1}y^{-1}xg \in \mathcal{C}_i^{-1} = \mathcal{C}_j$ for some $0 \leq j \leq d$, so $(y, x) \in R_j$ meaning the inverse of every relation exists and thus (A3) is proven. Now we must show (A4). Let $(x_1, y_1) \in R_k$ and $y \in \mathcal{C}_k$ be given. We want to show that the sets

$$\begin{aligned}
S_1 &= \{z \in G : (x_1, z) \in R_i, (z, y_1) \in R_j\} \\
&= \{z \in G : x_1^{-1}z \in \mathcal{C}_i \wedge z^{-1}y_1 \in \mathcal{C}_j\}, \\
S &= \{z \in \mathcal{C}_i : z^{-1}y \in \mathcal{C}_j\}
\end{aligned}$$

have the same size. Since $x_1^{-1}y_1 \in \mathcal{C}_k$, there exists g such that $g^{-1}x_1^{-1}y_1g = y$. We claim that $S_1 = x_1gSg^{-1}$. Let $z' \in S$. Then $z' \in \mathcal{C}_i$ and $z'^{-1}y \in \mathcal{C}_j$. If we take $z = x_1gz'g^{-1} \in x_1gSg^{-1}$ we find that $x_1^{-1}z = gz'g^{-1} \in \mathcal{C}_i$. Finally we see that $z^{-1}y_1 = gz'^{-1}g^{-1}x_1^{-1}y_1 = gz'^{-1}yg^{-1} \in \mathcal{C}_j$, so $z \in S_1$ meaning $S_1 = x_1gSg^{-1}$. So (A4) is proven, showing that we do have an association scheme.

Example. We will consider the conjugacy class association scheme of $\mathbb{Z}_n$. We have already shown that each conjugacy class in an abelian group has size 1, so the conjugacy classes of $\mathbb{Z}_n$ are given by $\mathcal{C}_i = \{i\}$ for $i = 0 \ldots n-1$. So each relation in $\{R_0, R_1, \ldots, R_{n-1}\}$ can be described by

$$R_b = \{(0,b), (1, b+1), \ldots, (n-b-1, n-1), (n-b, 0), (n-b+1, 1), \ldots, (n-1, b-1)\},$$

creating the associated adjacency matrix

$$A_b = \begin{array}{cc} \begin{array}{cccccccc} 0 & \cdots & b-1 & b & b+1 & b+2 & \cdots & n-1 \end{array} & \\ \begin{bmatrix} 0 & \cdots & 0 & 1 & \cdots & 0 & 0 & 0 \\ 0 & \cdots & 0 & 0 & 1 & \cdots & 0 & 0 \\ 0 & \cdots & 0 & 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 1 \\ 1 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 1 & 0 & 0 & 0 & \cdots & 0 \end{bmatrix} & \begin{array}{c} 0 \\ 1 \\ 2 \\ \vdots \\ n-b-1 \\ n-b \\ \vdots \\ n-1 \end{array} \end{array}$$

for all $b \in \mathbb{Z}_n$. We now want to find the parameters of the scheme. For the cyclic group, characterizing the intersection numbers proves to be simple; they are given by

$$p_{ij}^k = \begin{cases} 1, & i + j = k \pmod{n} \\ 0, & \text{otherwise.} \end{cases}$$

Similarly to the intersection numbers, we find that the Krein parameters for $\mathbb{Z}_n$ are given by

$$q_{ij}^k = \begin{cases} 1, & i + j = k \pmod{n} \\ 0, & \text{otherwise.} \end{cases}$$

So the cyclic group $\mathbb{Z}_n$ is a special case in which the intersection numbers and the Krein parameters are equal. We return to $\mathbb{Z}_n$ as an example again in Chapter 3.

3 Group Representations and Characters

In this chapter, we cover only the essentials of representation and character theory needed to motivate our results. The more interested reader should refer to [7], Ledermann's book "Introduction to Group Characters", from which the material below is taken unless another reference is given.

Recall that the general linear group $GL_n(\mathbb{F})$ is the group of $n \times n$ invertible matrices with entries in the field $\mathbb{F}$. It is well known that every finite group is isomorphic to a group of matrices. Since we have more tools to study the structure and properties of the general linear group than other groups, it is natural to want a connection between the two. We are interested primarily in homomorphisms into the general linear groups over the complex numbers as follows:

Definition. A degree n matrix representation of a group G is a group homomorphism $\rho : G \to GL_n(\mathbb{C})$.

Every group admits the trivial representation, or $\rho : G \to \mathbb{C}$ defined by $\rho(g) = 1$ for all group elements g. We are particularly concerned with *irreducible* representations, or a representation ρ so that no proper subspace of $\mathbb{C}^n$ is preserved by $\rho(g)$ for all $g \in G$. We note that all one-dimensional representations are irreducible, since there are no proper subspaces of $\mathbb{C}$. The function that sends each group element to the trace of the matrix $\rho(g)$ is called the *character* of the representation and is typically denoted by χ, so that $\chi(a) = \operatorname{tr} \rho(a)$. Note that if we have $a, b, g \in G$ such that $b = gag^{-1}$, then $\rho(b) = \rho(g)\rho(a)\rho(g)^{-1}$. Taking the trace gives

$$\begin{aligned}
\operatorname{tr} \rho(b) &= \operatorname{tr} \left[\rho(g)\rho(a)\rho(g)^{-1}\right] \\
&= \operatorname{tr} \left[\rho(g)^{-1}\rho(g)\rho(a)\right] \\
&= \operatorname{tr} \rho(a),
\end{aligned}$$

which we state as a lemma:

Lemma 3.1. *Let G be a finite group and $\rho : G \to GL_n(\mathbb{C})$ any representation with corresponding character $\chi(a) = \operatorname{tr} \rho(a)$. If a, b are conjugate elements then $\chi(a) = \chi(b)$.*

So these characters are examples of *class functions*, or functions that are constant over the conjugacy classes of a group. We will need one theorem from Ledermann (p. 49) below; this follows from an important theorem of Maschke's that every representation of a finite group G over $\mathbb{C}$ is equivalent to a direct sum of irreducible representations.

Theorem 3.2. *Let G be a group of order n. If G has $d + 1$ conjugacy classes, there are, up to equivalence, $d + 1$ distinct irreducible representations over $\mathbb{C}$ given by $\rho_0, \rho_1, \ldots, \rho_d$. If ρ_i is of degree n_i, then*

$$n = \sum_{i=0}^{d} n_i^2. \tag{1}$$

We will later use this theorem to determine completely the irreducible representations of a given group. Now let χ_i, χ_j be the characters of the representations ρ_i, ρ_j respectively and define their inner product by

$$\langle \chi_i, \chi_j \rangle = \frac{1}{|G|} \sum_{x \in G} \chi_i(x)\chi_j(x^{-1}).$$

Then we have the equations

$$\sum_{g\in G}\chi_i(g)\chi_j(g^{-1}) = |G|\delta_{ij} \tag{2}$$

$$\sum_{i=0}^{d}\chi_i(g_j)\chi_i(g_k^{-1}) = \frac{|G|}{|\mathcal{C}_j|}\delta_{jk} \tag{3}$$

where in (3) we have $g_j \in \mathcal{C}_j$ and $g_k \in \mathcal{C}_k$. These equations are known as the first and second orthogonality relations of characters respectively [7].

It is then convenient to display the characters in a table. Since all conjugate elements have the same character, and there are the same number of irreducible representations as there are conjugacy classes, the *character table* will have $d+1$ rows and $d+1$ columns. For our notation, the ij entry of the character table is the character χ_i evaluated at g_j for any $g_j \in \mathcal{C}_j$. We present an example of the character table for $G = D_{12}$ after a brief discussion of an important connection between the character table T and the previously mentioned second eigenmatrix Q of the conjugacy class association scheme. We will need the following well-known lemma:

Lemma 3.3 (Schur's Lemma)**.** *[7, p. 24] Suppose ρ, σ are irreducible representations of a finite group G with degrees m and n respectively. If there is a $n \times m$ matrix P such that $P\rho(g) = \sigma(g)P$ for all $g \in G$, then either*

(i) $P = 0$, or

(ii) $m = n$ and P is invertible.

