9-2022

Orthogonal Arrays and Legendre Pairs

Kristopher N. Kilpatrick

ORTHOGONAL ARRAYS AND LEGENDRE PAIRS

DISSERTATION

Kristopher N. Kilpatrick, Capt, USAF

AFIT-ENC-DS-22-S-004

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT-ENC-DS-22-S-004

ORTHOGONAL ARRAYS AND LEGENDRE PAIRS

DISSERTATION

Presented to the Faculty

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

in Partial Fulfillment of the Requirements for the

Degree of Doctor of Philosophy in Applied Mathematics

Kristopher N. Kilpatrick, M.S.

Capt, USAF

Sept 2022

AFIT-ENC-DS-22-S-004

ORTHOGONAL ARRAYS AND LEGENDRE PAIRS

DISSERTATION

Kristopher N. Kilpatrick, M.S.
Capt, USAF

Committee Membership:

Dursun A. Bulutoglu, Ph.D.
Chair

Matthew C. Fickus, Ph.D.
Member

Jonathan S. Turner, Ph.D.
Member

Brian J. Lunday, Ph.D.
Member

AFIT-ENC-DS-22-S-004

Abstract

Well-designed experiments greatly improve test and evaluation. Efficient experiments reduce the cost and time of running tests while improving the quality of the information obtained. Orthogonal Arrays (OAs) and Hadamard matrices are used as designed experiments to glean as much information as possible about a process with limited resources. However, constructing OAs and Hadamard matrices in general is a very difficult problem. Finding Legendre pairs (LPs) results in the construction of Hadamard matrices. This research studies the classification problem of OAs and the existence problem of LPs. In doing so, it makes two contributions to the discipline. First, it improves upon previous classification results of 2-symbol OAs of even-strength t and $t + 2$ columns. Second, it presents previously unknown impossible values for the dimension of the convex hull of all feasible points to the LP problem improving our understanding of its feasible set.

AFIT-ENC-DS-22-S-004

I thank my father for his guidance and continued support throughout this challenging endeavour.

Acknowledgements

I would like to thank my advisor, Dr. Bulutoglu, for his many hours of clearly explaining ideas, often in a multitude of ways, and finally for his great patience.

Kristopher N. Kilpatrick

Table of Contents

ORTHOGONAL ARRAYS AND LEGENDRE PAIRS

I. Introduction

1.1 Motivation

Test and evaluation is critical to the Department of Defense's success of providing the warfighter proven combat-ready systems that are essential in accomplishing the mission. The Department of Operational Test and Evaluation, Air Force Operational Test and Evaluation Center, United States Army Test and Evaluation Command, and other U.S. armed services endorse the use of design of experiments in test and evaluation to provide a rigorous and scientific approach to test and evaluation. In-depth discussions on design of experiments in the U.S. Air Force test community may be found in Johnson *et al.* [1], Hutto and Higdon [2], and Tucker *et al.* [3].

A designed experiment is a test carried out to determine the effect of factors, or input variables, each of which has several different levels, or settings, on an output response. A full factorial design is an experiment wherein all factor and all factor levels are tested with the response, or output variable, measured. To reduce the cost and time of running test, a more efficient experimental design is a fractional factorial design [4, 5]. A fractional factorial design tests only a subset of runs of a full factorial design, where a run is a prescribed level setting of each of the factors.

Orthogonal Arrays (OAs) and Hadamard matrices are used as designed experiments to glean as much information as possible about a process with limited resources. OAs are a subclass of fractional factorial designs. The least-square estimators for different effects in a designed experiment are uncorrelated, hence the name orthogonal array. OAs used in factorial experiments can estimate the intercept parameter, all components of main-effects, and all components of interactions bounded by a number dependent on the parity of the strength of the orthogonal array [6, 7]. Hadamard matrices are square matrices with entries of $+1$ or -1 wherein the rows are orthogonal. Hadamard matrices are ideal for conducting screening experiments in which each factor has two levels [8]. Hadamard matrices have applications in signal analysis and synthesis, error corrections in transmission of digital communication, and cryptography [9, 10, 11].

The utility of OAs and Hadamard matrices sets the problem to construct them and enumerate the number of distinct constructions that exist for given parameters. The construction and enumeration of OAs and Hadamard matrices will be called the classification problem. The construction of OAs and Hadamard matrices is in general a very difficult problem.

Classification of OAs has found success by their relation with codes, difference schemes, Latin squares, and finite projective geometries [6, 12, 13]. Formulating the problem in terms of an integer linear program wherein symmetries are exploited to apply isomorphism pruning has proved successful [14].

Construction of Hadamard matrices has been carried out by Sylvester [15], wherein the Kronecker product was used to inductively construct Hadamard matrices. Paley [16] constructed Hadamard matrices using Galois fields. Another approach to the construction of Hadamard matrices is the construction of Legendre pairs. The existence of a Legendre pair (LP) of odd length ℓ implies the existence of a Hadamard matrix of size $2\ell + 2$ [17]. The recent construction of LPs has relied on computer searches. Fletcher*et al.* [18] utilized the power spectral density (PSD) criterion, which improved exhaustive searches of LPs of lengths $\ell = 3, 5, \ldots, 45$ and incomplete searches for $\ell = 47, 49, 51$. Turner *et al.* [19] used δ-modular compression and discovered an LP of length $\ell = 77$ and produced an exhaustive generation of LPs of length $\ell = 55$. Elementary number-theoretic arguments and techniques that improved compression have lead to the discovery of LPs of lengths $\ell = 85, 87$ [20] and lengths $\ell = 117, 129, 133$ and 147 [21]. There are currently 10 open LP cases of length less than 200 that have yet to be discovered or proven to not exist [20].

1.2 Research Contribution

This research studies the classification problem OAs and the existence problem of LPs. In doing so, it makes two contributions to the discipline. First, it improves upon previous classification results of 2-symbol OAs of even-strength t and $t + 2$ columns. Second, it presents previously unknown impossible values for the dimension of the convex hull of all feasible points to the LP problem improving our understanding of its feasible set.

1.3 Organization of Dissertation

This dissertation is comprised of three chapters. Chapter II improves upon results of previous researchers in the classification of 2-symbol OAs of even-strength t and $t + 2$ columns. Chapter III provides bounds on the possible dimension of the convex hull of feasible points to the LP problem improving our understanding of its feasible set. Chapter II was submitted to Australasian Journal of Combinatorics and received with only minor revisions. It was resubmitted with the revisions. Chapter III will be submitted to Discrete Optimization with a few minor revisions. Chapter IV summarizes the results found in each chapter and discusses future research.

II. Classification of 2-symbol orthogonal arrays of even-strength t and $t+2$ columns up to OD-equivalence

2.1 Introduction

Throughout the paper let $[n] = \{1, \ldots, n\}$. We first define the concept of an orthogonal array (OA). Let $\lambda \geqslant 1, s \geqslant 2, k \geqslant 1, t \geqslant 1$ be integers, and $t \in [k]$. A $\lambda s^t \times k$ array $\mathbf{D}$ whose entries are symbols from $\{l_1, \ldots, l_s\}$ is an orthogonal array of strength t and index λ, denoted by $\mathrm{OA}(\lambda s^t, k, s, t)$, if each of the s^t symbol combinations from $\{l_1, \ldots, l_s\}^t$ appears λ times in every $\lambda s^t \times t$ subarray of $\mathbf{D}$.

Each of the $N!k!(s!)^k$ operations that involve permuting rows, columns and the symbols within each column of an s-symbol $N \times k$ array is called an *isomorphism operation.* Two arrays $\mathbf{D}_1$ and $\mathbf{D}_2$ are *isomorphic* if $\mathbf{D}_2$ can be obtained from $\mathbf{D}_1$ by applying an isomorphism operation. Each isomorphism operation maps an $\mathrm{OA}(\lambda s^t, k, s, t)$ to an $\mathrm{OA}(\lambda s^t, k, s, t)$.

Classification of OAs up to isomorphism in general is a challenging problem. Recently, there has been a renewed interest in classifying OAs [22, 23, 24]. However, these works make heavy use of computers. On the other hand, Yamamato *et al.* [25] were the first to analytically classify all $\mathrm{OA}(\lambda 2^t, k, 2, t)$ for $k = t+1, t+2$ up to permutations of columns. Stufken and Tang [26] strengthened the results in [25] by classifying all non-isomorphic $\mathrm{OA}(\lambda 2^t, t+2, 2, t)$ analytically. Their method of classification used J-characteristics for 2-symbol arrays.

For an $N \times k$ array $\mathbf{D} = [\mathbf{d}_1 \cdots \mathbf{d}_k]$ with symbols from $\{-1, 1\}$, Bulutoglu and Ryan [22] defined the column operation R_i on $\mathbf{D}$ by

$$R_i\mathbf{D} = \left[\mathbf{d}_1 \odot \mathbf{d}_i \quad \cdots \quad \mathbf{d}_{i-1} \odot \mathbf{d}_i \quad \mathbf{d}_i \quad \mathbf{d}_{i+1} \odot \mathbf{d}_i \quad \cdots \quad \mathbf{d}_k \odot \mathbf{d}_i\right], \tag{2.1.1}$$

and proved that each column operation R_i maps an $\mathrm{OA}(\lambda 2^t, k, 2, t)$ to an $\mathrm{OA}(\lambda 2^t, k, 2,$

t) if t is even. Each transformation that involves a column operation R_i and/or an isomorphism operation is called an *OD-equivalence operation* [27]. Hence, for even t, each OD-equivalence operation maps an OA$(\lambda 2^t, k, 2, t)$ to an OA$(\lambda 2^t, k, 2, t)$.

Two arrays $\mathbf{D}_1$ and $\mathbf{D}_2$ with symbols from $\{-1, 1\}$ are *OD-equivalent* if $\mathbf{D}_2$ can be obtained from $\mathbf{D}_1$ by applying an OD-equivalence operation [22]. Clearly, if $\mathbf{D}_1$ and $\mathbf{D}_2$ are isomorphic arrays, then $\mathbf{D}_1$ and $\mathbf{D}_2$ are OD-equivalent. However, $\mathbf{D}_1$ and $\mathbf{D}_2$ may be OD-equivalent without being isomorphic [22].

A set of non-OD-equivalent OA$(N, k, 2, t)$ can be used to generate a set of all non-isomorphic OA$(N, k, 2, t)$ [22]. In fact, Bulutoglu and Ryan [22] classified all non-isomorphic OA$(160, k, 2, 4)$ and OA$(176, k, 2, 4)$ for $k = 5, 6, \ldots, 10$ by first classifying each up to OD-equivalence. Also, it would not have been possible to obtain the classification results up to isomorphism in Bulutoglu and Ryan [22] without first classifying up to OD-equivalence. Furthermore, by applying OD-equivalence with the methods in Geyer *et al.* [27] we have found 83 non-OD-equivalent OA$(192, 9, 2, 4)$ after 6 months of CPU time on a 2.1 GHz processor. However, this is not a complete classification of all non-OD-equivalent OA$(192, 9, 2, 4)$. The OA$(192, 9, 2, 4)$ is currently the smallest OA$(N, 9, 2, 4)$ that has not been completely classified yet. Methods in Geyer *et al.* [27] that make heavy use of OD-equivalence bring a partial classification of non-OD-equivalent OA$(192, 9, 2, 4)$ within computational reach. Hence, classifying all non-OD-equivalent OA$(N, k, 2, t)$ is useful in solving the classification problem of OA$(N, k, 2, t)$ up to isomorphism. In this paper, we improve the results of Stufken and Tang [26] by analytically classifying all non-OD-equivalent OA$(\lambda 2^t, t + 2, 2, t)$ when the strength t is even.

The paper is structured as follows. Section 2.2 defines J-characteristics of 2-symbol arrays, and describes how OD-equivalence operations act on J-characteristics of such arrays. Section 2.3 presents the main result. Section 2.4 discusses future research. In Section 2.5 we provide the Theorems and Lemmas from [26] that we use in Section 2.3 to establish the main result of the paper.

2.2 J-characteristics and OD-equivalence

Throughout this section $\mathbf{D}$ will denote an $N \times k$ array with symbols from $\{-1, 1\}$.

For $\ell \subseteq [k]$, let

$$\mathbf{r}_\ell = [r_{\ell 1}, \dots, r_{\ell k}],$$

where

$$r_{\ell j} = \begin{cases} -1 & \text{if } j \in \ell, \\ 1 & \text{otherwise.} \end{cases}$$

Given an array $\mathbf{D}$, let x_ℓ be the number of times $\mathbf{r}_\ell$ appears as a row of $\mathbf{D}$. The *frequency vector* $\mathbf{x}$ of $\mathbf{D}$ is defined by

$$\mathbf{x} = [x_\varnothing, x_1, x_2, x_{12}, x_3, \dots, x_{1\dots k}]^\top \tag{2.2.1}$$

where $x_{i_1 \dots i_p}$ is used for $x_{\{i_1,\dots,i_p\}}$.

We now define the J-characteristics. Let $\mathbf{D} = [d_{ij}]$ be an array. For $\ell \subseteq [k]$, let

$$J_\ell(\mathbf{D}) = \sum_{i=1}^{N} \prod_{j \in \ell} d_{ij}.$$

(For $\ell = \varnothing$, $J_\ell(\mathbf{D}) := N$.) The $J_\ell(\mathbf{D})$ are called the *J-characteristics* of $\mathbf{D}$. Let $J_{i_1 \dots i_r}(\mathbf{D})$ denote $J_{\{i_1,\dots,i_r\}}(\mathbf{D})$, then the *$J$-vector* of $\mathbf{D}$ is defined by

$$\mathbf{J} = [J_\varnothing(\mathbf{D}), J_1(\mathbf{D}), J_2(\mathbf{D}), J_{12}(\mathbf{D}), J_3(\mathbf{D}), \dots, J_{1\dots k}(\mathbf{D})]^\top. \tag{2.2.2}$$

We now establish the connection between the frequency vector and J-vector of an array. A 2^k full factorial array, with Yates ordering, is expressed by the $2^k \times k$ matrix

$$\mathbf{F} = \left[\mathbf{r}_{\varnothing}^{\top}, \mathbf{r}_1^{\top}, \mathbf{r}_2^{\top}, \mathbf{r}_{12}^{\top}, \mathbf{r}_3^{\top}, \ldots, \mathbf{r}_{1\ldots k}^{\top}\right]^{\top},$$

where $\mathbf{r}_{i_1 \ldots i_p}$ is the shorthand notation for $\mathbf{r}_{\{i_1,\ldots,i_p\}}$. For $j \in [k]$, let $\mathbf{h}_j$ denote the jth column of $\mathbf{F}$. Then

$$\mathbf{F} = [\mathbf{h}_1, \ldots, \mathbf{h}_k].$$

The Hadamard product of $\mathbf{z}$ and $\mathbf{v}$ is

$$\mathbf{z} \odot \mathbf{v} = [z_1 v_1, \ldots, z_n v_n]^{\top}$$

for $\mathbf{z}, \mathbf{v} \in \{-1, 1\}^n$. For $\ell = \{i_1, \ldots, i_p\} \subseteq [k]$, let

$$\mathbf{h}_{\ell} = \mathbf{h}_{i_1} \odot \cdots \odot \mathbf{h}_{i_p}.$$

Let

$$\mathbf{H} = [\mathbf{h}_{\varnothing}, \mathbf{h}_1, \mathbf{h}_2, \mathbf{h}_{12}, \mathbf{h}_3, \ldots, \mathbf{h}_{1\ldots k}], \tag{2.2.3}$$

where $\mathbf{h}_{i_1 \ldots i_p}$ is used for for $\mathbf{h}_{\{i_1,\ldots,i_p\}}$. Then $\mathbf{H}$ is the $2^k \times 2^k$ *Sylvester Hadamard matrix* [28].

For $\ell \subseteq [k]$, we have

$$J_{\ell}(\mathbf{D}) = \sum_{i=1}^{N} \prod_{j \in \ell} d_{ij} = \sum_{u \subseteq [k]} \prod_{j \in \ell} r_{uj} x_u = \sum_{u \subseteq [k]} (\mathbf{h}_{\ell})_u x_u = \mathbf{h}_{\ell}^{\top} \mathbf{x}.$$

This implies $\mathbf{J} = \mathbf{H}^{\top}\mathbf{x}$. Since $\mathbf{H}\mathbf{H}^{\top} = 2^k \mathbf{I}_{2^k}$, where $\mathbf{I}_{2^k}$ is the $2^k \times 2^k$ identity matrix, we have the following fundamental result.

Lemma 2.2.1. *Let* $\mathbf{x}, \mathbf{J}$, *and* $\mathbf{H}$ *be as in equations (2.2.1), (2.2.2), and (2.2.3), then*

$$\mathbf{x} = 2^{-k}\mathbf{H}\mathbf{J}.$$

By Lemma 2.2.1, the J-vector of an array uniquely determines its frequency vector. The following lemma determines all $\mathrm{OA}(\lambda 2^t, k, 2, t)$ in terms of their J-characteristics.

Lemma 2.2.2 (Stufken and Tang [26]). *An array* $\mathbf{D}$ *is an* $OA(\lambda 2^t, k, 2, t)$ *if and only if* $J_\ell(\mathbf{D}) = 0$ *for all* $\ell \subseteq [k]$ *such that* $|\ell| \in [t]$.

The following result is from Stufken and Tang [26] and its generalization in Bulutoglu and Kaziska [29].

Lemma 2.2.3. *Let* $\mathbf{D}$ *be an* $OA(\lambda 2^t, k, 2, t)$ *with* $k \geqslant t+2$. *Then the following hold.*

(i) For any $\ell \subseteq [k]$, $J_\ell(\mathbf{D}) = u_\ell 2^t$ *for some integer* u_ℓ.

(ii) For any $\ell \subseteq [k]$ *and index* λ, *we have* $u_\ell \equiv \lambda\binom{|\ell|-1}{t}$ *(mod 2).*

For isomorphism operations we have the following lemma from Geyer *et al.* [27].

Lemma 2.2.4. *Let* $\ell \subseteq [k]$ *be such that* $|\ell| > 0$. *Let* g *be an isomorphism operation and* $g\mathbf{D}$ *be the array obtained after* g *is applied to* $\mathbf{D}$. *Then*

$$J_\ell(g\mathbf{D}) = \pm J_{\ell'}(\mathbf{D}),$$

where $|\ell'| = |\ell|$.

The operations R_i act on the J-characteristics as follows, as shown in Geyer *et al.* [27].

Lemma 2.2.5. *Let $\ell \subseteq [k]$ be such that $|\ell| > 0$. Let R_i be an OD-equivalence operation as defined in equation (2.1.1), $i \in [k]$. Then*

$$J_\ell(R_i\mathbf{D}) = \begin{cases} J_\ell(\mathbf{D}) & \text{if } |\ell| \text{ is even and } i \notin \ell, \\ J_{\ell\setminus\{i\}}(\mathbf{D}) & \text{if } |\ell| \text{ is even and } i \in \ell, \\ J_{\ell\cup\{i\}}(\mathbf{D}) & \text{if } |\ell| \text{ is odd and } i \notin \ell, \\ J_\ell(\mathbf{D}) & \text{if } |\ell| \text{ is odd and } i \in \ell. \end{cases}$$

Unlike isomorphism operations, the R_i operations allow J-characteristics indexed by ℓ to be mapped to J-characteristics indexed by ℓ' with $|\ell| \neq |\ell'|$. The R_i operations are key to improving the results of Stufken and Tang [26]. Lemmas 2.2.4 and 2.2.5 from Geyer *et al.* [27] characterize the action of OD-equivalence operations on the J-characteristics.

Lemma 2.2.6. *Let $\ell \subseteq [k]$ be such that $|\ell| > 0$. Let g be an OD-equivalence operation and $g\mathbf{D}$ be the array obtained after g is applied to $\mathbf{D}$. Then*

$$J_\ell(g\mathbf{D}) = \pm J_{\ell'}(\mathbf{D})$$

for some $\ell' \subseteq [k]$, where

$$|\ell'| = \begin{cases} |\ell| \text{ or } |\ell| + 1 & \text{if } |\ell| \text{ is odd,} \\ |\ell| \text{ or } |\ell| - 1 & \text{otherwise.} \end{cases}$$

By using Lemma 2.2.6, Bulutoglu and Ryan [22] showed the following.

Theorem 2.2.7. *Let $\mathbf{D}_1$ be an $OA(\lambda 2^t, k, 2, t)$ with $t \geqslant 1$. Then $\mathbf{D}_2$ is OD-equivalent to $\mathbf{D}_1$ if and only if there exists an OD-equivalence operation g such that $\mathbf{D}_2 = g\mathbf{D}_1$ up to permutation of rows. Moreover, if $\mathbf{D}_2$ is OD-equivalent to $\mathbf{D}_1$, then $\mathbf{D}_2$ is an*

$OA(\lambda 2^t, k, 2, 2\lfloor t/2 \rfloor)$.

By Theorem 2.2.7, if $\mathbf{D}$ is an $\mathrm{OA}(\lambda 2^t, k, 2, t)$ with even t, then any array OD-equivalent to $\mathbf{D}$ is an $\mathrm{OA}(\lambda 2^t, k, 2, t)$.

2.3 Classification of even strength $\mathbf{OA}(\lambda 2^t, t+2, 2, t)$ up to OD-equivalence

Let $\mathbf{D}$ be an $\mathrm{OA}(\lambda 2^t, t+2, 2, t)$. Since $k = t+2$, by Lemma 2.2.2, we need to consider only $k+1$ coordinates of the J-vector of $\mathbf{D}$. Let $\ell_j = [k] \backslash \{k+1-j\}$ for $j \in [k]$ and $\ell_{k+1} = [k]$. The following proposition was used to classify non-isomorphic $\mathrm{OA}(\lambda 2^t, t+2, 2, t)$ for even t.

Proposition 2.3.1 (Stufken and Tang [26])**.** *When $k = t+2$ is even, every OD-equivalence class of $OA(\lambda 2^t, t+2, 2, t)$ contains a unique array $\mathbf{D}$ whose J-vector satisfies either of the following conditions:*

$$J_{\ell_1}(\mathbf{D}) \leqslant \cdots \leqslant J_{\ell_k}(\mathbf{D}) \leqslant -|J_{\ell_{k+1}}(\mathbf{D})|, \tag{2.3.1}$$

$$J_{\ell_1}(\mathbf{D}) \leqslant \cdots \leqslant J_{\ell_{k-1}}(\mathbf{D}) \leqslant -|J_{\ell_k}(\mathbf{D})|, \quad J_{\ell_{k+1}}(\mathbf{D}) < -|J_{\ell_k}(\mathbf{D})|. \tag{2.3.2}$$

The following is our main lemma.

Lemma 2.3.2. *When $k = t+2$ is even, every OD-equivalence class of $OA(\lambda 2^t, t+2, 2, t)$ contains a unique array $\mathbf{D}$ whose J-vector satisfies*

$$J_{\ell_1}(\mathbf{D}) \leqslant \cdots \leqslant J_{\ell_k}(\mathbf{D}) \leqslant -|J_{\ell_{k+1}}(\mathbf{D})|. \tag{2.3.3}$$

Proof. Suppose that $\mathbf{D}$ is the array whose J-vector satisfies inequalities (2.3.2). We show there exists a unique OD-equivalent array to $\mathbf{D}$ whose J-vector satisfies inequalities (2.3.1). Let R_1 be as defined in equation (2.1.1) and let $\mathbf{D}' = R_1\mathbf{D}$. By Theorem 2.2.7, $\mathbf{D}'$ is an $\mathrm{OA}(\lambda 2^t, t+2, 2, t)$ that is OD-equivalent to $\mathbf{D}$. Furthermore, by Lemma 2.2.5

$$J_{\ell_{k+1}}(\mathbf{D}') = J_{\ell_k}(\mathbf{D}),\ J_{\ell_k}(\mathbf{D}') = J_{\ell_{k+1}}(\mathbf{D}), \text{ and } J_{\ell_j}(\mathbf{D}') = J_{\ell_j}(\mathbf{D})$$

for $j \in [k-1]$. Then

$$J_{\ell_1}(\mathbf{D}') \leqslant \cdots \leqslant J_{\ell_{k-1}}(\mathbf{D}') \leqslant -|J_{\ell_{k+1}}(\mathbf{D}')|, \quad J_{\ell_k}(\mathbf{D}') < -|J_{\ell_{k+1}}(\mathbf{D}')|.$$

Hence, we obtain an OD-equivalent array whose J-vector satisfies inequalities (2.3.1). Then, by Proposition 2.3.1, any J-vector of an $\mathrm{OA}(\lambda 2^t, t+2, 2, t)$ satisfying inequalities (2.3.3) is unique and therefore the corresponding $\mathrm{OA}(\lambda 2^t, t+2, 2, t)$ is unique. $\square$

Lemma 2.3.2 allows the classification of non-OD-equivalent $\mathrm{OA}(\lambda 2^t, k, 2, t)$ by finding solutions in only one case, namely under inequalities (2.3.3), whereas the classification of non-isomorphic $\mathrm{OA}(\lambda 2^t, k, 2, t)$ requires finding all solutions in two mutually exclusive cases, namely under either inequalities (2.3.1) or inequalities (2.3.2). This reduction in the number of cases that need to be searched significantly simplifies the $\mathrm{OA}(\lambda 2^t, t+2, 2, t)$ classification problem.

Suppose that $\mathbf{D}$ is an $\mathrm{OA}(\lambda 2^t, k, 2, t)$ whose J-vector satisfies inequalities (2.3.3). By Lemma 2.2.3, $J_{\ell_j}(\mathbf{D}) = u_j 2^t$, $j \in [k+1]$. Then

$$u_1 \leqslant \cdots \leqslant u_k \leqslant -|u_{k+1}|. \tag{2.3.4}$$

Lemma 2.3.3. *Suppose that $k = t+2$, t is even, and λ is odd. Let*

$$\lambda + u_1 + \cdots + u_{k+1} = 4p, \tag{2.3.5}$$

with $p \geqslant 0$, $u_j \in 2\mathbb{Z}+1$ such that $|u_j| \leqslant \lambda - 2$ for $j \in [k+1]$. Then the following hold.

(i) Each solution $(u_1, \ldots, u_{k+1}, p)$ to equation (2.3.5) under inequalities (2.3.4) determines an $OA(\lambda 2^t, t+2, 2, t)$ with J-vector given by $J_{\ell_j} = 2^t u_j$ for $j \in [k+1]$.

(ii) A complete set of non-OD-equivalent $OA(\lambda 2^t, t+2, 2, t)$ is given by collecting the arrays obtained in (i) over all solutions to equation (2.3.5).

Proof. The proof follows from Lemma 2.3.2 and Theorem 1 in Stufken and Tang [26], see Section 2.5. □

Lemma 2.3.4. *Suppose that $k = t+2$, t is even, and $\lambda = 2\lambda^*$ is even. Let*

$$\lambda^* + u_1 + \cdots + u_{k+1} = 2p, \tag{2.3.6}$$

with $p \geqslant 0$, $u_j \in \mathbb{Z}$ such that $|u_j| \leqslant \lambda^*$ for $j \in [k+1]$. Then the following hold.

(i) Each solution $(u_1, \ldots, u_{k+1}, p)$ to equation (2.3.6) under inequalities (2.3.4) determines an $OA(\lambda 2^t, t+2, 2, t)$ with J-vector given by $J_{\ell_j} = 2^{t+1} u_j$ for $j \in [k+1]$.

(ii) A complete set of non-OD-equivalent $OA(\lambda 2^t, t+2, 2, t)$ is given by collecting the arrays obtained in (i) over all solutions to equation (2.3.6).

Proof. The proof follows from Lemma 2.3.2 and Theorem 2 in Stufken and Tang [26], see Section 2.5. □

Let $Z[a, b]$ and $O[a, b]$ denote the set of integers and odd integers x such that $a \leqslant x \leqslant b$, respectively.

Theorem 2.3.5. *For even t, odd λ, and $k = t+2$, if $\lambda \leqslant t-1$, then equation (2.3.5) has no $OA(\lambda 2^t, k, 2, t)$ solution under inequalities (2.3.4); if $\lambda \geqslant t+1$, then equation (2.3.5) has at least one $OA(\lambda 2^t, k, 2, t)$ solution under inequalities (2.3.4),* *and the complete set S_1 of non-OD-equivalent $OA(\lambda 2^t, k, 2, t)$ solutions is given by*

$$\begin{aligned}
p &\in Z\left[0, \frac{\lambda - t - 1}{4}\right], \\
u_{k+1} &\in O\left[-\frac{\lambda - 4p}{k+1}, \frac{\lambda - 4p}{k-1}\right], \\
u_k &\in O\left[-\frac{\lambda - 4p + u_{k+1}}{k}, -|u_{k+1}|\right], \\
u_j &\in O\left[-\frac{\lambda - 4p + u_{j+1} + \cdots + u_{k+1}}{j}, u_{j+1}\right], \ j = k-1, k-2, \ldots, 2, \\
u_1 &= -(\lambda - 4p + u_2 + \cdots + u_{k+1}).
\end{aligned}$$

Proof. The proof follows from Lemma 2.3.3 and Lemma 7 in Stufken and Tang [26], see Section 2.5. □

Theorem 2.3.6. *For even t, even $\lambda = 2\lambda^*$, and $k = t + 2$, the complete set S_2 of non-OD-equivalent $OA(\lambda 2^t, k, 2, t)$ as solutions to equation (2.3.6) under inequalities (2.3.4) is given by*

$$\begin{aligned}
p &\in Z\left[0, \frac{\lambda^*}{2}\right], \\
u_{k+1} &\in Z\left[-\frac{\lambda^* - 2p}{k+1}, \frac{\lambda^* - 2p}{k-1}\right], \\
u_k &\in Z\left[-\frac{\lambda^* - 2p + u_{k+1}}{k}, -|u_{k+1}|\right], \\
u_j &\in Z\left[-\frac{\lambda^* - 2p + u_{j+1} + \cdots + u_{k+1}}{j}, u_{j+1}\right], \ j = k-1, k-2, \ldots, 2, \\
u_1 &= -(\lambda^* - 2p + u_2 + \cdots + u_{k+1}).
\end{aligned}$$

Proof. The proof follows from Lemma 2.3.4 and Lemma 9 in Stufken and Tang [26], see Section 2.5. □

For even t and $s = 2$, OD-equivalence reduces the solution set to S_1 for odd λ, and S_2 for even λ non-OD-equivalent $\text{OA}(\lambda 2^t, t+2, 2, t)$. The sizes of S_1 and S_2 are smaller than the corresponding sizes obtained for non-isomorphic OA($\lambda 2^t, t+2, 2, t$).