Corollary 3.4. *In the second case above, we have $P = \lambda I$.*

For a given degree m irreducible representation ρ_j of G, some fixed $x \in G$, and $0 \le i \le d$, consider the sum $\sum_{x\sim_i y}\rho_j(y)$. The elements y of G that are i^{th} associates of x are those that satisfy $x^{-1}y = g$ for some $g \in \mathcal{C}_i$, so the sum can be rewritten as

$$\sum_{x\sim_i y}\rho_j(y) = \sum_{g\in\mathcal{C}_i}\rho_j(xg) = \rho_j(x)\sum_{g\in\mathcal{C}_i}\rho_j(g),$$

since ρ_j is a homomorphism. Now let $M = \sum_{g\in\mathcal{C}_i}\rho_j(g)$. Note that $\rho_j(x)\rho_j(g)\rho_j(x^{-1}) = \rho_j(xgx^{-1})$ and, since $g \in \mathcal{C}_i$, we also have $xgx^{-1} \in \mathcal{C}_i$. Putting this together gives

$$\rho_j(x)M\rho_j(x)^{-1} = \sum_{g\in\mathcal{C}_i}\rho_j(xgx^{-1}) = M,$$

since by the definition of a conjugacy class $h\mathcal{C}_i h^{-1} = \mathcal{C}_i$ for all $h \in G$. So we have $\rho_j(x)M = M\rho_j(x)$ and thus, by Schur's lemma, we know $M = \lambda I$ for some λ. Now we have

$$\sum_{x\sim_i y}\rho_j(y) = M\rho_j(x) = \lambda\rho_j(x).$$

Let

$$\mathbf{u}(x) = \begin{bmatrix}\rho_j(x)_{11} & \rho_j(x)_{12} & \cdots & \rho_j(x)_{mm}\end{bmatrix}$$

for all $x \in G$; then the $|G| \times m^2$ matrix U with the x^{th} row given by $\mathbf{u}(x)$ satisfies $A_i U = \lambda U$ for some λ.

Since $M = \lambda I$ and M is an $m \times m$ matrix, $\operatorname{tr} M = \lambda m$. Then for $g \in \mathcal{C}_i$, we have $\operatorname{tr} \rho_j(g) = \chi_j(g_i)$ for any $g_i \in \mathcal{C}_i$, since χ_j is a class function. This gives the equality

$$\lambda m = |\mathcal{C}_i| \chi_j(g_i) \implies \lambda = \chi_j(g_i) \frac{|\mathcal{C}_i|}{m}$$

noting $m = \chi_j(1_G)$; but recalling the second orthogonality relation for characters, we also have

$$\lambda = \frac{|\mathcal{C}_i| Q_{ji}}{k},$$

where k is the dimension of the λ-eigenspace. It follows from Maschke's theorem and the Wedderburn structure theorem [3, Thm 18.4] that the columns of U are linearly independent, so using (1) we have $k = m^2$. So finally

$$\chi_j(g_i) \frac{|\mathcal{C}_i|}{m} = \frac{|\mathcal{C}_i|}{m^2} Q_{ji},$$

implying that $Q_{ji} = m \chi_j(g_i)$ for $g_i \in \mathcal{C}_i$.

Example. The following are the character table and eigenmatrix Q in D_{12}.

$$Q = \begin{bmatrix} 1 & 1 & 1 & 1 & 4 & 4 \\ 1 & 1 & -1 & -1 & 2 & -2 \\ 1 & 1 & 1 & 1 & -2 & -2 \\ 1 & 1 & -1 & -1 & -4 & 4 \\ 1 & -1 & 1 & -1 & 0 & 0 \\ 1 & -1 & -1 & 1 & 0 & 0 \end{bmatrix}$$

char.	χ_0	χ_1	χ_2	χ_3	χ_4	χ_5
class						
$\mathcal{C}_0$	1	1	1	1	2	2
$\mathcal{C}_1$	1	1	−1	−1	1	−1
$\mathcal{C}_2$	1	1	1	1	−1	−1
$\mathcal{C}_3$	1	1	−1	−1	−2	2
$\mathcal{C}_4$	1	−1	1	−1	0	0
$\mathcal{C}_5$	1	−1	−1	1	0	0

Example. As an example, we come back to $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$. Since $\mathbb{Z}_n$ is abelian, we know that all the conjugacy classes have size one and thus all its representations are degree one. So for $\mathbb{Z}_5$, the adjacency matrices are

$$A_0 = I_5, A_1 = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix}, A_2 = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{bmatrix} A_3 = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}, A_4 = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}.$$

We note that for all $b \in \mathbb{Z}_n$, it holds that $A_b^{-1} = A_b^T$. This follows from the the orthogonality of permutation matrices. Similarly it is true that $A_b = (A_1)^b$ in $\mathbb{Z}_n$. We use these facts to simultaneously diagonalize the adjacency matrices of $\mathbb{Z}_n$ by first diagonalizing A_1.

It can be calculated easily that the characteristic polynomial of A_1 is given by $f(\lambda) = \lambda^n - 1$. Let $\omega = \exp(2\pi i/n)$, a primitive n^{th} root of unity. Then the eigenvalues of A_1 are given by $\{1, \omega, \omega^2, \ldots, \omega^{n-1}\}$.

With this we find that

$$\chi_j = \begin{bmatrix} \omega^0 \\ \omega^j \\ \omega^{2j} \\ \vdots \\ \omega^{(n-1)j} \end{bmatrix}$$

for $0 \leq j \leq n-1$ are the eigenvectors for A_1. So by letting

$$P = \begin{bmatrix} \vdots & \vdots & & \vdots \\ \chi_0 & \chi_1 & \cdots & \chi_{n-1} \\ \vdots & \vdots & & \vdots \end{bmatrix}$$

we can find the equality $A_1 = PD_1P^{-1}$ where

$$D_1 = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & \omega^1 & 0 & \cdots & 0 \\ 0 & 0 & \omega^2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \omega^{(n-1)} \end{bmatrix}.$$

Finally, taking matrix powers shows that $(A_1)^b = (PD_1P^{-1})^b$, implying $A_b = P(D_1)^bP^{-1}$. So the A_b are simultaneously diagonalizable by P as $(D_1)^b$ is given by

$$D_b := \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & \omega^b & 0 & \cdots & 0 \\ 0 & 0 & \omega^{2b} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \omega^{(n-1)b} \end{bmatrix}.$$

We find that irreducible representations of $\mathbb{Z}_n$ (all of degree one) are given by

$$\chi_j(a) = \omega^{ja}$$

for $j = 0, \ldots, n-1$. So we now have all the needed information to fully construct the character table of $\mathbb{Z}_n$, which will take the form

$$T = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & \omega & \cdots & \omega^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{n-1} & \cdots & \omega \end{bmatrix}.$$

So in this case, we can see that $P = Q = T$.