Theorems 2.3.5 and 2.3.6 were validated by comparing to the classification results obtained by the methods of Geyer *et al.* [27] for the following cases of OAs: OA($4\lambda, 4, 2, 2$) for $\lambda \in [51]$, OA($16\lambda, 6, 2, 4$) for $\lambda \in [30]$, OA($64\lambda, 8, 2, 6$) for $\lambda \in [30]$, OA($256\lambda, 10, 2\ , 8$) for $\lambda = 1, 3, 5$, and OA($1024\lambda, 12, 2, 10$) for $\lambda = 1, 3$. The numbers of non-OD-equivalent classes generated by both were in agreement.

2.4 Conclusion

In this paper we used OD-equivalence operations, a larger set of operations than isomorphism operations, to analytically classify all non-OD-equivalent OA($\lambda 2^t, t+2, 2, t$) when t is even. Future research will involve classifying OA($\lambda 2^t, t+3, 2, t$) up to OD-equivalence for even t. We anticipate that classifying OA($\lambda 2^t, t+3, 2, t$) up to OD-equivalence for even t is more tangible than classifying up to isomorphism.

2.5 Addendum

Let

$$\lambda + u_1 + \cdots + u_{k+1} = 4p, \tag{2.5.1}$$

where p is a non-negative integer and $u_j \in 2\mathbb{Z}+1$ are such that $|u_j| \leqslant \lambda - 2$ for $j = 1, \ldots, k+1$. Furthermore, let

$$u_1 \leqslant \cdots \leqslant u_k \leqslant -|u_{k+1}|, \tag{2.5.2}$$

$$u_1 \leqslant \cdots \leqslant u_{k-1} \leqslant -|u_k|, \quad u_{k+1} \leqslant -|u_k| - 2. \tag{2.5.3}$$

Theorem 1. *Suppose that t is even and λ is odd. We then have that: (i) each solution $(u_1, \ldots, u_{k+1}, p)$ to equation (2.5.1) under either (2.5.2) or (2.5.3) determines an OA($\lambda 2^t, t+2, 2, t$) with J-vector given by $J_{\ell_j} = 2^t u_j$ for $j = 1, \ldots, k+1$; (ii) the* *complete set of non-isomorphic $OA(\lambda 2^t, t+2, 2, t)$s is given by collecting the arrays obtained in (i) over all the solutions to equation (2.5.1).*

Let $\lambda = 2\lambda^*$, where λ^* is a non-negative integer. Let

$$\lambda^* + u_1 + \cdots + u_{k+1} = 2p, \tag{2.5.4}$$

where p is a non-negative integer and $u_j \in \mathbb{Z}$ are such that $|u_j| \leqslant \lambda^*$ for $j = 1, \ldots, k+1$. Furthermore, let

$$u_1 \leqslant \cdots \leqslant u_k \leqslant -|u_{k+1}|, \tag{2.5.5}$$

$$u_1 \leqslant \cdots \leqslant u_{k-1} \leqslant -|u_k|, \quad u_{k+1} \leqslant -|u_k| - 1. \tag{2.5.6}$$

Theorem 2. *Suppose that t is even and $\lambda = 2\lambda^*$ is also even. We then have that: (i) each solution $(u_1, \ldots, u_{k+1}, p)$ to equation (2.5.4) under either (2.5.5) or (2.5.6) determines an $OA(\lambda 2^t, t+2, 2, t)$ with J-vector given by $J_{\ell_j} = 2^{t+1} u_j$ for $j = 1, \ldots, k+1$; (ii) the complete set of non-isomorphic $OA(\lambda 2^t, t+2, 2, t)$s for even t and even λ is given by collecting the arrays obtained in (i) over all the solutions to equation (2.5.4).*

Lemma 7. *For even t and odd λ, if $\lambda \leqslant t-1$, then equation (2.5.1) has no solution under inequalities (2.5.2). If $\lambda \geqslant t+1$, then equation (2.5.1) has at least one solution* *under inequalities (2.5.2) and the complete set S_1 of solutions is given by*

$$
\begin{aligned}
p &\in Z\left[0, \frac{\lambda - t - 1}{4}\right], \\
u_{k+1} &\in O\left[-\frac{\lambda - 4p}{k+1}, \frac{\lambda - 4p}{k-1}\right], \\
u_k &\in O\left[-\frac{\lambda - 4p + u_k + 1}{k}, -|u_{k+1}|\right], \\
u_j &\in O\left[-\frac{\lambda - 4p + u_{j+1} + \cdots + u_{k+1}}{j}, u_{j+1}\right], \ j = k-1, k-2, \ldots, 2, \\
u_1 &= -(\lambda - 4p + u_2 + \cdots + u_{k+1}).
\end{aligned}
$$

Lemma 9. *For even t, even $\lambda = 2\lambda^*$, the complete set S_2 of solutions to (2.5.4) under inequalities (2.5.5) is given by*

$$
\begin{aligned}
p &\in Z\left[0, \frac{\lambda^*}{2}\right], \\
u_{k+1} &\in Z\left[-\frac{\lambda^* - 2p}{k+1}, \frac{\lambda^* - 2p}{k-1}\right], \\
u_k &\in Z\left[-\frac{\lambda^* - 2p + u_{k+1}}{k}, -|u_{k+1}|\right], \\
u_j &\in Z\left[-\frac{\lambda^* - 2p + u_{j+1} + \cdots + u_{k+1}}{j}, u_{j+1}\right], \ j = k-1, k-2, \ldots, 2, \\
u_1 &= -(\lambda^* - 2p + u_2 + \cdots + u_{k+1}).
\end{aligned}
$$

III. The dimension of the convex hull of feasible points for the Legendre pair problem

3.1 Introduction

A well-known problem in combinatorics is finding Hadamard matrices. A *Hadamard matrix* $\mathbf{H}$ is a $n \times n$ matrix of ± 1's satisfying $\mathbf{H}\mathbf{H}^\top = n\mathbf{I}_n$, where $\mathbf{I}_n$ is the $n \times n$ identity matrix. It is well known that for a Hadamard matrix of order n to exist, n must be divisible by 4. It has been long conjectured (i.e., the Hadamard conjecture) that, for each n divisible by 4, there exists a Hadamard matrix of order n.

A Hadamard matrix can be constructed by finding a solution to a system of constraints for a pair of vectors. To define this system of constraints, let $\mathbb{Z}_\ell = \{0, \ldots, \ell - 1\}$ denote the integers mod ℓ. Let $\mathbf{u}, \mathbf{v} \in \{-1, 1\}^\ell$. Then $(\mathbf{u}, \mathbf{v})$ is a Legendre pair (LP) if $\mathbf{1}^\top \mathbf{u} = \mathbf{1}^\top \mathbf{v}$ and

$$P_{\mathbf{u}}(j) + P_{\mathbf{v}}(j) = -2, \quad \forall j \in \mathbb{Z}_\ell - \{0\}, \tag{3.1.1}$$

where $P_{\mathbf{u}}(j) = \sum_{i \in \mathbb{Z}_\ell} \mathbf{u}(i)\mathbf{u}(i-j)$ is the *periodic autocorrelation function* of $\mathbf{u}$. The problem of finding solutions to the system of constraints (3.1.1) is known as the *LP problem.*

Let $\mathbb{Q}^{\mathbb{Z}_\ell}$ be the vector space of all functions from $\mathbb{Z}_\ell$ to $\mathbb{Q}$. A *circulant shift* of $\mathbf{u} \in \mathbb{Q}^{\mathbb{Z}_\ell}$ by $j \in \mathbb{Z}_\ell$, denoted by $c_j\mathbf{u}$, is a transformation such that $c_j\mathbf{u}(i) = \mathbf{u}(i-j), i \in \mathbb{Z}_\ell$. The *circulant matrix* of $\mathbf{u} \in \mathbb{Q}^{\mathbb{Z}_\ell}$, denoted by $\mathbf{C}_{\mathbf{u}}$, is a matrix such that $(j+1)$th row of $\mathbf{C_u}$ is $(c_j\mathbf{u})^\top$. If $(\mathbf{u},\mathbf{v})$ is an LP, then

$$\mathbf{H} = \begin{bmatrix} -1 & -1 & \mathbf{1}^\top & \mathbf{1}^\top \\ -1 & 1 & \mathbf{1}^\top & -\mathbf{1}^\top \\ \mathbf{1} & \mathbf{1} & \mathbf{C_v} & \mathbf{C_u} \\ \mathbf{1} & -\mathbf{1} & \mathbf{C_u}^\top & -\mathbf{C_v}^\top \end{bmatrix}$$

is a $(2\ell+2)\times(2\ell+2)$ Hadamard matrix, where $\mathbf{1}$ is the vector of all 1s of length ℓ [17]. Hence, to construct a $(2\ell+2)\times(2\ell+2)$ Hadamard matrix for some odd ℓ, it suffices to find an LP of length ℓ. It is conjectured that an LP of length ℓ exists for each odd ℓ, where this conjecture implies the Hadamard conjecture. It is shown in Arasu *et al.* [17] that an LP $(\mathbf{u},\mathbf{v})$ must satisfy

$$\mathbf{1}^\top\mathbf{u} = \mathbf{1}^\top\mathbf{v} = \pm 1.$$

In this paper, we choose an LP $(\mathbf{u},\mathbf{v})$ to satisfy

$$\mathbf{1}^\top\mathbf{u} = \mathbf{1}^\top\mathbf{v} = -1. \tag{3.1.2}$$

Let $\rtimes$ be the semidirect product as defined in Rotman [30]. Then, the group $\mathbb{Z}_\ell \rtimes \mathbb{Z}_\ell^\times$ acts on $\mathbf{u} \in \mathbb{Q}^{\mathbb{Z}_\ell}$ by $(j,k)\mathbf{u}(i) = \mathbf{u}((j,k)^{-1}i)$ for each $(j,k) \in \mathbb{Z}_\ell \rtimes \mathbb{Z}_\ell^\times, i \in \mathbb{Z}_\ell$. The group $(\mathbb{Z}_\ell \times \mathbb{Z}_\ell) \rtimes \mathbb{Z}_\ell^\times$ acts on any pair $(\mathbf{u},\mathbf{v}) \in \mathbb{Q}^{\mathbb{Z}_\ell} \oplus \mathbb{Q}^{\mathbb{Z}_\ell}$ by

$$((i,j),k))(\mathbf{u},\mathbf{v}) = ((i,k)\mathbf{u},(j,k)\mathbf{v})$$

for each $((i,j),k)) \in (\mathbb{Z}_\ell \times \mathbb{Z}_\ell) \rtimes \mathbb{Z}_\ell^\times$. Two pairs $(\mathbf{u},\mathbf{v}),(\mathbf{u}',\mathbf{v}')$ are *equivalent* if they are in the same orbit under the action of $(\mathbb{Z}_\ell \times \mathbb{Z}_\ell) \rtimes \mathbb{Z}_\ell^\times$. If $(\mathbf{u},\mathbf{v})$ is an LP and $(\mathbf{u}',\mathbf{v}')$ is equivalent to $(\mathbf{u},\mathbf{v})$, then $(\mathbf{u}',\mathbf{v}')$ is also an LP [17].

For the group $(\mathbb{Z}_\ell \times \mathbb{Z}_\ell) \rtimes \mathbb{Z}_\ell^\times$ and the constraints

$$\boldsymbol{\beta}_1^\top \mathbf{u} = c_1, \quad \boldsymbol{\beta}_2^\top \mathbf{v} = c_2 \tag{3.1.3}$$

for some $c_1, c_2 \in \mathbb{R}$ implied by the integrality of the constraints (3.1.1) of the LP problem, the non-trivial constraints

$$((j,k)(\boldsymbol{\beta}_1) - \boldsymbol{\beta}_1)^\top \mathbf{u} = 0 \text{ and } ((i,k)(\boldsymbol{\beta}_2) - \boldsymbol{\beta}_2)^\top \mathbf{v} = 0 \tag{3.1.4}$$

for $((i,j),k) \in (\mathbb{Z}_\ell \times \mathbb{Z}_\ell) \rtimes \mathbb{Z}_\ell^\times$ are valid for the feasible set of pairs $(\mathbf{u}, \mathbf{v})$ satisfying constraints (3.1.1). The valid equalities (3.1.4) based on $(\mathbb{Z}_\ell \times \mathbb{Z}_\ell) \rtimes \mathbb{Z}_\ell^\times$ put restrictions on the dimension of the convex hull of all feasible solutions to the set of constraints (3.1.1). It is far from clear what these restrictions would be. By using methods of representation theory as developed by Bulutoglu [31], we establish Corollary 3.1.3 which provides such restrictions for the LP problem. We also provide sets of equality constraints of the form in equations (3.1.4) that could be satisfied by the feasible set of non-linear constraints (3.1.1) that define an LP. Finally, by using recent results in number theory, we show that equations (3.1.2) are the only equations of the form as given by equations (3.1.3) that are satisfied by an LP $(\mathbf{u}, \mathbf{v})$ for $\ell = p^n$ or $\ell = pq$, where p, q are distinct odd primes and n is a positive integer.

Throughout the paper, for a set of vectors S in a vector space over the field of scalars $\mathbb{F}$, $\mathrm{Span}_{\mathbb{F}}(S)$ is the span, $\mathrm{Aff}_{\mathbb{F}}(S)$ is the affine hull, and $\dim_{\mathbb{F}}(S)$ is the dimension of the affine hull of the vectors in S over $\mathbb{F}$. If $\mathbb{F}$ is not provided, then $\mathbb{F} = \mathbb{R}$. Also, let $\mathrm{Conv}(S)$ be the convex hull of the vectors in S.

Let $(\mathbf{u}^0, \mathbf{v}^0)$ be an LP, and $\mathcal{F}_{\mathbf{u}^0} = (\mathbb{Z}_\ell \rtimes \mathbb{Z}_\ell^\times)\mathbf{u}^0$ and $\mathcal{F}_{\mathbf{v}^0} = (\mathbb{Z}_\ell \rtimes \mathbb{Z}_\ell^\times)\mathbf{v}^0$ be the orbits of $\mathbf{u}^0$ and $\mathbf{v}^0$ under the action of $\mathbb{Z}_\ell \rtimes \mathbb{Z}_\ell^\times$, respectively. Let $\mathcal{F}$ be the feasible set of all pairs $(\mathbf{u}, \mathbf{v})$ satisfying constraints (3.1.1). In this chapter, we determine $\dim(\mathrm{Conv}(\mathcal{F}))$, and investigate all possible values of $\dim(\mathrm{Conv}(\mathcal{F}_{\mathbf{u}^0}))$ and $\dim(\mathrm{Conv}(\mathcal{F}_{\mathbf{v}^0}))$. For each $n \in \mathbb{Z}_{\geqslant 1}$, let $[n] = \{1, \ldots, n\}$. The following theorems and corollary are our main results.

Theorem 3.1.1. *Let ℓ be an odd positive integer. Let $\mathcal{F}$ be the feasible set of of all pairs $(\mathbf{u}, \mathbf{v})$ satisfying constraints (3.1.1). If $\mathcal{F} \neq \varnothing$, then*

$$\dim(\mathrm{Conv}(\mathcal{F})) = 2\ell - 2.$$

Theorem 3.1.2. *Let $(\mathbf{u}^0, \mathbf{v}^0)$ be a Legendre pair. Then there exists $U_1, U_2 \subseteq \{d \in [\ell] : d \mid \ell\}$ such that $U_1 \cap U_2 = \varnothing$ and*

$$\begin{aligned} \dim(\mathrm{Conv}(\mathcal{F}_{\mathbf{u}^0})) &= \ell - 1 - \left(\textstyle\sum_{d \in U_1} \phi\left(\frac{l}{d}\right)\right), \\ \dim(\mathrm{Conv}(\mathcal{F}_{\mathbf{v}^0})) &= \ell - 1 - \left(\textstyle\sum_{d \in U_2} \phi\left(\frac{l}{d}\right)\right). \end{aligned} \tag{3.1.5}$$

Corollary 3.1.3. *Let p, q be distinct odd primes and $n \in \mathbb{Z}_{\geqslant 1}$. If $\ell = p^n$ or $\ell = pq$, then* $\dim(\mathrm{Conv}(\mathcal{F}_{\mathbf{u}^0})) = \dim(\mathrm{Conv}(\mathcal{F}_{\mathbf{v}^0})) = \ell - 1$.

In Section 3.2, we present necessary background in representation theory, the power spectral density, vanishing sums of roots of unity, and affine geometry. In Section 3.3, we prove our main result. Section 3.4, presents recent advancements. Section 3.5 discusses future work.

3.2 Background theory

Let G be a finite group and V be a finite dimensional vector space over a field $\mathbb{F}$. Let $\mathrm{GL}(V)$ be the $\mathbb{F}$-automorphisms of V. An $\mathbb{F}$-*representation* of G is a pair (ρ, V), where $\rho \colon G \to \mathrm{GL}(V)$ is a homomorphism. A subspace W of V is a *subrepresentation* of V if $\rho(g)W \subseteq W$ for all $g \in G$. In this case, we say that W is G-*stable*. A representation (ρ, V) of G is an *irreducible* representation if the only subrepresentations of V

are $\mathrm{Span}_{\mathbb{F}}(\mathbf{0})$ and V. The only fields $\mathbb{F}$ that we consider are $\mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$, the rational, real, and complex numbers, respectively. Every representation may be assumed unitary with respect to a complex inner product [32] which will be denoted by $\langle\cdot|\cdot\rangle$. We use the convention $\langle\alpha\mathbf{u}|\mathbf{v}\rangle = \bar{\alpha}\langle\mathbf{u}|\mathbf{v}\rangle$ for $\alpha \in \mathbb{F}$ and $\mathbf{u}, \mathbf{v} \in V$. Throughout the paper, every group G is finite, every vector space V is finite dimensional, and every representation is unitary.

Theorem 3.2.1. *[Maschke] Every unitary representation of a finite group may be decomposed as a direct sum into orthogonal irreducible subrepresentations.*

The decomposition in Theorem 3.2.1 is said to be *multiplicity-free* if each irreducible appears only once.

The *character* of an $\mathbb{F}$-representation (ρ, V) of G is the map $\chi_\rho\colon G \to \mathbb{F}$ defined by $\chi_\rho(g) = \mathrm{Tr}(\rho(g))$, where $\mathrm{Tr}(\rho(g))$ is the trace of $\rho(g)$. We say that the character is an *irreducible character* if the character corresponds to an irreducible representation. We may simply write the character as χ if the representation is clear from the context.

The following theorem is from Serre [32].

Theorem 3.2.2. *Let (ρ, V) be a $\mathbb{C}$-representation of a group G. Let*

$$V = m_1V_1 \oplus \ldots \oplus m_hV_h$$

with $m_i \in \mathbb{Z}_{\geqslant 1}$ be a decomposition of V into irreducibles (ρ_i, V_i) with characters χ_i for each $i \in [h]$, where $\chi_i = \chi_{\rho_i}$. Then the orthogonal projection $\mathbf{P}_i$ of V onto $m_iV_i = \bigoplus_{k=1}^{m_i} V_i$ is given by

$$\mathbf{P}_i = \frac{\dim_{\mathbb{C}}(V_i)}{|G|}\sum_{g\in G}\overline{\chi_i(g)}\mathbf{M}_{\rho(g)}.$$

where $\mathbf{M}_{\rho(g)}$ is the matrix of $\rho(g)$ in some orthonormal basis for V.

The *exponent* m of a group G is the smallest nonnegative integer such that $g^m = e$ for all $g \in G$. Let (ρ, V) be a $\mathbb{C}$-representation of a group G with exponent m. Then $\rho(g)^m = id$ for each $g \in G$, where id is the identity mapping on V. Therefore, the eigenvalues of $\rho(g)$ are mth roots of unity. Throughout the paper, let ζ_m be a primitive mth root of unity, where primitive means ζ_m has order m. Since $\chi(g)$ is the trace of $\rho(g)$, $\chi(g) \in \mathbb{Q}(\zeta_m)$, where $\mathbb{Q}(\zeta_m)$ is the field extension of $\mathbb{Q}$ obtained by adjoining ζ_m. It is well known that the automorphism group $\mathrm{Aut}(\mathbb{Q}(\zeta_m))$ of $\mathbb{Q}(\zeta_m)$ is isomorphic to $\mathbb{Z}_\ell^\times = \{k \in \mathbb{Z}_\ell \mid (k, m) = 1\}$, where (k, m) is the greatest common divisor of k and m. Since $\chi(g) \in \mathbb{Q}(\zeta_m)$, there is a natural action on the characters of the representations.

The following theorem is from Bulutoglu [31].

Theorem 3.2.3. *Let (ρ, V) be a $\mathbb{Q}$-representation of a group G with exponent m. Let*

$$V = W_1 \oplus \cdots \oplus W_b$$

be a decomposition of V into irreducible $\mathbb{Q}$-subrepresentations. Let $V_\mathbb{C}, W_{i\mathbb{C}}$ be the $\mathbb{C}$-representations obtained from V, W_i by extending the field of scalars of V, W_i to $\mathbb{C}$. Let

$$V_\mathbb{C} = W_{(1,1)} \oplus \cdots \oplus W_{(1,r_1)} \oplus \cdots \oplus W_{(b,1)} \oplus \cdots \oplus W_{(b,r_b)}$$

be a decomposition of $V_\mathbb{C}$ into $(\rho_{(i,j)}, W_{(i,j)})$ irreducible $\mathbb{C}$-subrepresentations with characters $\chi_{\rho_{(i,j)}}$, where

$$W_{i\mathbb{C}} = W_{(i,1)} \oplus \cdots \oplus W_{(i,r_i)} \ \ \text{for} \ \ i \in [b].$$

For each $i \in [b]$, let $\mathcal{O}_{\rho_{(i,1)}}$ be the $\mathrm{Aut}(\mathbb{Q}(\zeta_m))$-orbit of $\chi_{\rho_{(i,1)}}$. Let $\mathbf{M}_{\rho(g)}$ be the matrix of $\rho(g)$ for each $g \in G$, with respect to the standard basis. If $V_\mathbb{C}$ is multiplicity-free, *then*

$$\mathbf{P}_{W_i} = \frac{\dim_{\mathbb{C}}(W_{(i,1)})}{|G|} \sum_{g \in G} \left(\sum_{\chi \in \mathcal{O}_{\rho_{(i,1)}}} \overline{\chi(g)} \mathbf{M}_{\rho(g)} \right)$$

is the orthogonal projection matrix into the ith irreducible $\mathbb{Q}$-subrepresentation subspace $\mathrm{Col}_{\mathbb{Q}}(\mathbf{P}_{W_i})$ for each $i \in [b]$.

Theorem 3.2.4. *For each $k \in \mathbb{Z}_\ell$, let χ_k be the irreducible character of the $\mathbb{C}$-representation of $\mathbb{Z}_\ell$. For each divisor d of ℓ, let $\mathcal{O}_d = \{\chi_k \mid (k, \ell) = d \text{ and } k \in \mathbb{Z}_\ell\}$. Then*

(i) $|\mathcal{O}_d| = \phi(\ell/d)$, *where ϕ is Euler's totient function.*

(ii) $\mathcal{O}_d = \mathrm{Aut}(\mathbb{Q}(\zeta_{\ell/d}))\chi_d$.

Proof. Let d be a divisor of ℓ. (i) follows immediately from the definition of Euler's totient function. To prove (ii), note that $(d, \ell) = d$ implies $\chi_d \in \mathcal{O}_d$. Also, since $o(\chi_d(1)) = o(\zeta_\ell^d) = \ell/(d, \ell) = \ell/d$, $\chi_d(1)$ is a primitive (ℓ/d)th root of unity, where $o(\zeta_\ell^d)$ is the order of ζ_ℓ^d in the group of all ℓ roots of unity. Therefore the cyclic group generated by $\chi_d(1)$ contains all (ℓ/d)th roots of unity. Then a (ℓ/d)th root of unity has the form $(\chi_d(1))^r$ for some integer r and is primitive if and only if $r \in \mathbb{Z}_{\ell/d}^\times$ because $o\left((\chi_d(1))^r\right) = (\ell/d)/((r, \ell/d)) = \ell/d$.

Let $\chi_s \in \mathcal{O}_d$. Since $\chi_s(1)$ is a primitive (ℓ/d)th root of unity, there exists $r \in \mathbb{Z}_{\ell/d}^\times$ such that $\chi_s(1) = (\chi_d(1))^r$. Since $\mathrm{Aut}(\mathbb{Q}(\zeta_{\ell/d})) \cong \mathbb{Z}_{\ell/d}^\times$, there exists $\sigma_r \in \mathrm{Aut}(\mathbb{Q}(\zeta_{\ell/d}))$ such that $\chi_s(1) = \sigma_r(\chi_d(1))$. Since the χ_i's are uniquely determined by their value on 1, we have $\chi_s = \sigma_r \chi_d$. Therefore, $\chi_s \in \mathrm{Aut}(\mathbb{Q}(\zeta_{\ell/d}))\chi_d$. Hence, $\mathcal{O}_d \subseteq \mathrm{Aut}(\mathbb{Q}(\zeta_{\ell/d}))\chi_d$.

Conversely, let $\chi_s \in \mathrm{Aut}(\mathbb{Q}(\zeta_{\ell/d}))\chi_d$. Then there exists $\sigma_r \in \mathrm{Aut}(\mathbb{Q}(\zeta_{\ell/d}))$ such that $\chi_s = \sigma_r \chi_d$. We will show that $(s, \ell) = d$. Suppose that $(s, \ell) = c$. We have

$$\zeta_\ell^s = \chi_s(1) = \sigma_r(\chi_d(1)) = \zeta_\ell^{rd}.$$

Then

$$s \equiv rd \pmod{\ell}. \tag{3.2.1}$$

Since $d \mid \ell$ and $d \mid rd$, we have $d \mid s$. Therefore, $d \mid c$. Equation (3.2.1) and $c = (s, \ell)$ implies that c. Since $(r, \ell/d) = 1$, there exists $m, n \in \mathbb{Z}$ such that $mr + n\ell/d = 1$. Also, since $mrd + n\ell = d$, we have that c. Hence, $c = d$. It follows that $\chi_s \in \mathcal{O}_d$. Thus, $\mathcal{O}_d = \mathrm{Aut}(\mathbb{Q}(\zeta_{\ell/d}))\chi_d$. $\square$

The standard basis

$$\mathbf{e}_i(j) = \begin{cases} 1 & \text{if } j = i, \\ 0 & \text{otherwise.} \end{cases}$$

spans $\mathbb{Q}^{\mathbb{Z}_\ell}$. Note that $\mathbb{Q}^{\mathbb{Z}_\ell}$ is isomorphic to $\mathbb{Q}^\ell$. We further equip $\mathbb{Q}^{\mathbb{Z}_\ell}$ with an inner product $\langle \cdot | \cdot \rangle$ such that $\{\mathbf{e}_i\}_{i \in \mathbb{Z}_\ell}$ is an orthonormal basis.

The *regular representation* of a group G is the linear space generated by the basis $\{\mathbf{e}_g\}_{g \in G}$ and G acts on the basis by $h\mathbf{e}_g = \mathbf{e}_{hg}$ for each $h, g \in G$.

The following theorem is well known.

Theorem 3.2.5. *Let $(R, \mathbb{Q}^{\mathbb{Z}_\ell})$ be the regular $\mathbb{Q}$-representation of $\mathbb{Z}_\ell$. Let $(\mathbb{Q}^{\mathbb{Z}_\ell})_{\mathbb{C}}$ be the $\mathbb{C}$-representation obtained by extending the field of scalars to $\mathbb{C}$. Then*

$$(\mathbb{Q}^{\mathbb{Z}_\ell})_{\mathbb{C}} = \bigoplus_{i \in \mathbb{Z}_\ell} V_i$$

is the decomposition of $(\mathbb{Q}^{\mathbb{Z}_\ell})_{\mathbb{C}}$ into the one-dimensional irreducible $\mathbb{C}$-representations of $\mathbb{Z}_\ell$, where the $\mathbb{C}$-representations $(\rho_k, V_k), k \in \mathbb{Z}_\ell$ are given by $\rho_k(1)\colon V_k \to V_k$, $\mathbf{v} \mapsto \zeta_\ell^k \mathbf{v}$. Moreover, $\chi_k(i) = \mathrm{Tr}(\rho_k(i)) = \zeta_\ell^{ki}$ for each $k, i \in \mathbb{Z}_\ell$.

Theorem 3.2.6. *Let $(R, \mathbb{Q}^{\mathbb{Z}_\ell})$ be the regular $\mathbb{Q}$-representation of $\mathbb{Z}_\ell$. Let*

$$\mathbf{P}_d = \frac{1}{\ell} \sum_{i \in \mathbb{Z}_\ell} \sum_{\chi \in \mathcal{O}_d} \overline{\chi(i)} \mathbf{M}_{R(i)}$$

for each divisor d of ℓ, where $\mathbf{M}_{R(i)}$ is the matrix of $R(i)$ with respect to the standard basis $\{\mathbf{e}_i\}_{i\in\mathbb{Z}_\ell}$, and $\mathcal{O}_d$ is defined in Theorem 3.2.4. Then

$$\mathbb{Q}^{\mathbb{Z}_\ell} = \bigoplus_{d|\ell} \mathrm{Col}_{\mathbb{Q}}(\mathbf{P}_d)$$

is the decomposition of $\mathbb{Q}^{\mathbb{Z}_\ell}$ into irreducible $\mathbb{Q}$-subrepresentations.