4 Delsarte Theory

Though the focus of this project is the dihedral groups, we move away from this briefly to give some needed background and history of the theory. In the late 1960s, Philippe Delsarte (at Philips Labs) studied subsets of the vertices of association schemes due to their applications in digital communications. In particular, there was interest in their application to error-correcting codes, or codes of binary numbers such that a message can be recovered even if some bits are mistakenly flipped. As an example, consider the 3-cube below with vertices labelled by the binary vectors of length 3. For this scheme we say that x and y are i^{th} associates if they are *Hamming distance* i apart, where the Hamming distance is the number of coordinates in which x and y differ. We quickly calculate that for $n = 3$ there are four relations whose adjacency matrices are given, with vertices ordered as $G = \{000, 001, 010, 011, 100, 101, 110, 111\}$, by $A_0 = I_8$ and

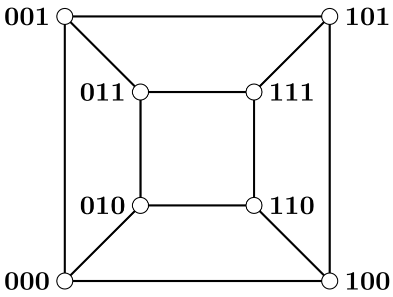


Figure 1: The Hamming scheme for $n = 3$.

$$A_1 = \begin{bmatrix} 0&1&1&0&1&0&0&0\\ 1&0&0&1&0&1&0&0\\ 1&0&0&1&0&0&1&0\\ 0&1&1&0&0&0&0&1\\ 1&0&0&0&0&1&1&0\\ 0&1&0&0&1&0&0&1\\ 0&0&1&0&1&0&0&1\\ 0&0&0&1&0&1&1&0 \end{bmatrix}, A_2 = \begin{bmatrix} 0&0&0&1&0&1&1&0\\ 0&0&1&0&1&0&0&1\\ 0&1&0&0&1&0&0&1\\ 1&0&0&0&0&1&1&0\\ 0&1&1&0&0&0&0&1\\ 1&0&0&1&0&0&1&0\\ 1&0&0&1&0&1&0&0\\ 0&1&1&0&1&0&0&0 \end{bmatrix}, A_3 = \begin{bmatrix} 0&0&0&0&0&0&0&1\\ 0&0&0&0&0&0&1&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 1&0&0&0&0&0&0&0 \end{bmatrix}.$$

From this we find the basis of primitive idempotents $E_0 = \frac{1}{8}J_8$,

$$E_1 = \begin{bmatrix} \frac{3}{8}&\frac{1}{8}&\frac{1}{8}&-\frac{1}{8}&\frac{1}{8}&-\frac{1}{8}&-\frac{1}{8}&-\frac{3}{8}\\ \frac{1}{8}&\frac{3}{8}&-\frac{1}{8}&\frac{1}{8}&-\frac{1}{8}&\frac{1}{8}&-\frac{3}{8}&-\frac{1}{8}\\ \frac{1}{8}&-\frac{1}{8}&\frac{3}{8}&\frac{1}{8}&-\frac{1}{8}&-\frac{3}{8}&\frac{1}{8}&-\frac{1}{8}\\ -\frac{1}{8}&\frac{1}{8}&\frac{1}{8}&\frac{3}{8}&-\frac{3}{8}&-\frac{1}{8}&-\frac{1}{8}&\frac{1}{8}\\ \frac{1}{8}&-\frac{1}{8}&-\frac{1}{8}&-\frac{3}{8}&\frac{3}{8}&\frac{1}{8}&\frac{1}{8}&-\frac{1}{8}\\ -\frac{1}{8}&\frac{1}{8}&-\frac{3}{8}&-\frac{1}{8}&\frac{1}{8}&\frac{3}{8}&-\frac{1}{8}&\frac{1}{8}\\ -\frac{1}{8}&-\frac{3}{8}&\frac{1}{8}&-\frac{1}{8}&\frac{1}{8}&-\frac{1}{8}&\frac{3}{8}&\frac{1}{8}\\ -\frac{3}{8}&-\frac{1}{8}&-\frac{1}{8}&\frac{1}{8}&-\frac{1}{8}&\frac{1}{8}&\frac{1}{8}&\frac{3}{8} \end{bmatrix}, E_2 = \begin{bmatrix} \frac{3}{8}&-\frac{1}{8}&-\frac{1}{8}&-\frac{1}{8}&-\frac{1}{8}&-\frac{1}{8}&-\frac{1}{8}&\frac{3}{8}\\ -\frac{1}{8}&\frac{3}{8}&-\frac{1}{8}&-\frac{1}{8}&-\frac{1}{8}&-\frac{1}{8}&\frac{3}{8}&-\frac{1}{8}\\ -\frac{1}{8}&-\frac{1}{8}&\frac{3}{8}&-\frac{1}{8}&-\frac{1}{8}&\frac{3}{8}&-\frac{1}{8}&-\frac{1}{8}\\ -\frac{1}{8}&-\frac{1}{8}&-\frac{1}{8}&\frac{3}{8}&\frac{3}{8}&-\frac{1}{8}&-\frac{1}{8}&-\frac{1}{8}\\ -\frac{1}{8}&-\frac{1}{8}&-\frac{1}{8}&\frac{3}{8}&\frac{3}{8}&-\frac{1}{8}&-\frac{1}{8}&-\frac{1}{8}\\ -\frac{1}{8}&-\frac{1}{8}&\frac{3}{8}&-\frac{1}{8}&-\frac{1}{8}&\frac{3}{8}&-\frac{1}{8}&-\frac{1}{8}\\ -\frac{1}{8}&\frac{3}{8}&-\frac{1}{8}&-\frac{1}{8}&-\frac{1}{8}&-\frac{1}{8}&\frac{3}{8}&-\frac{1}{8}\\ \frac{3}{8}&-\frac{1}{8}&-\frac{1}{8}&-\frac{1}{8}&-\frac{1}{8}&-\frac{1}{8}&-\frac{1}{8}&\frac{3}{8} \end{bmatrix},$$

$$E_3 = \begin{bmatrix} \frac{1}{8} & -\frac{1}{8} & -\frac{1}{8} & \frac{1}{8} & -\frac{1}{8} & \frac{1}{8} & \frac{1}{8} & -\frac{1}{8} \\ -\frac{1}{8} & \frac{1}{8} & \frac{1}{8} & -\frac{1}{8} & \frac{1}{8} & -\frac{1}{8} & -\frac{1}{8} & \frac{1}{8} \\ -\frac{1}{8} & \frac{1}{8} & \frac{1}{8} & -\frac{1}{8} & \frac{1}{8} & -\frac{1}{8} & -\frac{1}{8} & \frac{1}{8} \\ \frac{1}{8} & -\frac{1}{8} & -\frac{1}{8} & \frac{1}{8} & -\frac{1}{8} & \frac{1}{8} & \frac{1}{8} & -\frac{1}{8} \\ -\frac{1}{8} & \frac{1}{8} & \frac{1}{8} & -\frac{1}{8} & \frac{1}{8} & -\frac{1}{8} & -\frac{1}{8} & \frac{1}{8} \\ \frac{1}{8} & -\frac{1}{8} & -\frac{1}{8} & \frac{1}{8} & -\frac{1}{8} & \frac{1}{8} & \frac{1}{8} & -\frac{1}{8} \\ \frac{1}{8} & -\frac{1}{8} & -\frac{1}{8} & \frac{1}{8} & -\frac{1}{8} & \frac{1}{8} & \frac{1}{8} & -\frac{1}{8} \\ -\frac{1}{8} & \frac{1}{8} & \frac{1}{8} & -\frac{1}{8} & \frac{1}{8} & -\frac{1}{8} & -\frac{1}{8} & \frac{1}{8} \end{bmatrix}$$

from which we can obtain the first and second eigenmatrices

$$P = Q = \begin{bmatrix} 1 & 3 & 3 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & -1 \\ 1 & -3 & 3 & -1 \end{bmatrix}$$