Proof. Let d be a divisor of ℓ. By Theorem 3.2.4, the inner sum of $\mathbf{P}_d$ corresponds to the orbit of χ_d under the action of $\mathrm{Aut}(\mathbb{Q}(\zeta_{\ell/d}))$. Further, by Theorem 3.2.5 $(\mathbb{Q}^{\mathbb{Z}_\ell})_{\mathbb{C}}$ is multiplicity-free. Then by Theorem 3.2.3, $\mathrm{Col}_{\mathbb{Q}}(\mathbf{P}_d)$ is an irreducible $\mathbb{Q}$-subrepresentation of $\mathbb{Q}^{\mathbb{Z}_\ell}$. Now, by the identity $\ell = \sum_{d|\ell}\phi(\ell/d)$, it suffices to show that $\dim_{\mathbb{Q}}(\mathrm{Col}_{\mathbb{Q}}(\mathbf{P}_d)) = \phi(\ell/d)$. Since R is the regular representation of $\mathbb{Z}_\ell$, only $R(0)$ will contribute to the trace of $\mathbf{P}_d$. Then

$$\begin{aligned}
\mathrm{Tr}\left(\mathbf{P}_d\right) &= \mathrm{Tr}\left(\frac{1}{\ell}\sum_{i\in\mathbb{Z}_\ell}\sum_{\chi\in\mathcal{O}_d}\overline{\chi(i)}\mathbf{M}_{R(i)}\right)\\
&= \frac{1}{\ell}\sum_{i\in\mathbb{Z}_\ell}\sum_{\chi\in\mathcal{O}_d}\overline{\chi(i)}\,\mathrm{Tr}\left(\mathbf{M}_{R(i)}\right)\\
&= \frac{1}{\ell}\sum_{\chi\in\mathcal{O}_d}\mathrm{Tr}\left(\mathbf{M}_{R(0)}\right)\\
&= \frac{1}{\ell}\sum_{\chi\in\mathcal{O}_d}\ell\\
&= \sum_{\chi\in\mathcal{O}_d}1\\
&= |\mathcal{O}_d|\\
&= \phi\left(\frac{l}{d}\right).
\end{aligned}$$

□

The group $\mathbb{Z}_\ell \rtimes \mathbb{Z}_\ell^\times$ acts on $\mathbb{Z}_\ell$ by $(a,b)i = bi + a$ for each $i \in \mathbb{Z}_\ell$ and $(a,b) \in \mathbb{Z}_\ell \rtimes \mathbb{Z}_\ell^\times$. Then a representation $(T, \mathbb{Q}^{\mathbb{Z}_\ell})$ of $\mathbb{Z}_\ell \rtimes \mathbb{Z}_\ell^\times$ is given by the action on the basis $T(a,b)\mathbf{e}_i = \mathbf{e}_{bi+a}$. We find that $\mathbb{Q}^{\mathbb{Z}_\ell}$ has the same decomposition as in Theorem 3.2.6.

Theorem 3.2.7. *The decomposition* $\mathbb{Q}^{\mathbb{Z}_\ell} = \bigoplus_{d|\ell} \mathrm{Col}_{\mathbb{Q}}(\mathbf{P}_d)$ *is a decomposition of* $\mathbb{Q}^{\mathbb{Z}_\ell}$ *into irreducible* $\mathbb{Q}$*-subrepresentations of* $\mathbb{Z}_\ell \rtimes \mathbb{Z}_\ell^\times$*.*

Proof. Let d be a divisor of ℓ. We have $\mathrm{Col}_{\mathbb{C}}(\mathbf{P}_d) = \bigoplus_{(k,\ell)=d} V_k$, where the V_k are spanned by $\mathbf{v}_k = \sum_{i\in\mathbb{Z}_\ell} \bar{\zeta}_\ell^{ki}\mathbf{e}_i$. Let $(a,b) \in \mathbb{Z}_\ell \rtimes \mathbb{Z}_\ell^\times$. Observe

$$T(a,b)^{-1}\mathbf{v}_k = \sum_{i\in\mathbb{Z}_\ell} \bar{\zeta}_\ell^{k(a,b)i}\mathbf{e}_i = \bar{\zeta}_\ell^{ka} \sum_{i\in\mathbb{Z}_\ell} \bar{\zeta}_\ell^{kbi}\mathbf{e}_i = \bar{\zeta}_\ell^{ka}\mathbf{v}_{bk}.$$

Since $(b,\ell) = 1$, $(bk,\ell) = d$ if and only if $(k,\ell) = d$. Therefore, $\mathrm{Col}_{\mathbb{C}}(\mathbf{P}_d)$ is a $\mathbb{C}$-subrepresentation of $\mathbb{Z}_\ell \rtimes \mathbb{Z}_\ell^\times$. Since $\mathrm{Col}_{\mathbb{Q}}(\mathbf{P}_d)$ is an irreducible $\mathbb{Q}$-subrepresentation of $\mathbb{Z}_\ell$ and $\mathbb{Z}_\ell$ is a subgroup of $\mathbb{Z}_\ell \rtimes \mathbb{Z}_\ell^\times$, $\mathrm{Col}_{\mathbb{Q}}(\mathbf{P}_d)$ is an irreducible $\mathbb{Q}$-subrepresentation of $\mathbb{Z}_\ell \rtimes \mathbb{Z}_\ell^\times$. ∎

Observe that $\mathbb{Q}^{\mathbb{Z}_\ell} \oplus \mathbb{Q}^{\mathbb{Z}_\ell}$ is spanned by $\{(\mathbf{e}_i, \mathbf{0}), (\mathbf{0}, \mathbf{e}_i)\}_{i,j\in\mathbb{Z}_\ell}$. Let $(L, \mathbb{Q}^{\mathbb{Z}_\ell} \oplus \mathbb{Q}^{\mathbb{Z}_\ell})$ be the $\mathbb{Q}$-representation of $(\mathbb{Z}_\ell \times \mathbb{Z}_\ell) \rtimes \mathbb{Z}_\ell^\times$ defined by $L((a,b),n))(\mathbf{e}_i, \mathbf{0}) = (\mathbf{e}_{ni+a}, \mathbf{0})$ and $L((a,b),n))(\mathbf{0}, \mathbf{e}_i) = (\mathbf{0}, \mathbf{e}_{ni+b})$ for each $((a,b),n) \in (\mathbb{Z}_\ell \times \mathbb{Z}_\ell) \rtimes \mathbb{Z}_\ell^\times$ and $i \in \mathbb{Z}_\ell$.

Lemma 3.2.8. *The maps defined by*

$$\begin{aligned} \pi_i \colon (\mathbb{Z}_\ell \times \mathbb{Z}_\ell) \rtimes \mathbb{Z}_\ell^\times &\to \mathbb{Z}_\ell \rtimes \mathbb{Z}_\ell^\times \\ ((a_1,a_2),n) &\mapsto (a_i, n) \end{aligned}$$

$i = 1, 2,$ *are homomorphisms.*

Proof. We show that $\pi_1 \colon (\mathbb{Z}_\ell \times \mathbb{Z}_\ell) \rtimes \mathbb{Z}_\ell^\times \to \mathbb{Z}_\ell \rtimes \mathbb{Z}_\ell^\times$ is a homomorphism. The other map is shown to be a homomorphism similarly. Let $((a,b),n), ((a',b'),n') \in (\mathbb{Z}_\ell \times \mathbb{Z}_\ell) \rtimes \mathbb{Z}_\ell^\times$.

Then

$$\begin{aligned}\pi_1(((a,b),n)((a',b'),n')) &= \pi_1(((a,b)+n(a',b'),nn')) \\ &= \pi_1(((a+na',b+nb'),nn')) \\ &= (a+na',nn') \\ &= (a,n)(a',n') \\ &= \pi_1(((a,b),n))\pi_1(((a',b'),n')). \qquad \square\end{aligned}$$

Theorem 3.2.9. *Let $(L, \mathbb{Q}^{\mathbb{Z}_\ell} \oplus \mathbb{Q}^{\mathbb{Z}_\ell})$ be the $\mathbb{Q}$-representation of $(\mathbb{Z}_\ell \times \mathbb{Z}_\ell) \rtimes \mathbb{Z}_\ell^\times$ defined above. Then*

$$\mathbb{Q}^{\mathbb{Z}_\ell} \oplus \mathbb{Q}^{\mathbb{Z}_\ell} = \bigoplus_{d|\ell} \mathrm{Col}_{\mathbb{Q}}(\mathbf{P}_d) \oplus \bigoplus_{d'|\ell} \mathrm{Col}_{\mathbb{Q}}(\mathbf{P}_{d'}) \tag{3.2.2}$$

is the decomposition into irreducible $\mathbb{Q}$-subrepresentations of $(\mathbb{Z}_\ell \times \mathbb{Z}_\ell) \rtimes \mathbb{Z}_\ell^\times$.

Proof. Let $\pi_i\colon (\mathbb{Z}_\ell \times \mathbb{Z}_\ell) \rtimes \mathbb{Z}_\ell^\times \to \mathbb{Z}_\ell \rtimes \mathbb{Z}_\ell^\times$ for $i = 1, 2$ be the homomorphisms defined in Lemma 3.2.8. Let $(T, \mathbb{Q}^{\mathbb{Z}_\ell})$ be the $\mathbb{Q}$-representation of $\mathbb{Z}_\ell \rtimes \mathbb{Z}_\ell^\times$. Then the maps $T \circ \pi_i\colon (\mathbb{Z}_\ell \times \mathbb{Z}_\ell) \rtimes \mathbb{Z}_\ell^\times \to \mathrm{GL}(\mathbb{Q}^{\mathbb{Z}_\ell}), i = 1, 2$ are homomorphisms. Let $((a,b),n) \in (\mathbb{Z}_\ell \times \mathbb{Z}_\ell) \rtimes \mathbb{Z}_\ell^\times$. Observe

$$(T\circ\pi_1 \oplus T\circ\pi_2)((a,b),n)(\mathbf{e}_i,\mathbf{0}) = T(a,n)\oplus T(b,n))(\mathbf{e}_i,\mathbf{0}) = (T(a,n)\mathbf{e}_i,\mathbf{0}) = (\mathbf{e}_{ni+a},\mathbf{0})$$

and similarly $(T\circ\pi_1 \oplus T\circ\pi_2)((a,b),n)(\mathbf{0},\mathbf{e}_i) = (\mathbf{0},\mathbf{e}_{ni+b})$. Therefore, $L = T\circ\pi_1 \oplus T\circ\pi_2$. Then, $L\colon (\mathbb{Z}_\ell \times \mathbb{Z}_\ell) \rtimes \mathbb{Z}_\ell^\times \to \mathrm{GL}(\mathbb{Q}^{\mathbb{Z}_\ell}) \oplus \mathrm{GL}(\mathbb{Q}^{\mathbb{Z}_\ell})$. By Theorem 3.2.7, the representation $(T, \mathbb{Q}^{\mathbb{Z}_\ell})$ of $\mathbb{Z}_\ell \rtimes \mathbb{Z}_\ell^\times$ has the decomposition $\mathbb{Q}^{\mathbb{Z}_\ell} = \bigoplus_{d|\ell} \mathrm{Col}_{\mathbb{Q}}(\mathbf{P}_d)$. Thus, $\mathbb{Q}^{\mathbb{Z}_\ell} \oplus \mathbb{Q}^{\mathbb{Z}_\ell}$ has the decomposition (3.2.2) into irreducible $\mathbb{Q}$-subrepresentations of $(\mathbb{Z}_\ell \times \mathbb{Z}_\ell) \rtimes \mathbb{Z}_\ell^\times$. $\square$

For $k \in \mathbb{Z}_\ell$, let $\mathbf{v}_k = \sum_{i\in\mathbb{Z}_\ell} \bar{\zeta}_\ell^{ki} \mathbf{e}_i$ be the basis vector for the one-dimensional $\mathbb{C}$-representation V_k of $\mathbb{Z}_\ell$. The vectors $\mathbf{v}_0, \ldots, \mathbf{v}_{\ell-1}$ will be called the *discrete Fourier basis*. The *discrete Fourier transform* (DFT) of $\mathbf{u} \in \mathbb{Q}^{\mathbb{Z}_\ell}$ is $\mu_k(\mathbf{u}) = \langle \mathbf{v}_k | \mathbf{u} \rangle$, $k \in \mathbb{Z}_\ell$.

The *power spectral density* (PSD) of $\mathbf{u} \in \mathbb{Q}^{\mathbb{Z}_\ell}$ is $|\mu_k(\mathbf{u})|^2, k \in \mathbb{Z}_\ell$. The following theorem states an equivalent condition that an LP must satisfy in terms of the PSD.

Theorem 3.2.10 (Fletcher *et al.* [18]). *Let $\mathbf{u}, \mathbf{v} \in \{-1,1\}^\ell$. Then $(\mathbf{u},\mathbf{v})$ is an LP if and only if*

$$|\mu_k(\mathbf{u})|^2 + |\mu_k(\mathbf{v})|^2 = 2(\ell+1), \quad \textit{for } k \in \mathbb{Z}_\ell - \{0\}.$$

We say that there is a *vanishing sum of m ℓth roots of unity* if there exists m ℓth roots of unity $x_1, \dots, x_m$ (not necessarily distinct) satisfying $x_1 + \dots + x_m = 0$. We have the following result.

Theorem 3.2.11 (Lam and Leung [33]). *Suppose that $\ell = p_1^{n_1} \dots p_s^{n_s}$ for distinct primes $p_1, \dots, p_s$ and $n_1, \dots, n_s \in \mathbb{Z}_{\geqslant 1}$. Then there exists a vanishing sum of m ℓth roots of unity if and only if $m = a_1p_1 + \dots + a_sp_s$ for some $a_1, \dots, a_s \in \mathbb{Z}_{\geqslant 0}$.*

Let $0 \leqslant m \leqslant \ell$. We say ℓ is *m-balanced* if there is a vanishing sum of m distinct ℓth roots of unity. Since $\sum_{j=0}^{\ell-1} \zeta_\ell^j = 0$, ℓ is m-balanced if and only if ℓ is $(\ell-m)$-balanced.

Theorem 3.2.12 (Sivek [34]). *Suppose that $\ell = p_1^{n_1} \dots p_s^{n_s}$ for distinct primes $p_1, \dots, p_s$ and $n_1, \dots, n_s \in \mathbb{Z}_{\geqslant 1}$. Then ℓ is m-balanced if and only if $m = a_1p_1 + \dots + a_sp_s$ and $\ell - m = b_1p_1 + \dots + b_sp_s$ for some $a_1, \dots, a_s, b_1, \dots, b_s \in \mathbb{Z}_{\geqslant 0}$.*

Let $\mathbf{u} \in \{-1,1\}^\ell$ satisfy $\langle \mathbf{1} | \mathbf{u} \rangle = -1$. Let $J = \{j \in \mathbb{Z}_\ell \,|\, \mathbf{u}(j) = -1\}$. Then $\mu_k(\mathbf{u})$, for $k \neq 0$, has two forms

$$\mu_k(\mathbf{u}) = -2\sum_{j \in J} \zeta_\ell^{kj} = 2\sum_{j \notin J} \zeta_\ell^{kj}. \tag{3.2.3}$$

Note that $|J| = (\ell+1)/2$.

Lemma 3.2.13. *Let $\ell = p^n$, p an odd prime, and $n \in \mathbb{Z}_{\geqslant 1}$. Let $\mathbf{u} \in \{-1,1\}^\ell$ satisfy $\langle \mathbf{1} | \mathbf{u} \rangle = -1$. Then $\mu_k(\mathbf{u}) \neq 0$ for each $k \in \mathbb{Z}_\ell$.*

Proof. Since $\mu_0(\mathbf{u}) = -1$ we need to only verify for $k \in [\ell - 1]$. Suppose for a contradiction that $\mu_k(\mathbf{u}) = 0$ for some $k \in [\ell - 1]$. By equation (3.2.3), $\sum_{j\in J} \zeta_\ell^{kj} = 0$. By Theorem 3.2.11,

$$\frac{\ell + 1}{2} = ap$$

for some $a \in \mathbb{Z}_{\geqslant 0}$. This means that $p \mid ((\ell + 1)/2)$, a contradiction. Therefore, $\mu_k(\mathbf{u}) \neq 0$ for each $k \in \mathbb{Z}_\ell$. □

Lemma 3.2.14. *Let $\ell = pq$, p, q distinct odd primes. Let $\mathbf{u} \in \{-1, 1\}^\ell$ satisfy $\langle \mathbf{1}|\mathbf{u}\rangle = -1$. Then $\mu_k(\mathbf{u}) \neq 0$ for each $k \in \mathbb{Z}_\ell$.*

Proof. Since $\mu_0(\mathbf{u}) = -1$ we need to only verify for $k \in [\ell - 1]$. Suppose for a contradiction that $\mu_k(\mathbf{u}) = 0$ for some $k \in [\ell - 1]$. By equation (3.2.3),

$$\sum_{j\in J} \zeta_\ell^{kj} = \sum_{j\notin J} \zeta_\ell^{kj} = 0. \tag{3.2.4}$$

We proceed by considering the cases $(k, \ell) = 1, p, q$. We need not consider the case $(k, \ell) = \ell$ as $k \leqslant \ell - 1$. Suppose that $(k, \ell) = 1$. Then ζ_ℓ^k is a primitive ℓth root of unity. Therefore, the summands in equations (3.2.4) are of distinct roots of unity. This means ℓ is $(\ell + 1)/2$-balanced. By Theorem 3.2.12,

$$\frac{\ell + 1}{2} = ap + bq \text{ and } \frac{\ell - 1}{2} = cp + dq$$

for some $a, b, c, d \in \mathbb{Z}_{\geqslant 0}$. This means

$$\ell = \frac{\ell + 1}{2} + \frac{\ell - 1}{2} = (a + c)p + (b + d)q.$$

If $a + c \neq 0$ and $b + d \neq 0$, then $p \mid (b + d)$ and $q \mid (a + c)$. Consequently,

$$\ell = (a + c)p + (b + d)q \geqslant pq + pq = 2\ell,$$

a contradiction. Suppose that $a+c=0$. Then $a=c=0$ subsequently $q \mid ((\ell+1)/2)$, a contradiction. A similar contradiction occurs if $b+d=0$. Therefore, $\mu_k(\mathbf{u}) \neq 0$.

Suppose that $(k,\ell)=p$. Since $o(\zeta_\ell^k) = \ell/(k,\ell) = (pq)/p = q$, ζ_ℓ^k is a primitive qth root of unity. This means $\sum_{j\in J} \zeta_\ell^{kj} = 0$ is a vanishing sum of qth roots of unity. By Theorem 3.2.11,

$$\frac{\ell+1}{2} = aq$$

for some $a \in \mathbb{Z}_{\geqslant 0}$ subsequently $q \mid ((\ell+1)/2)$, a contradiction. A similar contradiction is reach in the case of $(k,\ell)=q$. Therefore, $\mu_k(\mathbf{u}) \neq 0$ for each $k \in \mathbb{Z}_\ell$. $\square$

Lemma 3.2.15. *Let V be a vector space over $\mathbb{F}$. Let $S \subseteq V$. Then $\mathrm{Aff}(S) - x$ is a linear space for any $x \in \mathrm{Aff}(S)$.*

Proof. Let $x \in \mathrm{Aff}(S)$ and let $W = \mathrm{Aff}(S) - x$. W is non-empty as $0 = x - x \in W$. Let $w, w' \in W$ and $\alpha \in \mathbb{F}$. Then $w = \sum_i \lambda_i s_i - x, w' = \sum_j \mu_j s_j - x$, where $\lambda_j, \mu_j \in \mathbb{F}$ and $\sum_i \lambda_i = \sum_j \mu_j = 1$. Observe

$$\alpha w + w' = \alpha(\sum_i \lambda_i s_i - x) + \sum_j \mu_j s_j - x = \sum_i \alpha\lambda_i s_i + \sum_j \mu_j s_j - \alpha x - x$$

and

$$\sum_i \alpha\lambda_i + \sum_j \mu_j - \alpha = \alpha + 1 - \alpha = 1.$$

Therefore, $\alpha w + w' \in W$ which means W is a linear space. $\square$

Lemma 3.2.16. *Let V be a vector space over $\mathbb{F}$. Let $S \subseteq V$. Then $\mathrm{Aff}_{\mathbb{F}}(S) = \mathrm{Span}_{\mathbb{F}}(S)$ if and only if $\mathbf{0} \in \mathrm{Aff}_{\mathbb{F}}(S)$.*

Proof. If $\mathrm{Aff}(S) = \mathrm{Span}(S)$, then $\mathrm{Aff}(S)$ is a linear space which means $\mathbf{0} \in \mathrm{Aff}(S)$. Suppose now that $\mathbf{0} \in \mathrm{Aff}(S)$. By Lemma 3.2.15, $\mathrm{Aff}(S) = \mathrm{Aff}(S) - \mathbf{0}$ is a linear space. Then since $S \subseteq \mathrm{Aff}(S)$, $\mathrm{Span}(S) \subseteq \mathrm{Aff}(S)$. Furthermore, since affine combinations are linear combinations, $\mathrm{Aff}(S) \subseteq \mathrm{Span}(S)$. Therefore, $\mathrm{Aff}(S) = \mathrm{Span}(S)$. $\square$

Let (ρ, V) be a unitary representation of a group G. Let $S \subseteq V$ be nonempty. Then the *barycenter* of S is $\beta(S) = (1/|S|)\sum_{\mathbf{v}\in S}\mathbf{v}$. The *fixed space* of V is $V^G = \{\mathbf{v} \in V \mid \rho(g)\mathbf{v} = \mathbf{v}\ \forall g \in G\}$. It is easy to show that V^G is a subrepresentation of V. By Theorem 3.2.1, there exists a subrepresentation orthogonal to V^G. Let $\mathbf{P}$ be the orthogonal projection matrix onto V^G.

Lemma 3.2.17. *Let (ρ, V) be a unitary representation of a group G. Let $\mathbf{x} \in V$. Then $\mathbf{P}\mathbf{x} = \beta(G\mathbf{x})$.*

Proof. Let $\mathbf{u}_1, \ldots, \mathbf{u}_k$ be an orthonormal basis for V^G. Then

$$\mathbf{P}\mathbf{y} = \sum_{i\in[k]}\langle \mathbf{u}_i|\mathbf{y}\rangle \mathbf{u}_i.$$

for any $\mathbf{y} \in V$. Let $S = G\mathbf{x}$. Then, for each $i \in [k]$ and $\mathbf{v} = r\mathbf{x} \in S$ for some $r \in G$, we have

$$\langle \mathbf{u}_i|r\mathbf{x}\rangle = \langle r\mathbf{u}_i|r\mathbf{x}\rangle = \langle \mathbf{u}_i|\mathbf{x}\rangle.$$

Then

$$\langle \mathbf{u}_i|\beta(G\mathbf{x})\rangle = \frac{1}{|S|}\sum_{r\mathbf{x}\in S}\langle \mathbf{u}_i|r\mathbf{x}\rangle = \frac{1}{|S|}\sum_{r\mathbf{x}\in S}\langle \mathbf{u}_i|\mathbf{x}\rangle = \langle \mathbf{u}_i|\mathbf{x}\rangle.$$

Since $\beta(G\mathbf{x}) \in V^G$,

$$\beta(G\mathbf{x}) = \sum_{i\in[k]}\langle \mathbf{u}_i|\beta(G\mathbf{x})\rangle \mathbf{u}_i = \sum_{i\in[k]}\langle \mathbf{u}_i|\mathbf{x}\rangle \mathbf{u}_i = \mathbf{P}\mathbf{x}.$$

□

Lemma 3.2.18. *Let $(R, \mathbb{Q}^{\mathbb{Z}_\ell})$ be the regular $\mathbb{Q}$-representation of $\mathbb{Z}_\ell$. Then the projection matrix $\mathbf{P}_0$ onto the fixed space of $\mathbb{Q}^{\mathbb{Z}_\ell}$ is $(1/\ell)\mathbf{J}$, where $\mathbf{J}$ is the $\ell \times \ell$ matrix of all one's.*

Proof. Notice that the fixed space of V is a direct sum of copies of the trivial representation of $\mathbb{Z}_\ell$. By Theorem 3.2.2,

$$\mathbf{P}_0 = \frac{1}{\ell}\sum_{j\in\mathbb{Z}_\ell} \overline{\chi_0(j)}\mathbf{M}_{R(j)} = \frac{1}{\ell}\sum_{j\in\mathbb{Z}_\ell} \mathbf{M}_{R(j)} = \frac{1}{\ell}\mathbf{J}. \qquad \square$$

3.3 Main results

We start with the proof of the first of our main results.

Proof of Theorem 3.1.1.

Proof. Let $\mathcal{F}_1 = \{\mathbf{u} \in \{-1,1\}^\ell \,|\, \exists \mathbf{v} \ni (\mathbf{u},\mathbf{v}) \text{ is an LP}\}$ and $\mathcal{F}_2 = \{\mathbf{v} \in \{-1,1\}^\ell \,|\, \exists \mathbf{u} \ni (\mathbf{u},\mathbf{v}) \text{ is an LP}\}$. By symmetry, $\mathcal{F}_1 = \mathcal{F}_2$. Since $\mathcal{F} \neq \varnothing$, there exists $(\mathbf{u}^\top, \mathbf{v}^\top)^\top \in \mathcal{F}$. Then $\mathbf{u} \in \mathcal{F}_1$ and $\mathbf{v} \in \mathcal{F}_2$. Let $\mathbf{p} = \beta(\mathbb{Z}_\ell \mathbf{u}) = -1/\ell\mathbf{1}$. Then $\mathbf{p} \in \mathrm{Conv}(\mathcal{F}_1) \subseteq \mathrm{Aff}(\mathcal{F}_1)$. To reach the desired conclusion observe the following facts:

(i) Since $\mathcal{F}_1 = \mathcal{F}_2$, $\mathrm{Span}_{\mathbb{C}}(\mathcal{F}_1 - \mathbf{p}) = \mathrm{Span}_{\mathbb{C}}(\mathcal{F}_2 - \mathbf{p})$.

(ii) Since both $\mathrm{Span}_{\mathbb{C}}(\mathcal{F}_1 - \mathbf{p})$ and $\mathrm{Span}_{\mathbb{C}}(\mathcal{F}_2 - \mathbf{p})$ are $\mathbb{Z}_\ell$-stable subrepresentations of $(\mathbb{Q}^{\mathbb{Z}_\ell})_{\mathbb{C}}$ orthogonal to $\mathbf{1}$, both $\mathrm{Span}_{\mathbb{C}}(\mathcal{F}_1 - \mathbf{p})$ and $\mathrm{Span}_{\mathbb{C}}(\mathcal{F}_2 - \mathbf{p})$ must be an orthogonal direct sum of the irreducible $\mathbb{C}$-representations $V_1, \ldots, V_{\ell-1}$ of $(\mathbb{Q}^{\mathbb{Z}_\ell})_{\mathbb{C}}$.

(ii) Both $\mathrm{Span}_{\mathbb{C}}(\mathcal{F}_1 - \mathbf{p})$ and $\mathrm{Span}_{\mathbb{C}}(\mathcal{F}_2 - \mathbf{p})$ cannot be orthogonal to an irreducible V_k for some $k = 1, \ldots, \ell - 1$. For this would imply that the DFT of $\mathbf{u}$ and $\mathbf{v}$ must satisfy

$$\mu_k(\mathbf{u}) = \langle \mathbf{u} | \mathbf{v}_k \rangle = \langle \mathbf{u} - \mathbf{p} | \mathbf{v}_k \rangle = 0,$$

similarly, $\mu_k(\mathbf{v}) = 0$, contradicting Theorem 3.2.10.

By (i),(ii), and (iii),

$$\mathrm{Span}_{\mathbb{C}}(\mathcal{F}_1 - \mathbf{p}) = V_1 \oplus \cdots \oplus V_{\ell-1} \text{ and } \mathrm{Span}_{\mathbb{C}}(\mathcal{F}_2 - \mathbf{p}) = V_1 \oplus \cdots \oplus V_{\ell-1}.$$

Let $\mathbf{f} = \beta((\mathbb{Z}_\ell \times \mathbb{Z}_\ell)(\mathbf{u}^\top, \mathbf{v}^\top)^\top) = -1/\ell(\mathbf{1}^\top, \mathbf{1}^\top)^\top$. Then $\mathbf{f} \in \mathrm{Conv}(\mathcal{F}) \subseteq \mathrm{Aff}(\mathcal{F})$. It is evident that

$$\mathrm{Span}_{\mathbb{C}}(\mathcal{F} - \mathbf{f}) = \mathrm{Span}_{\mathbb{C}}(\mathcal{F}_1 - \mathbf{p}) \oplus \mathrm{Span}_{\mathbb{C}}(\mathcal{F}_2 - \mathbf{p}).$$

Then by Theorem 3.2.6, $\mathrm{Span}_{\mathbb{Q}}(\mathcal{F}_i - \mathbf{p}) = \bigoplus_{\substack{d|\ell \\ d\neq\ell}} \mathrm{Col}_{\mathbb{Q}}(\mathbf{P}_d)$ for $i = 1, 2$, and by fact (i),

$$\mathrm{Span}_{\mathbb{Q}}(\mathcal{F} - \mathbf{f}) = \left(\bigoplus_{\substack{d|\ell \\ d\neq\ell}} \mathrm{Col}_{\mathbb{Q}}(\mathbf{P}_d) \right) \oplus \left(\bigoplus_{\substack{d|\ell \\ d\neq\ell}} \mathrm{Col}_{\mathbb{Q}}(\mathbf{P}_d) \right).$$

Hence,

$$\dim(\mathrm{Conv}(\mathcal{F}) = \dim(\mathrm{Span}(\mathcal{F}-\mathbf{f})) = \dim_{\mathbb{Q}}(\mathrm{Span}_{\mathbb{Q}}(\mathcal{F}-\mathbf{f})) = (\ell-1)+(\ell-1) = 2\ell-2. \quad \square$$

The complexification of a vector space $U_{\mathbb{C}}$ of U over $\mathbb{Q}$ is defined as $U_{\mathbb{C}} = \mathbb{C} \otimes_{\mathbb{Q}} U$. Suppose that $\langle \cdot | \cdot \rangle$ is the inner product of V. It is plain to show that an inner product on $V_{\mathbb{C}}$ may be defined as $\langle z \otimes \mathbf{v} | z' \otimes \mathbf{v}' \rangle = z\overline{z'} \langle \mathbf{v} | \mathbf{v}' \rangle$. Then the following lemma follows immediately.