So if we want a set of "easily distinguishable words", then we should choose vertices that are pairwise far apart. Take the subset $C = \{000, 111\}$. If we transmit the message 000, and there is one error, the possibilities are 001, 010, and 100. So if the receiever knows there was exactly one error, they can determine that the correct message was 000. A useful tool for understanding the error-correcting properties of a code is the vector $\mathbf{a}_C$ of length $d+1$ whose i^{th} entry a_i gives the number of pairs of vectors in C that are at Hamming distance i apart and scale the vector by $|C|^{-1}$ we obtain

$$\mathbf{a}_C = \begin{bmatrix} 1 & 0 & 0 & 1 \end{bmatrix}$$

and observe that the two zeros in the middle represent the number of errors needed for a code to be undecipherable—so in our case, if there is at most one error per code word during transmission, the message is still decipherable. Later we will refer to this vector as the inner distribution of C. As a second example, consider

$$C^{\perp} = \{000, 011, 101, 110\}$$

and note that while C is the binary rowspace of the matrix [1 1 1], $C^{\perp}$ is the nullspace of this matrix over the binary ring $\mathbb{Z}_2$; this is called the *dual code* of C. For our example, C has dual distribution

$$a_C Q = \begin{bmatrix} 2 & 0 & 6 & 0 \end{bmatrix};$$

to shed light on this terminology, we give the inner distribution and dual distribution of the dual code $C^{\perp}$:

$$a_{C^{\perp}} = \begin{bmatrix} 1 & 0 & 3 & 0 \end{bmatrix}, \; a_{C^{\perp}} Q = \begin{bmatrix} 4 & 0 & 0 & 4 \end{bmatrix}.$$

In our project, subsets of the dihedral group will not have natural duals, but we are still interested in the combinatorial properties of the inner and dual distributions. We now formally describe this theory in order to apply it to any finite group.

Let $A_0, \ldots, A_d$ and $E_0, \ldots, E_d$ be the adjacency matrices and idempotents of the conjugacy class association scheme over a finite group G. Let some nonempty subset C of G be given; the following definitions and theorems are largely adapted from Delsarte's thesis at [8]. We first denote by $\mathbf{x}$ the characteristic vector of C so that $\mathbf{x}$ has one entry for each $g \in G$ and

$$x_g = \begin{cases} 1 & g \in C \\ 0 & g \notin C. \end{cases}$$

Then the h-entry of $\mathbf{y} = A_i\mathbf{x}$ is equal to $|h\mathcal{C}_i \cap C|$. We now define two distributions on C. For a row vector $\mathbf{a}$ of length $d+1$, let

$$a_i = \frac{1}{|C|}|\{x, y \in C : x^{-1}y \in \mathcal{C}_i\}|.$$

Informally, each entry a_i gives the "average" number of elements of C that are i^{th} associates of an additional element of C chosen uniformly at random. This vector is referred to as the *inner distribution* of C. We also find that

$$a_i = \frac{1}{|C|}\mathbf{x}^T A_i \mathbf{x};$$

this can be seen by recalling that the gh entry of A_i is 1 if $g^{-1}h \in \mathcal{C}_i$ (and 0 otherwise) so $\mathbf{x}^T A_i \mathbf{x}$ counts the number of pairs $(g, h) \in C \times C$ such that $g^{-1}h \in \mathcal{C}_i$, matching the first definition of a_i. We define the *dual distribution* of C similarly, with

$$b_j = \frac{|G|}{|C|}\mathbf{x}^T E_j \mathbf{x}$$

for $0 \leq j \leq d$ and present the following lemma from [6] and [9]:

Lemma 4.1. *Let C be a nonempty subset of a group G and let $\mathbf{a}, \mathbf{b}$ be the inner and dual distributions of C respectively. Then*

1. *$a_i \geq 0$ for all i*
2. *$a_0 = 1$*
3. *$a_0 + a_1 + \cdots + a_d = |C|$*
4. *$b_j \geq 0$ for all j*
5. *$b_0 = |C|$*
6. *$b_0 + b_1 + \cdots + b_d = |G|$*
7. *$\mathbf{b} = \mathbf{a}Q$.*

Proof. (1) is clear from the first definition of a_i as $1/|C|$ times the cardinality of a set. Recalling that $\mathcal{C}_0 = \{1\}$, we know that if $x^{-1}y \in \mathcal{C}_0$ then $x = y$. There are $|C|$ pairs of elements in $|C|$ satisfying this, so $a_0 = |C|/|C| = 1$. Next we can write

$$a_0 + \cdots + a_d = \frac{1}{|C|}(\mathbf{x}^T A_0 \mathbf{x} + \cdots + \mathbf{x}^T A_d \mathbf{x}) = \frac{1}{|C|}\mathbf{x}^T(A_0 + \cdots + A_d)\mathbf{x} = \frac{1}{|C|} \cdot |C|^2 = |C|,$$

as $A_0 + \cdots + A_d = J$. Recall that the E_j are orthogonal projection matrices—then we can use the facts $E_j = E_j^2 = E_j^\dagger$ to show that

$$b_j = \frac{|G|}{|C|}\mathbf{x}^T E_j^T E_j \mathbf{x} = \frac{|G|}{|C|}\langle E_j\mathbf{x}, E_j\mathbf{x}\rangle \geq 0,$$

so $b_j \geq 0$ for all j. Next we have

$$b_0 = \frac{|G|}{|C|}\mathbf{x}^T E_0 \mathbf{x} = \frac{1}{|C|} \cdot |C|^2 = |C|,$$

since $E_0 = \frac{1}{|G|}J$. So $b_0 = |C|$. Then we can write

$$b_0 + \cdots + b_d = \frac{|G|}{|C|}(\mathbf{x}^T E_0 \mathbf{x} + \cdots + \mathbf{x}^T E_d \mathbf{x}) = \frac{|G|}{|C|}\mathbf{x}^T (E_0 + \cdots + E_d)\mathbf{x} = |G|,$$

as $E_0 + \cdots + E_d = I$ and $\mathbf{x}^T\mathbf{x} = |C|$. Finally we observe that, given j,

$$\sum_{i=0}^{d} a_i Q_{ji} = \sum_{i=0}^{d} \frac{Q_{ji}}{|C|}\mathbf{x}^T A_i \mathbf{x} = \frac{1}{|C|}\mathbf{x}^T \left[\sum_{i=0}^{d} Q_{ji} A_i\right] \mathbf{x} = \frac{|G|}{|C|}\mathbf{x}^T E_j \mathbf{x} = b_j,$$

proving that $b_j = \sum_{i=0}^{d} a_i Q_{ji}$ and thus that $\mathbf{b} = \mathbf{a}Q$. □

As in the motivating example of the Hamming scheme, we are interested in the number and positions of zeros in the dual distribution $\mathbf{b}$. For a subset $\mathcal{T} \subset \{0, 1, \ldots, d\}$, we say that a nonempty subset $C \subset G$ is a $\mathcal{T}$-design if the dual distribution of C satisfies $b_i = 0$ for all $i \in \mathcal{T}$. We often want to know exactly which of the entries are equal to zero, so we also define the set

$$\mathcal{T}(C) = \{j \neq 0 \mid b_j = 0\}.$$

An equivalent definition for a $\mathcal{T}$ design is a subset $\mathcal{T} \subset \{0, 1, \ldots, d\}$ so that each irreducible representation ρ_i of G satisfies

$$\operatorname{tr}\left[\sum_{h\in C}\sum_{g\in C}\rho_i(g^{-1}h)\right] = 0$$

for all $i \in \mathcal{T}$.

5 Dihedral Group

5.1 Structure

We now focus entirely on the dihedral group. Recall that the dihedral group D_{2n} is the group of order $2n$ with presentation $\langle r, s \mid r^n = s^2 = srsr = 1\rangle$. We will call group elements of the form r^{2i} and sr^{2i} even rotations and even reflections respectively, and we will call elements of the form r^{2i+1} and sr^{2i+1} odd rotations and odd reflections respectively. Additionally, we let R denote the subgroup consisting of all the rotations and we let S denote $D_{2n} \setminus R$.

We first want to characterize all subgroups of D_{2n}. We claim that every subgroup is either cyclic or dihedral, including Klein-4 for n even. Let $H \leq D_{2n}$ and first suppose that $H \leq \langle r\rangle$. Since $\langle r\rangle$ is cyclic of order n there is exactly one subgroup of order k for each divisor k of n, in particular $\langle r^{n/k}\rangle$. So H must be of this form for some k dividing n. Next suppose that H is not a subset of the rotations. Then $H = \langle r^k, t\rangle$ for some $0 \leq k \leq n$ and some reflection t. If k is relatively prime to n, then we have $H = D_{2n}$, so assume k divides n. If $k = 0$ then the subgroup is simply $\{1, t\}$, since every reflection is its own inverse. Then if $k \neq 0$, H is isomorphic to the dihedral group of order $2n/k$. We remark that in this case we call the dihedral subgroup "degenerate" if $k = n/2$ (in which case it is isomorphic to the Klein-4 group).

Next, we want to determine which of these subgroups are normal. Recall that a subgroup $N \leq G$ is normal if $gNg^{-1} = N$ for all $g \in G$. It is immediately clear that if N is a subgroup of the rotations, then it is normal in D_{2n}. We claim that if n is odd, the only other normal subgroup is the trivial group and D_{2n} itself. But when n is even, there are two more; namely $\langle r^2, s\rangle$ and $\langle r^2, sr\rangle$.

5.2 Association Scheme

Theorem 5.1. *The conjugacy classes of D_{2n} are given by $\mathcal{C}_i = \{r^i, r^{-i}\}$ for $i = 0 \dots \lfloor \frac{n}{2} \rfloor$ and $\mathcal{C}_{\frac{n}{2}+1} = \{s, sr^2, \dots, sr^{n-2}\}, \mathcal{C}_{\frac{n}{2}+2} = \{sr, sr^3, \dots, sr^{n-1}\}$ (for n even) or $\mathcal{C}_{\lceil \frac{n}{2} \rceil} = \{s, sr, \dots, sr^{n-1}\}$ (for n odd).*

Proof. Consider the following table of conjugations gxg^{-1}:

$x \backslash g$	r^j	sr^j
r^i	r^i	r^{-i}
sr^i	sr^{i-2j}	sr^{2j-i}

This demonstrates that every rotation is conjugate only to itself and its inverse, and reflections are conjugate to reflections of the same parity (for n even) or to each other reflection (for n odd). □

With this we find that there are $d + 1$ relations in the conjugacy class association scheme over D_{2n}, where

$$d = \begin{cases} \frac{n}{2} + 2, & n \text{ even} \\ \frac{n-1}{2} + 1, & n \text{ odd.} \end{cases}$$

Example. The conjugacy classes of D_{12} are given by $\mathcal{C}_0 = \{1\}, \mathcal{C}_1 = \{r, r^5\}, \mathcal{C}_2 = \{r^2, r^4\}, \mathcal{C}_3 = \{r^3\}, \mathcal{C}_4 = \{s, sr^2, sr^4\}, \mathcal{C}_5 = \{sr, sr^3, sr^5\}$ and the adjacency matrices by

$$A_0 = I_{12},\ A_1 = \left[\begin{array}{cccccc|cccccc}
0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\hline
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0
\end{array}\right], A_2 = \left[\begin{array}{cccccc|cccccc}
0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\hline
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0
\end{array}\right]$$

$$A_3 = \left[\begin{array}{cccccc|cccccc}
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\hline
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0
\end{array}\right], A_4 = \left[\begin{array}{cccccc|cccccc}
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\
\hline
1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0
\end{array}\right]$$

$$A_5 = \left[\begin{array}{cccccc|cccccc}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
\hline
0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{array}\right]$$

We now present a few results on the intersection numbers of the scheme, beginning with two examples. We define the matrices L_i so that the jk entry of L_i is equal to p^j_{ik}.

Example. For D_{10}, the L_i are

$$L_0 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, L_1 = \begin{bmatrix} 0 & 2 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 2 \end{bmatrix}, L_2 = \begin{bmatrix} 0 & 0 & 2 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 2 \end{bmatrix}, L_3 = \begin{bmatrix} 0 & 0 & 0 & 5 \\ 0 & 0 & 0 & 5 \\ 0 & 0 & 0 & 5 \\ 1 & 2 & 2 & 0 \end{bmatrix}.$$

Example. For D_{12}, the L_i are

$$L_0 = I, L_1 = \begin{bmatrix} 0 & 2 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 2 & 0 \end{bmatrix}, L_2 = \begin{bmatrix} 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 \end{bmatrix}, L_3 = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix},$$

$$L_4 = \begin{bmatrix} 0 & 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 & 0 & 3 \\ 1 & 0 & 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 1 & 0 & 0 \end{bmatrix}, L_5 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 & 3 & 0 \\ 0 & 2 & 0 & 1 & 0 & 0 \\ 1 & 0 & 2 & 0 & 0 & 0 \end{bmatrix}.$$

We see that for any dihedral group, L_0 will be equal to the identity matrix. This is because A_0 is the identity matrix, so the product of A_0 with any other A_i will be equal to A_i. For the remainder of the results, the odd and even cases must be considered separately. First suppose n is odd. Our first special case is if $k = 0$, then

$$p^0_{ij} = \begin{cases} 0, & i \neq j \\ 2, & i = j \text{ and } 0 < i < d \\ n, & i = j \text{ and } i = d \end{cases}.$$

Since $k = 0$, without loss of generality we can choose $a = b = 1$ as we just need that $a^{-1}b \in \mathcal{C}_0$. So given $c \in D_{2n}$ such that $a^{-1}c \in \mathcal{C}_i$ and $c^{-1}b \in \mathcal{C}_j$, we can deduce $c \in \mathcal{C}_i$ and $c \in \mathcal{C}_j$, since conjugacy classes in the dihedral group are inverse closed. So if $i \neq j$, $p^0_{ij} = 0$ since conjugacy classes partition the group. But when $i = j$, $p^0_{ii} = |\mathcal{C}_i|$ thus n if $i = d$ or 2 otherwise.

For the second special case, suppose $j = d$. Then

$$p^k_{id} = \begin{cases} 0, & 0 < i < d \text{ and } k < d \\ 2, & 0 < i < d \text{ and } k = d \end{cases}.$$

For the third special case, suppose $i = d = j$. Then

$$p_{dd}^{k} = \begin{cases} n, & k < d \\ 0, & k = d \end{cases}$$

For the fourth special case, suppose $k = d$. Then

$$p_{ij}^{d} = 0, \qquad 0 < i < d \text{ and } 0 < j < d$$

For the rest, there are 4 equations that determine whether p_{ij}^{k} is 1 or 0 for $0 < i, j, k, < d$.

$$p_{ij}^{k} = \begin{cases} 1, & k = \pm(i+j) \pmod{n} \\ 1, & k = \pm(i-j) \pmod{n} \\ 0, & else \end{cases}$$

This characterizes all the intersection numbers of D_{2n} for n odd. Results on the intersection numbers for n even are given in [10].

5.3 Representations and Characters

We now fully determine the irreducible representations and their associated characters, allowing us to write down a general form of the character table. Recall from Section 3 that, up to equivalence, the number of irreducible representations is equal to the number of conjugacy classes and that

$$\sum_{i=0}^{d} n_i^2 = |G|$$

where n_i is the degree of the representation ρ_i for $i = 0, \ldots, d$. We also know from Theorem 2.8 in [7] that the number of degree one irreducible representations is equal to the order of the quotient group D_{2n}/N where N is the commutator subgroup of D_{2n}. We use these facts to first decide the order of the representations. Consider the table of products $xyx^{-1}y^{-1}$ below:

$x \backslash y$	r^j	sr^j
r^i	1	r^{2i}
sr^i	r^{-2j}	r^{2j-2i}

This demonstrates that the commutator subgroup N is equal to the subgroup generated by r^2, giving $\{1, r^2, r^4, \ldots, r^{(n/2)-2}\}$ for n even and $\{1, r, r^2, \ldots, r^{(n-1)/2}\}$ for n odd. Thus $|D_{2n}/N| = 4$ for n even, giving 4 one-dimensional irreducible representations, and $|D_{2n}/N| = 2$ for n odd, giving 2 one-dimensional irreducible representations.