Lemma 3.3.1. *Let V be an inner product space over $\mathbb{Q}$ and U, W subspaces of V. Then U is orthogonal to W if and only if $U_{\mathbb{C}}$ is orthogonal to $W_{\mathbb{C}}$.*

Lemma 3.3.2. *Let p, q be distinct odd primes and $n \in \mathbb{Z}_{\geqslant 1}$. Suppose that $\ell = p^n$ or $\ell = pq$. Let $\mathbf{u} \in \{-1, 1\}^\ell$ satisfy $\langle \mathbf{1} | \mathbf{u} \rangle = -1$ and let $\mathbf{y} = \mathbf{u} + (1/\ell)\mathbf{1}$. Then*

$$\mathrm{Span}_{\mathbb{Q}}(\mathbb{Z}_\ell \mathbf{y}) = \bigoplus_{\substack{d|\ell \\ d\neq\ell}} \mathrm{Col}_{\mathbb{Q}}(\mathbf{P}_d),$$

where $\mathbf{P}_d$ is defined in Theorem 3.2.6.

Proof. Since $\mathrm{Span}_{\mathbb{Q}}(\mathbb{Z}_\ell \mathbf{y})$ is $\mathbb{Z}_\ell$-stable, it is a $\mathbb{Q}$-subrepresentation of $\mathbb{Q}^{\mathbb{Z}_\ell}$. Then, by Theorem 3.2.1, $\mathrm{Span}_{\mathbb{Q}}(\mathbb{Z}_\ell \mathbf{y})$ is an orthogonal direct sum of irreducible $\mathbb{Q}$-subrepresentations of $\mathbb{Q}^{\mathbb{Z}_\ell}$. By Theorem 3.2.6, the irreducible $\mathbb{Q}$-subrepresentations of $\mathbb{Q}^{\mathbb{Z}_\ell}$ are $\mathrm{Col}_{\mathbb{Q}}(\mathbf{P}_d)$ for each divisor d of ℓ. We first show that $\mathrm{Span}_{\mathbb{Q}}(\mathbb{Z}_\ell \mathbf{y})$ is orthogonal only to $\mathrm{Col}_{\mathbb{Q}}(\mathbf{P}_0)$. Since $\mathrm{Col}_{\mathbb{Q}}(\mathbf{P}_0) = \mathrm{Span}_{\mathbb{Q}}(\mathbf{1})$, $\langle \mathbf{y} | \mathbf{1} \rangle = 0$, and the representation is unitary, we have $\mathrm{Span}_{\mathbb{Q}}(\mathbb{Z}_\ell \mathbf{y})$ is orthogonal to $\mathrm{Col}_{\mathbb{Q}}(\mathbf{P}_0)$.

Consider now $d \neq \ell$. Since $(\mathrm{Col}_{\mathbb{Q}}(\mathbf{P}_d))_{\mathbb{C}} = \mathrm{Col}_{\mathbb{C}}(\mathbf{P}_d)$ is spanned by $\mathbf{v}_k = \sum_{i \in \mathbb{Z}_\ell} \bar{\zeta}_\ell^{ki} \mathbf{e}_i$ for $k \in \mathbb{Z}_\ell$ such that $(k, \ell) = d$,

$$\langle \mathbf{v}_k | \mathbf{y} \rangle = \langle \mathbf{v}_k | \mathbf{u} + \frac{1}{\ell} \mathbf{1} \rangle = \langle \mathbf{v}_k | \mathbf{u} \rangle = \mu_k(\mathbf{u}).$$

By Lemmas 3.2.13 and 3.2.14, $\langle \mathbf{y} | \mathbf{v}_k \rangle \neq 0$. Since this holds for each k, by Lemma 3.3.1, $\mathrm{Span}_{\mathbb{Q}}(\mathbb{Z}_\ell \mathbf{y})$ is not orthogonal to $\mathrm{Col}_{\mathbb{Q}}(\mathbf{P}_d)$. As this holds for each divisor $d \neq \ell$ of ℓ, we must have

$$\mathrm{Span}_{\mathbb{Q}}(\mathbb{Z}_\ell \mathbf{y}) = \bigoplus_{\substack{d|\ell \\ d \neq \ell}} \mathrm{Col}_{\mathbb{Q}}(\mathbf{P}_d). \qquad \square$$

Corollary 3.3.3. *Let ℓ and $\mathbf{y}$ be as in Lemma 3.3.2. Then* $\dim_{\mathbb{Q}}(\mathrm{Span}_{\mathbb{Q}}(\mathbb{Z}_\ell \mathbf{y})) = \ell - 1$.

Proof. By Lemma 3.3.2, $\mathrm{Span}_{\mathbb{Q}}(\mathbb{Z}_\ell \mathbf{y}) = \bigoplus_{\substack{d|\ell \\ d \neq \ell}} \mathrm{Col}_{\mathbb{Q}}(\mathbf{P}_d)$. Since $\dim_{\mathbb{Q}}(\mathrm{Col}_{\mathbb{Q}}(\mathbf{P}_0)) = 1$, we have

$$\dim_{\mathbb{Q}}(\mathrm{Span}_{\mathbb{Q}}(\mathbb{Z}_\ell \mathbf{y})) = \dim_{\mathbb{Q}}(\mathbb{Q}^{\mathbb{Z}_\ell}) - \dim_{\mathbb{Q}}(\mathrm{Col}_{\mathbb{Q}}(\mathbf{P}_0)) = \ell - 1. \qquad \square$$

Corollary 3.3.4. *Let $\mathbf{1}^\perp$ denote the orthogonal complement of* $\mathrm{Span}_{\mathbb{Q}}(\mathbf{1})$ *in* $\mathbb{Q}^{\mathbb{Z}_\ell}$. *Then*

$$\mathbf{1}^\perp = \bigoplus_{\substack{d|\ell \\ d \neq \ell}} \mathrm{Col}_{\mathbb{Q}}(\mathbf{P}_d)$$

is the decomposition of $\mathbf{1}^\perp$ into irreducible subrepresentations of $\mathbb{Q}^{\mathbb{Z}_\ell}$.

Proof. Since $\mathbb{Q}^{\mathbb{Z}_\ell} = \mathrm{Span}_{\mathbb{Q}}(\mathbf{1}) \oplus \mathbf{1}^\perp$, we have $\mathbf{I}_{\mathbb{Q}^{\mathbb{Z}_\ell}} = \mathbf{P}_0 + \mathbf{P}_{\mathbf{1}^\perp}$, where $\mathbf{I}_{\mathbb{Q}^{\mathbb{Z}_\ell}}$ is the identity matrix on $\mathbb{Q}^{\mathbb{Z}_\ell}$. Since $\mathbf{I}_{\mathbb{Q}^{\mathbb{Z}_\ell}} = \sum_{d|\ell} \mathbf{P}_d$, we have

$$\mathbf{P}_{\mathbf{1}^\perp} = \mathbf{I}_{\mathbb{Q}^{\mathbb{Z}_\ell}} - \mathbf{P}_0 = \sum_{\substack{d|\ell \\ d\neq\ell}} \mathbf{P}_d.$$

Therefore,

$$\mathbf{1}^\perp = \mathrm{Col}_{\mathbb{Q}}(\mathbf{P}_{\mathbf{1}^\perp}) = \mathrm{Col}_{\mathbb{Q}}(\sum_{\substack{d|\ell \\ d\neq\ell}} \mathbf{P}_d) = \bigoplus_{\substack{d|\ell \\ d\neq\ell}} \mathrm{Col}_{\mathbb{Q}}(\mathbf{P}_d).$$

Here we used the fact that the $\mathbf{P}_d$'s are orthogonal projection matrices that necessarily satisfy $\mathbf{P}_d\mathbf{P}_{d'} = \delta_{dd'}\mathbf{P}_d$, where $\delta_{dd'}$ is the Kronecker delta function. $\square$

Corollary 3.3.5. *Let $\mathbf{1}^\perp$ be as defined in Corollary 3.3.4. Then*

$$\dim_{\mathbb{Q}}(\mathbf{1}^\perp) = \ell - 1.$$

Proof. Since $\mathbb{Q}^{\mathbb{Z}_\ell} = \mathrm{Span}_{\mathbb{Q}}(\mathbf{1}) \oplus \mathbf{1}^\perp$, the result follows immediately. $\square$

Lemma 3.3.6. *Let p, q be distinct odd primes and $n \in \mathbb{Z}_{\geqslant 1}$. Suppose that $\ell = p^n$ or $\ell = pq$. Let $\mathbf{u} \in \{-1, 1\}^\ell$ satisfy $\langle \mathbf{1}|\mathbf{u}\rangle = -1$. Then* $\dim(\mathrm{Aff}(\mathbb{Z}_\ell\mathbf{u})) = \ell - 1$.

Proof. Let $\mathbf{y} = \mathbf{u} - \mathbf{P}_0\mathbf{u}$, where $\mathbf{P}_0$ is the projection onto the fixed space of $\mathbb{Q}^{\mathbb{Z}_\ell}$. By Lemma 3.2.18, $\mathbf{y} = \mathbf{u} + (1/\ell)\mathbf{1}$. Since $\mathbf{P}_0\mathbf{y} = \mathbf{P}_0\mathbf{u} - \mathbf{P}_0^2\mathbf{u} = \mathbf{0}$ and $\beta(\mathbb{Z}_\ell\mathbf{y}) = \mathbf{P}_0\mathbf{y}$ by Lemma 3.2.17, $\mathbf{0} = \beta(\mathbb{Z}_\ell\mathbf{y}) \in \mathrm{Conv}_{\mathbb{Q}}(\mathbb{Z}_\ell\mathbf{y})$ as $\beta(\mathbb{Z}_\ell\mathbf{y})$ is a convex combination of points of $\mathbb{Z}_\ell\mathbf{y}$. Then by Lemma 3.2.16, we have $\mathrm{Span}_{\mathbb{Q}}(\mathbb{Z}_\ell\mathbf{y}) = \mathrm{Aff}_{\mathbb{Q}}(\mathbb{Z}_\ell\mathbf{y})$. Observe that

$$\dim_{\mathbb{Q}}(\mathrm{Aff}_{\mathbb{Q}}(\mathbb{Z}_\ell\mathbf{u})) = \dim_{\mathbb{Q}}(\mathrm{Aff}_{\mathbb{Q}}(\mathbb{Z}_\ell\mathbf{u}) + (1/\ell)\mathbf{1}) = \dim_{\mathbb{Q}}(\mathrm{Aff}_{\mathbb{Q}}(\mathbb{Z}_\ell\mathbf{y})) = \dim_{\mathbb{Q}}(\mathrm{Span}_{\mathbb{Q}}(\mathbb{Z}_\ell\mathbf{y})).$$

Then by Corollary 3.3.3,

$$\dim(\mathrm{Aff}(\mathbb{Z}_\ell\mathbf{u})) = \dim_{\mathbb{Q}}(\mathrm{Aff}_{\mathbb{Q}}(\mathbb{Z}_\ell\mathbf{u})) = \dim_{\mathbb{Q}}(\mathrm{Span}_{\mathbb{Q}}(\mathbb{Z}_\ell\mathbf{y})) = \ell - 1. \qquad \square$$

We now prove the main results.

Proof of Theorem 3.1.2.

Let $\dim_{\mathbb{Q}}(\mathrm{Aff}_{\mathbb{Q}}(\mathcal{F}_{\mathbf{u}^0})) = r_1$ and $\dim_{\mathbb{Q}}(\mathrm{Aff}_{\mathbb{Q}}(\mathcal{F}_{\mathbf{v}^0})) = r_2$. Let $X_1 = (\mathbb{Z}_\ell \rtimes \mathbb{Z}_\ell^\times)\mathbf{u}^0$, $X_2 = (\mathbb{Z}_\ell \rtimes \mathbb{Z}_\ell^\times)\mathbf{v}^0$. Since $\beta(X_i) = -(1/\ell)\mathbf{1}$ for $i = 1, 2$, $-(1/\ell)\mathbf{1}$ is a convex combination of points of X_i. Then, $-(1/\ell)\mathbf{1} \in \mathrm{Aff}_{\mathbb{Q}}(\mathcal{F}_{\mathbf{u}^0})$ and $-(1/\ell)\mathbf{1} \in \mathrm{Aff}_{\mathbb{Q}}(\mathcal{F}_{\mathbf{v}^0})$ as $X_1 = \mathcal{F}_{\mathbf{u}^0}$ and $X_2 = \mathcal{F}_{\mathbf{v}^0}$. Hence,

$$\dim_{\mathbb{Q}}(\mathrm{Span}_{\mathbb{Q}}(X_i + (1/\ell)\mathbf{1})) = r_i.$$

Since X_i and $\{\mathbf{1}\}$ are $\mathbb{Z}_\ell$-stable sets, $\mathrm{Span}_{\mathbb{Q}}(X_i + (1/\ell)\mathbf{1})$ is $\mathbb{Z}_\ell$-stable for $i = 1, 2$. Moreover, $\mathrm{Span}_{\mathbb{Q}}(X_i + (1/\ell)\mathbf{1}) \subseteq \mathbf{1}^\perp$ as each vector in $X_i + (1/\ell)\mathbf{1}$ is in $\mathbf{1}^\perp$. Now, by Theorem 3.2.7, there exists $U_i \subseteq \{d \in [\ell] : d \mid \ell\}$ such that

$$\mathbf{1}^\perp = \mathrm{Span}_{\mathbb{Q}}(X_i + \frac{1}{\ell}\mathbf{1}) \oplus \left(\oplus_{d \in U_i} \mathrm{Col}_{\mathbb{Q}}(\mathbf{P}_d)\right).$$

Since $\dim_{\mathbb{Q}}(\mathbf{1}^\perp) = \ell - 1$,

$$\dim_{\mathbb{Q}}(\mathrm{Span}_{\mathbb{Q}}(X_i + \frac{1}{\ell}\mathbf{1})) = \ell - 1 - \left(\sum_{d \in U_i} \phi\left(\frac{l}{d}\right)\right) = \sum_{d \mid \ell,\, d \neq \ell,\, d \notin U_i} \phi\left(\frac{l}{d}\right)$$

for $i = 1, 2$.