We now have $d-3$ more irreducible representations of unknown degree ($n_i > 1$) for n even, and $d-1$ more for n odd. First consider n even. We know that the sums of the squares of the degrees of all representations is equal to $2n$, giving

$$n_4^2 + n_2^5 + \cdots + n_d^2 = 2n - 4.$$

Note that $n_4 = n_5 = \cdots = n_d = 2$ is a solution to this equation, since the left hand side would then reduce to $4(d-3) = 4(\frac{n}{2} + 2 - 3) = 2n - 4$. But this shows that we cannot increase any of the $n_i's$ to a number greater than 2, as then a subset of the other $n_j's$ would have to decrease to 0 or 1, neither of which are possible. So for n even all remaining representations are 2-dimensional, and a similar argument works for n odd.

We are now ready to exactly determine the irreducible representations of the dihedral group. We first consider one-dimensional irreducible representations of D_{2n} for n even. Of course ρ_0 is the trivial representation, giving 1 for all conjugacy classes. We claim that the remaining one-dimensional irreducible representations are given by

$$\begin{aligned}
\rho_1(r) &= 1,\ \rho_1(s) = -1 \\
\rho_2(r) &= -1,\ \rho_2(s) = 1 \\
\rho_3(r) &= -1,\ \rho_3(s) = -1
\end{aligned}$$

Since these are distinct one-dimensional representations, we know that they are irreducible. Now we look for the two-dimensional irreducible representations, of which there must be $d-3$. Consider the homorphisms defined by

$$\rho_j(r) = \begin{bmatrix} \cos(2\pi j/n) & -\sin(2\pi j/n) \\ \sin(2\pi j/n) & \cos(2\pi j/n) \end{bmatrix},\ \rho_j(s) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

for $j = 4 \ldots d$. Because these matrices do not commute, they are irreducible. In order to differentiate the characters of the two-dimensional representations from those of the one-dimensonal representations, we will denote them by ψ_i for $i = 1 \ldots d-3$ (n even) or for $i = 1 \ldots d-1$ (n odd). We find that $\psi_j(sr^k) = 0$ and that $\psi_j(r^k) = 2\cos(2\pi jk/n)$. Then the two-dimensional irreducible representations for n odd are of the same form as those for n even, and the only one-dimensional irreducible representations for n odd are the trivial representation and the representation that sends $r \mapsto 1$ and $s \mapsto -1$. So the general form of the character tables is as follows:

	χ_0	χ_1	χ_2	χ_3	ψ_1	$\cdots$	ψ_k	$\cdots$	$\psi_{\frac{n}{2}-1}$
$\mathcal{C}_0$	1	1	1	1	2	$\cdots$	2	$\cdots$	2
$\mathcal{C}_1$	1	1	-1	-1	$2\cos(\frac{2\pi}{n})$	$\cdots$	$2\cos(\frac{2\pi k}{n})$	$\cdots$	$2\cos(\frac{(n-2)\pi}{n})$
$\mathcal{C}_2$	1	1	1	1	$2\cos(\frac{4\pi}{n})$	$\cdots$	$2\cos(\frac{4\pi k}{n})$	$\cdots$	$2\cos(\frac{2(n-2)\pi}{n})$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\cdots$	$\vdots$	$\cdots$	$\vdots$
$\mathcal{C}_{\frac{n}{2}}$	1	1	$(-1)^{n/2}$	$(-1)^{n/2}$	$2\cos(\pi)$	$\cdots$	$2\cos(\pi k)$	$\cdots$	$2\cos((\frac{n-2}{2})\pi)$
$\mathcal{C}_{\frac{n}{2}+1}$	1	-1	1	-1	0	$\cdots$	0	$\cdots$	0
$\mathcal{C}_{\frac{n}{2}+2}$	1	-1	-1	1	0	$\cdots$	0	$\cdots$	0

(n even)

	χ_0	χ_1	ψ_1	$\cdots$	ψ_k	$\cdots$	$\psi_{\frac{n-1}{2}}$
$\mathcal{C}_0$	1	1	2	$\cdots$	2	$\cdots$	2
$\mathcal{C}_1$	1	1	$2\cos(\frac{2\pi}{n})$	$\cdots$	$2\cos(\frac{2\pi}{n}k)$	$\cdots$	$2\cos(\frac{(n-1)\pi}{n})$
$\mathcal{C}_2$	1	1	$2\cos(\frac{4\pi}{n})$	$\cdots$	$2\cos(\frac{4\pi}{n}k)$	$\cdots$	$2\cos(\frac{2(n-1)\pi}{n})$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\cdots$	$\vdots$	$\cdots$	$\vdots$
$\mathcal{C}_{d-1}$	1	1	$2\cos(\frac{(n-1)\pi}{n})$	$\cdots$	$2\cos(\frac{(n-1)\pi}{n}k)$	$\cdots$	$2\cos((\frac{(n-1)\pi}{n}(d-1))$
$\mathcal{C}_d$	1	-1	0	$\cdots$	0	$\cdots$	0

(n odd).

6 Designs in the Dihedral Group

We briefly saw natural interpretations of $\mathcal{T}$-designs in the 3-cube, and we now focus on $\mathcal{T}$-designs in the conjugacy class association scheme of the dihedral groups. We will begin by characterizing the designs for $|\mathcal{T}| = 1$ and then combining restrictions in order to discover larger designs. For brevity, in the case where $\mathcal{T} = \{i\}$ we say the subset is an i-design. It turns out that the task of determining designs on the one-dimensional representations of D_{2n} is much simpler than for the two-dimensional representations—this is in part because the nature of the one-dimensional representations depends only on the parity of n. Thus we present first some results on designs for the one-dimensional representations.

Theorem 6.1. *For n even, if a subset $C \subset D_{2n}$ satisfies:*

- *$|R| = |S|$, then C is a 1-design;*
- *$|C_e| = |C_o|$ where $C_e = \{s^i r^j \in C \mid j \text{ even}\}$, $C_o = \{s^i r^j \in C \mid j \text{ odd}\}$, then C is a 2-design;*
- *$|C_1| = |C_2|$ where $C_e = \{s^i r^j \in C \mid i + j \text{ even}\}$, $C_o = \{s^i r^j \in C \mid i + j \text{ odd}\}$ then C is a 3-design.*

Proof. Suppose we have $C \subset D_{2n}$ containing k rotations and k reflections. Recall that a product $x^{-1}y$ for $x, y \in D_{2n}$ will equal a rotation if x and y are either both rotations or both reflections, and will equal a reflection otherwise. So we have $2k^2$ pairs in C whose product is a rotation, and $2k^2$ pairs whose product is a reflection. Since the value of χ_1 is 1 for a rotation and -1 for a reflection, having an equal number of products equal to rotations and reflections means $b_1 = 0$.

Next take $C \subset D_{2n}$ so that $|C_e| = |C_o| = k$. Since n is even we know that g is of the same parity as g^{-1} for all $g \in D_{2n}$. Then for $x, y \in C$, $x^{-1}y$ lies in C_e if x, y are of the same parity and in C_o otherwise. Just as above, there are $2k^2$ pairs of each kind. Since χ_2 sends even rotations to 1 and odd rotations to -1, we have $b_2 = 0$.

Finally take $C \subset D_{2n}$ with $|C_1| = |C_2| = k$. Note that we can write

$$C_1 = \{r^j \in C \mid \text{j even}\} \cup \{sr^j \in C \mid \text{j odd}\}$$
$$C_2 = \{r^j \in C \mid \text{j odd}\} \cup \{sr^j \in C \mid \text{j even}\};$$

so for $x, y \in C$ we find that $x^{-1}y$ is contained in C_1 if $x, y \in C_1$ or if $x, y \in C_2$ and $x^{-1}y$ is contained in C_2 otherwise. So there are still $2k^2$ pairs of each kind. The character χ_3 sends elements in C_1 to 1 and elements in C_2 to -1, so we have $b_3 = 0$. □

We note that the first part of the proof also works for n odd, so that we have also found the 1-designs of D_{2n} for n odd.

Theorem 6.2. *For n odd, if a subset $C \subset D_{2n}$ satisfies $|R| = |S|$, then C is a 1-design.*

For convenience, we display these results as a table:

	condition on C	
i	n even	n odd
1	$\lvert R\rvert = \lvert S\rvert$	$\lvert R\rvert = \lvert S\rvert$
2	$\lvert C_e\rvert = \lvert C_o\rvert$ where $C_e = \{s^i r^j \in C : j \text{ even}\}$ $C_o = \{s^i r^j \in C : j \text{ odd}\}$	N/A
3	$\lvert C_1\rvert = \lvert C_2\rvert$ where $C_1 = \{s^i r^j \in C : i+j \text{ even}\}$ $C_2 = \{s^i r^j \in C : i+j \text{ odd}\}$	N/A

For the next conjecture, recall that we defined the set $\mathcal{T}(C) = \{j \neq 0 \mid b_j = 0\}$.

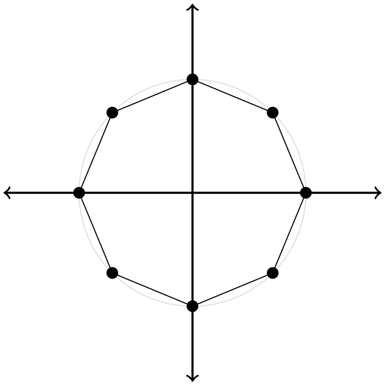
Conjecture 6.3. *For n even and all $\mathcal{T} \subset \{1, 2, 3\}$, there exists a C with $\mathcal{T}(C) = \mathcal{T}$.*

In other words, there exists a subset C so that there are zeroes *only* in the specified positions. We note that the case $\mathcal{T} = \{1, 2, 3\}$ is satisfied by any C with an equal number of even rotations, odd rotations, even reflections, and odd reflections.

We now move on to some theorems and conjectures about designs corresponding to the two-dimensional representations. We will say that a subset is a design in the two-dimensional representations if the dual distribution has zeros in the entries corresponding to the two-dimensional representations.

Theorem 6.4. *The subgroup $\langle r^2\rangle$ is a design only in the two-dimensional representations of D_{2n} for any even $n \geq 2$.*

Proof. Before proceeding to a proof we present a fact from basic geometry. Consider the n-gon with its vertices placed around the unit circle as below:



A subset consisting of k vertices that are evenly spaced around the polygon sums to the center of the polygon at (0, 0).

Since $C = \langle r^2\rangle$ consists of only even rotations, it is clearly not a 1-design, since there are no reflections. It is also not a 2- or 3- design. So all we have to show is that it is a design for all of the two-dimensional representations.

Now let n be even and consider the case where n is divisible by 4. Then the inner distribution of C will take the form

$$\mathbf{a} = \begin{bmatrix} n & 0 & 2n & 0 & 2n & 0 & \cdots & n & 0 & 0 \end{bmatrix}.$$

Now take some two-dimensional representation ψ_k. Then the character afforded by this representation is

$$Q_k = \begin{bmatrix} 2 \\ 2\cos(\frac{2\pi k}{n}) \\ 2\cos(\frac{4\pi k}{n}) \\ \vdots \\ 2\cos(\frac{(n-2)\pi k}{n}) \\ 2\cos(\pi k) \\ 0 \\ 0 \end{bmatrix}.$$

So we have

$$b_k = \mathbf{a}Q_k = 2n + 4n\cos(\frac{4\pi k}{n}) + \cdots + 2n\cos(\pi k) = 2n(1 + 2\cos(\frac{4\pi k}{n}) + \cdots + \cos(\pi k)) = 0,$$

since this is a sum of cosines of angles equally spaced by $\frac{4\pi}{n}\gcd(n,k)$. We chose k arbitrarily, so our set is a design for all two-dimensional representations.

Now suppose n is not divisible by 4. In this case we find that the inner distribution of C is given by

$$\mathbf{a} = \begin{bmatrix} n & 0 & 2n & 0 & \cdots & 2n & 0 & 0 & 0 \end{bmatrix}.$$

Again take some two-dimensional representation ψ_k. Then character afforded by this representation is also

$$Q_k = \begin{bmatrix} 2 \\ 2\cos(\frac{2\pi k}{n}) \\ 2\cos(\frac{4\pi k}{n}) \\ \vdots \\ 2\cos(\frac{(n-2)\pi k}{n}) \\ 2\cos(\pi k) \\ 0 \\ 0 \end{bmatrix},$$

and taking the dot product gives

$$b_k = \mathbf{a}Q_k = 2n + 4n\cos(\frac{4\pi k}{n}) + \cdots + 2n\cos(\frac{(n-2)\pi k}{n}) = 2n(1 + 2\cos(\frac{4\pi k}{n}) + \cdots + 2\cos(\frac{(n-2)\pi k}{n})) = 0$$

since this is a sum of cosines of angles equally spaced by $\frac{4\pi}{n}\gcd(n/2,k)$. □

Theorem 6.5. *Let n be even and suppose we have $C \subset D_{2n}$ as a $\mathcal{T}$-design for $\mathcal{T} = \{2\} \sqcup \mathcal{D}$ where $3 \notin \mathcal{D}$ and $\mathcal{T}(C) = \mathcal{T}$. Let $\mathcal{T}' = \{3\} \sqcup \mathcal{D}$. Then there exists C' so that C' is a $\mathcal{T}'$-design and $\mathcal{T}(C') = \mathcal{T}'$.*

Proof. Given an appropriate subset C, we provide a simple construction of a satisfactory C'. Decompose C

into the disjoint union of four sets C_0, C_1, C_2, C_2 where

$$\begin{aligned} C_0 &= \{r^j \in C \mid \text{j even}\} \\ C_1 &= \{r^j \in C \mid \text{j odd}\} \\ C_2 &= \{sr^j \in C \mid \text{j odd}\} \\ C_3 &= \{sr^j \in C \mid \text{j even}\}. \end{aligned}$$

From Theorem 6.1 we know that, because C is a 2-design, then $|C_0 \cup C_3| = |C_1 \cup C_2|$. Now consider $C' = (C \cap \langle r\rangle) \cup r(C \setminus \langle r\rangle)$; informally, C' is obtained from C by left-multiplying all reflections by r. With this we get that $|C'_2| = |C_3|$ and $|C'_3| = |C_2|$, so our new subset satisfies

$$|C'_0 \cup C'_2| = |C'_1 \cup C'_3|,$$

the definition of a 3-design. We now must show that C' is still a $\mathcal{D}$-design. Whether or not C' is a 1-design is unchanged, since our transformation did not change the number of rotations and reflections. As for the remaining representations, recall that the character of any reflection under any two-dimensional representation is zero, so the products of the rotations in C' with the translated reflections in C' do not change the dual distribution. We can also see that for arbitrary i, j,

$$\begin{aligned} (sr^i)^{-1}sr^j &= r^{-i}ssr^j = r^{j-i}, \text{ but also} \\ (sr^{i+1})^{-1}sr^{j+1} &= r^{-i-1}ssr^{j+1} = r^{j-i}; \end{aligned}$$

so the products of the shifted reflections with the shifted reflections also remain unchanged. Thus the dual distribution $\mathbf{b}'$ of C', in all entries apart from b_2 and b_3, is the same as the dual distribution of C. So the theorem is proven. □

Conjecture 6.6. *For n prime, the only non-trivial design in the two-dimensional representations is the set of rotations.*

Let $C \subset \mathbb{Z}_p$ for p prime. This conjecture can be proved by showing that if we have $\sum_{a\in C} \omega^a \in \mathbb{R}$ for $\omega = \exp(2\pi i/p)$, then it must be that $C = \mathbb{Z}_p$. We believe that this can be argued using the irreducibility of the p^{th} cyclotomic polynomial for p prime.

Conjecture 6.7. *For any $n \geq 2$ there exists a design only in the even two-dimensional representations and there exists a design only in the odd two-dimensional representations.*

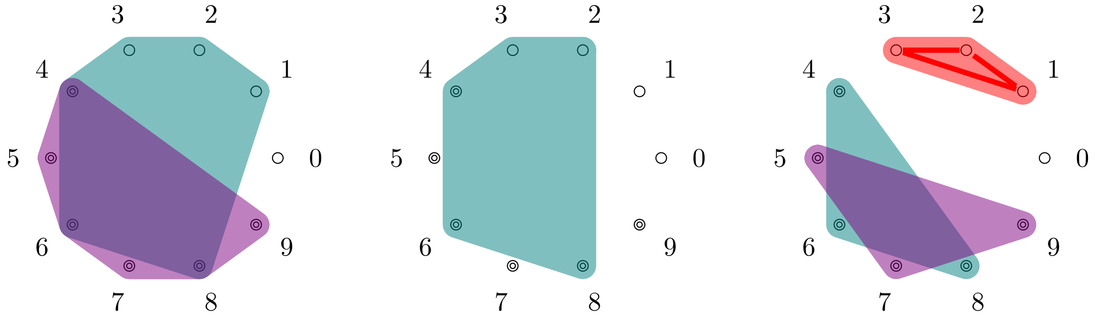
As an example, in any group D_{2n} for n divisible by 4 we will have $\{1, r^{n/2}\}$ as a design only for $\psi_1, \psi_3, \ldots$.

Conjecture 6.8. *Given $k|n$, the subgroup of D_{2n} given by $\langle r^{\frac{n}{k}}, s\rangle \cong D_{2k}$ is a design for every two-dimensional representation except ψ_{ik} for $i = 1, \ldots, \lfloor\frac{n-2}{2k}\rfloor$. Furthermore,*

- *when n is odd, this subgroup is also a 1-design;*
- *when n is even and not divisible by 4, this subgroup is a $\{1, 2\}$-design and is a 3-design if and only if k is even;*

- *when n is divisible by 4, this subgroup is a $\{1,2\}$-design and is never a 3-design.*

Let $\mathbb{T}$ be the collection of subsets $\mathcal{T} \subset \{0,\dots,d\}$ such that there exists $C \subset D_{2n}$ as a $\mathcal{T}$-design satisfying $\mathcal{T}(C) = \mathcal{T}$. We now consider the problem of displaying the elements of $\mathbb{T}$ in a format that is compact while remaining easily understandable. As n grows larger, so does the size of $\mathbb{T}$, so many presentations quickly become unreadable. Regardless of the manner in which we structure the figures, it is natural to order $\mathbb{T}$ lexicographically. Below we present two options, the first of which is optimal when $\mathbb{T}$ is sparse due to its compactness, and the second of which is optimal when there are many subsets due to its readability regardless of the size of our collection.



(a) $|\mathcal{T}|$=7

(b) $|\mathcal{T}|$=5

(c) $|\mathcal{T}|$=3

Figure 2: A display of the subsets in $\mathbb{T}$ for D_{28}. We use double circles to distinguish entries corresponding to the two-dimensional representations. An additional line indicates that both a subset and all of its nonempty subsets are in $\mathbb{T}$.

$|\mathcal{T}| = 7:$

0	1	2	3	4	5	6	7	8
	○	○	○	○	○	○		○
	○	○	○	○	○		○	○
	○	○		○	○	○	○	○
	○		○	○	○	○	○	○
		○	○	○	○	○	○	○

$|\mathcal{T}| = 6:$

0	1	2	3	4	5	6	7	8
	○	○	○	○		○		○
	○	○		○	○		○	○
	○	○		○		○	○	○
	○		○	○	○		○	○
	○		○	○		○	○	○
		○	○	○	○	○		○
		○	○	○	○		○	○

$|\mathcal{T}| = 5:$

0	1	2	3	4	5	6	7	8
	○	○	○		○	○		
	●	●	●		●		●	
	○	○		○		○		○
	○		○	○		○		○
	○			○	○		○	○
	○			○		○	○	○
		○	○	○	○			○
		○	○	○		○		○
		○		○	○		○	○
			○	○	○		○	○
				○	○	○	○	○

$|\mathcal{T}| = 4:$

0	1	2	3	4	5	6	7	8
	●	●	●			●		
	○	○		○				○
	○	○				○	○	
	○		○	○				○
	○		○			○	○	
	○			○		○		○
	○			○			○	○
		○	○	○				○
		○	○		○	○		
		○		○		○		○
			○	○		○		○
				○	○	○		○
				○	○		○	○
				○		○	○	○

$|\mathcal{T}| = 3:$

0	1	2	3	4	5	6	7	8
	○				○			○
	●					●	●	
		○		○				○
			○	○				○
				○	○			○
				○		○		○
				○			○	○

$|\mathcal{T}| = 2:$

0	1	2	3	4	5	6	7	8
				○				○
					●	●		

Figure 3: A display of the subsets in $\mathbb{T}$ for D_{24} ordered by size and lexicographically. We use filled dots to indicate that a subset and all of its nonempty subsets are in $\mathbb{T}$. We use a double line to demarcate entries corresponding to the two-dimensional representations.

References

[1] Rosemary A. Bailey. *Association Schemes: Designed Experiments, Algebra and Combinatorics.* Cambridge Studies in Advanced Mathematics. Cambridge University Press, Cambridge, 2004.

[2] Alena Ernst and Kai-Uwe Schmidt. Transitivity in finite general linear groups. (arXiv:2209.07927), September 2022. arXiv:2209.07927 [math].

[3] David S. Dummit and Richard M. Foote. *Abstract Algebra, 3rd Edition.* Wiley, Hoboken, NJ, 3rd edition edition, July 2003.

[4] Serge Lang. *Linear Algebra.* Springer, 3 edition, 1987.

[5] Andries E. Brouwer, Arjeh M. Cohen, and Arnold Neumaier. *Distance-Regular Graphs.* Springer, Berlin, Heidelberg, 1989.

[6] Eiichi Bannai and Tatsurō Itō. *Algebraic combinatorics I: association schemes.* Mathematics lecture note series. Benjamin/Cummings Pub. Co., Menlo Park, Calif., 1984. OCLC: 10162172.

[7] Walter Ledermann. *Introduction to Group Characters.* Cambridge University Press, Cambridge, 2 edition, 1987.

[8] Philippe Delsarte. *An Algebraic Approach to the Association Schemes of Coding Theory.* Number 10 in Philips Research Reports Supplements. Philips Research Laboratories, 1973.

[9] William J. Martin and Hajime Tanaka. Commutative association schemes. *European Journal of Combinatorics*, 30(6):1497–1525, August 2009. arXiv:0811.2475 [math].

[10] Yue Meng-tian and Li Zeng-ti. Construction of an assocation scheme over dihedral group. *Journal of Mathematics*, 35(1), 2015.

[11] Eiichi Bannai, Etsuko Bannai, Tatsuro Ito, and Rie Tanaka. *Algebraic Combinatorics.* De Gruyter, Berlin Boston, 1st edition edition, February 2021.

[12] William J. Martin and Bruce E. Sagan. A new notion of transitivity for groups and sets of permutations. *Journal of the London Mathematical Society*, 73(1):1–13, 2006.