Now, we prove that $U_1 \cap U_2 = \varnothing$. For the sake of contradiction let $d' \in U_1 \cap U_2$ be such that $d' \neq \ell$. This implies that for each $i = 1, 2$, $\mathrm{Span}_{\mathbb{C}}(X_i + (1/\ell)\mathbf{1})$ is orthogonal to $\mathrm{Col}_{\mathbb{C}}(\mathbf{P}_{d'})$. Also, $\mathrm{Col}_{\mathbb{C}}(\mathbf{P}_{d'}) \subset (\mathbb{Q}^{\mathbb{Z}_\ell})_{\mathbb{C}}$ and $\mathrm{Col}_{\mathbb{C}}(\mathbf{P}_{d'})$ is invariant under the action of $\mathbb{Z}_\ell$. Then by Theorems 3.2.1 and 3.2.5, there exists $U' \subset \mathbb{Z}_\ell - \{0\}$ such that $\mathrm{Col}_{\mathbb{C}}(\mathbf{P}_{d'}) = \bigoplus_{i \in U'} V_i$. This implies that for each $i = 1, 2$, $\mathrm{Span}_{\mathbb{C}}(X_i + (1/\ell)\mathbf{1})$ is orthogonal to an irreducible V_k for some $k \in [\ell - 1]$. Then

$$\mu_k(\mathbf{u}^0) = \mu_k(\mathbf{u}^0 + \frac{1}{\ell}\mathbf{1}) = 0,$$

similarly, $\mu_k(\mathbf{v}^0) = 0$, contradicting Theorem 3.2.10.

Now, equations (3.1.5) for $\mathcal{F}_{\mathbf{u}^0}$ and $\mathcal{F}_{\mathbf{v}^0}$ follow because

$$\dim_{\mathbb{Q}}(\mathrm{Aff}_{\mathbb{Q}}(\mathcal{F}_{\mathbf{u}^0})) = \dim(\mathrm{Aff}(\mathcal{F}_{\mathbf{u}^0})) \text{ and } \dim_{\mathbb{Q}}(\mathrm{Aff}_{\mathbb{Q}}(\mathcal{F}_{\mathbf{v}^0})) = \dim(\mathrm{Aff}(\mathcal{F}_{\mathbf{v}^0})). \quad \square$$

Proof of Corollary 3.1.3. Since $\mathbb{Z}_\ell \mathbf{u}^0 \subseteq \mathcal{F}_{\mathbf{u}^0}$, $\mathrm{Conv}(\mathbb{Z}_\ell \mathbf{u}^0) \subseteq \mathrm{Conv}(\mathcal{F}_{\mathbf{u}^0})$. Then, by Lemma 3.3.6,

$$\ell - 1 = \dim_{\mathbb{Q}}(\mathrm{Aff}_{\mathbb{Q}}(\mathbb{Z}_\ell \mathbf{u}^0)) = \dim(\mathrm{Aff}(\mathbb{Z}_\ell \mathbf{u}^0)) = \dim(\mathrm{Conv}(\mathbb{Z}_\ell \mathbf{u}^0)) \leqslant \dim(\mathrm{Conv}(\mathcal{F}_{\mathbf{u}^0})).$$

The result now follows from Theorem 3.1.2 as $U = \varnothing$ is the only possibility. $\square$

Corollary 3.3.7. *Let p, q be distinct odd primes and $n \in \mathbb{Z}_{\geqslant 1}$. Let $\ell = p^n$ or $\ell = pq$. Let $(\mathbf{u}^0, \mathbf{v}^0)$ be an LP of length ℓ. Then the only linear constraints implied by the integrality of the constraints (3.1.1) are of the form*

$$\mathbf{1}^\top \mathbf{u}^0 = -1 \textit{ and } \mathbf{1}^\top \mathbf{v}^0 = -1. \tag{3.3.1}$$

Proof. Any other linear constraint different from constraints (3.3.1) would necessarily imply that $\dim(\mathrm{Conv}(\mathcal{F}_{\mathbf{u}^0})) < \ell - 1$ and $\dim(\mathrm{Conv}(\mathcal{F}_{\mathbf{v}^0})) < \ell - 1$, contradicting Corollary 3.1.3. $\square$

3.4 Recent advancements

The work presented in this section are results that have been established recently that will be used in continuing work for the LP problem.

Lemma 3.4.1 (Sylvester)**.** *Let $a, b, n \in \mathbb{Z}_{\geqslant 0}$. If $(a, b) = 1$ and $n \geqslant (a-1)(b-1)$, then there exists integers $x, y \geqslant 0$ such that $n = xa + yb$.*

Suppose that $\ell = pqm$ where p, q are odd primes, $3 \leqslant p < q$ and m is an odd integer such that $m > 2$. Since $\ell > 2(p-1)(q-1)$, we have $\ell - 1 \geqslant 2(p-1)(q-1)$, which implies $(\ell-1)/2 \geqslant (p-1)(q-1)$. By Lemma 3.4.1, $(\ell+1)/2 = ap + bq$ and $(\ell-1)/2 = cp + dq$ for some $a, b, c, d \in \mathbb{Z}_{\geqslant 0}$. Hence, by Theorem 3.2.12 there exists a $J \subset \mathbb{Z}_\ell$ such that $|J| = (\ell+1)/2$ and the corresponding $\mu_k(\mathbf{u})$ is 0 whenever k satisfies $(k, \ell) = 1$. This means that $\dim(\mathrm{Conv}(\mathcal{F}_{\mathbf{u}^0})) \leqslant \ell - 1 - \phi(\ell) < \ell - 1$. The results below allow us to exclude a given vector $\mathbf{u}$ to form an LP with another vector $\mathbf{v}$.

Lemma 3.4.2. *Let $m, n \in \mathbb{Z}$. If $m-2 \geqslant 2, n-2 \geqslant 1$ or $m-2 \geqslant 1, n-2 \geqslant 2$, then $n-2 \geqslant 2(n-1)/m$.*

Proof. If $m-2 \geqslant 2, n-2 \geqslant 1$ or $m-2 \geqslant 1, n-2 \geqslant 2$, then $(m-2)(n-2) \geqslant 2$. Adding $2(n-2)$ to $(m-2)(n-2) \geqslant 2$ yields $m(n-2) \geqslant 2(n-1)$, and so $n-2 \geqslant 2(n-1)/m$. □

Lemma 3.4.3. *Let p, q be distinct odd primes. Then the quotient of $2(q-1)(p-1)$ by division of p is at least q.*

Proof. Since for any integer k, $2(q-1)(p-1) = (2(q-1)-k)p + (kp - 2(q-1))$ we may choose the smallest such k such that $kp - 2(q-1) \geqslant 0$. Then $k = \lceil 2(q-1)/p \rceil$, where $\lceil n \rceil$ is the ceiling of n. Write $2(q-1)(p-1) = sp + r$, where $s = (2(q-1)-k)$ and $r = (kp - 2(q-1))$. Now, as p, q are distinct odd primes, WLOG suppose that $p \geqslant 3$, then $q \geqslant 5 \geqslant 4$. Since $p-2 \geqslant 1$ and $q-2 \geqslant 2$, by the above remark, $q-2 \geqslant 2(q-1)/p$. Therefore, $q-2 \geqslant k$. Then $s - q = 2(q-1) - k - q = q - 2 - k \geqslant k - k = 0$. □

Note that since $k - 1 < 2(q-1)/p$, then $r = pk - 2(q-1) < p$. Therefore, s and r are the quotient and remainder of $2(q-1)(p-1)$ upon division by p.

Lemma 3.4.4. *Let $\ell = p^\alpha q^\beta$, where p, q are distinct odd primes and $\alpha, \beta \in \mathbb{Z}_{\geqslant 1}$. Then $\phi(\ell) > (\ell - 1)/2$.*

Proof. By Lemma 3.4.3, $2(q-1)(p-1) = sp + r$ where $s \geqslant q$. Then

$$\begin{aligned}
2\phi(\ell) &= 2(q-1)(p-1)p^{\alpha-1}q^{\beta-1} \\
&= (sp + r)p^{\alpha-1}q^{\beta-1} \\
&\geqslant p^\alpha q^\beta + rp^{\alpha-1}q^{\beta-1} \\
&> p^\alpha q^\beta - 1 \\
&= \ell - 1
\end{aligned}$$

and the result follows. □

Theorem 3.4.5. *Let $\ell = pqm$, p, q odd primes, $3 \leqslant p < q$ and m an odd integer such that $m \geqslant 3$. Then no vector $\mathbf{u} \in \{-1, 1\}^\ell$ satisfying $\mu_k(\mathbf{u}) = 0$, $k \in \mathbb{Z}_\ell^\times$ belongs to an LP.*

Proof. Suppose for contradiction that $(\mathbf{u}, \mathbf{v})$ is an LP. Then $\mu_k(\mathbf{u}) = 0$ implies $\mu_k(\mathbf{u}) = 0$ for $k \in \mathbb{Z}_\ell^\times$. By Theorem 3.2.10,

$$|\mu_k(\mathbf{v})|^2 = 2(\ell + 1),\ k \in \mathbb{Z}_\ell^\times.$$

Then, by Corollary 3.4.8 and Lemma 3.4.4,

$$\sum_{k=1}^{\ell-1} |\mu_k(\mathbf{v})|^2 = (\ell+1)(\ell-1) < 2\phi(\ell)(\ell+1) \leqslant \sum_{k=1}^{\ell-1} |\mu_k(\mathbf{v})|^2,$$

a contradiction. □

The Fourier translation of the LP problem gave us equalities and inequalities that allowed us to exclude a vector from being an LP. The strength of Fourier analysis to the LP problem will be a continuing study.

Lemma 3.4.6. *Let* $\mathbf{u} \in \mathbb{Q}^\ell$. *Then* $\sum_{s \in \mathbb{Z}_\ell} P_{\mathbf{u}}(s) = (\mathbf{1}^\top \mathbf{u})^2$.

Proof. Let $\mathbf{C}_\mathbf{u}$ be the circulant matrix of $\mathbf{u}$. Then

$$\sum_{s \in \mathbb{Z}_\ell} P_{\mathbf{u}}(s) = \frac{1}{\ell}(\mathbf{1}^\top \mathbf{C}_\mathbf{u}^\top \mathbf{C}_\mathbf{u} \mathbf{1}) = \mathbf{1}^\top \mathbf{u} \mathbf{1}^\top \mathbf{u} = (\mathbf{1}^\top \mathbf{u})^2. \qquad \square$$

Lemma 3.4.7. *Let* $\mathbf{u} \in \mathbb{Q}^\ell$. *Then*

$$||\boldsymbol{\mu}(\mathbf{u})||^2 = \ell ||\mathbf{u}||^2.$$

Proof. Since $\boldsymbol{\mu} = \mathbf{U}^\top \mathbf{u}$, where $\mathbf{U}$ is the matrix whose columns are the discrete Fourier basis $\mathbf{v}_0, \ldots, \mathbf{v}_{\ell-1}$,

$$||\boldsymbol{\mu}(\mathbf{u})||^2 = \sum_{k \in \mathbb{Z}_\ell} |\mu_k(\mathbf{u})|^2 = \boldsymbol{\mu}^* \boldsymbol{\mu} = \mathbf{u}^\top \mathbf{U}^* \mathbf{U} \mathbf{u} = \mathbf{u}^\top \ell \mathbf{I}_\ell \mathbf{u} = \ell ||\mathbf{u}||^2,$$

where we used the fact that $\mathbf{U}^* \mathbf{U} = \ell \mathbf{I}_\ell$, $\mathbf{I}_\ell$ the $\ell \times \ell$ identity matrix. $\square$

Corollary 3.4.8. *Let* $\mathbf{u} \in \mathbb{Q}^{\mathbb{Z}_\ell}$ *satisfying* $||\mathbf{u}||^2 = \ell$ *and* $\langle \mathbf{1} | \mathbf{u} \rangle = -1$. *Then*

$$\sum_{k=1}^{\ell-1} |\mu_k(\mathbf{u})|^2 = (\ell+1)(\ell-1).$$

Proof. By Lemma 3.4.7,

$$\sum_{k=1}^{\ell-1} |\mu_k(\mathbf{u})|^2 = ||\boldsymbol{\mu}(\mathbf{u})||^2 - |\mu_0(\mathbf{u})|^2 = \ell^2 - 1 = (\ell+1)(\ell-1). \qquad \square$$

The Ramanujan's sum [35] is defined by $c_\ell(n) = \sum_{\substack{0<k<\ell \\ (k,\ell)=1}} e^{2\pi i k n/\ell}$. It is well known that for each $\ell, n \in \mathbb{N}$

$$c_\ell(n) = \mu\left(\frac{\ell}{(\ell,n)}\right)\frac{\phi(\ell)}{\phi\left(\frac{\ell}{(\ell,n)}\right)},$$

where

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ (-1)^r & \text{if } n = p_1 \dots p_r \text{ for distinct primes } p_1, \dots, p_r, \\ 0 & \text{if } n \text{ is divisible by some prime square} \end{cases}$$

is the Möbius function.

Theorem 3.4.9. *Let $\ell > 1$ and $\mathbf{u} \in \mathbb{Q}^\ell$. If d is a divisor of ℓ, then*

$$\sum_{\substack{0<k<\ell \\ (k,\ell)=d}} |\mu_k(\mathbf{u})|^2 = \sum_{s \in \mathbb{Z}_\ell} c_{\frac{\ell}{d}}(s) P_{\mathbf{u}}(s).$$

Proof. First note that

$$\sum_{\substack{0<k<\ell \\ (k,\ell)=d}} \zeta^{k(j-h)} = \sum_{\substack{0<k<\ell \\ (k,\ell)=d}} e^{\frac{2\pi i k(j-h)}{\ell}} = \sum_{\substack{0<r<\frac{\ell}{d} \\ (r,\frac{\ell}{d})=1}} e^{\frac{2\pi i r(j-h)}{\frac{\ell}{d}}} = c_{\frac{\ell}{d}}(j-h).$$

Let $\mathbf{1}, \mathbf{v}_1, \dots, \mathbf{v}_{\ell-1}$ be the discrete Fourier basis. Note that $\mathbf{v}_k\mathbf{v}_k^* = [a_{hj}]$, where $a_{hj} = \zeta^{k(j-h)}$. Then

$$\sum_{\substack{0<k<\ell \\ (k,\ell)=d}} \mathbf{v}_k\mathbf{v}_k^* = [b_{hj}^d],$$

where $b_{hj}^d = c_{\ell/d}(j-h)$. Since $\mu_k(\mathbf{u}) = \mathbf{u}^\top\mathbf{v}_k$,

$$|\mu_k(\mathbf{u})|^2 = \mu_k(\mathbf{u})\overline{\mu_k(\mathbf{u})} = (\mathbf{u}^\top\mathbf{v}_k)(\mathbf{v}_k^*\mathbf{u}) = \mathbf{u}^\top(\mathbf{v}_k\mathbf{v}_k^*)\mathbf{u}.$$

Then

$$
\begin{aligned}
\sum_{\substack{0<k<\ell\\(k,\ell)=d}} |\mu_k(\mathbf{u})|^2 &= \mathbf{u}^\top \left(\sum_{\substack{0<k<\ell\\(k,\ell)=d}} \mathbf{v}_k \mathbf{v}_k^* \right) \mathbf{u} \\
&= \sum_{h,j\in\mathbb{Z}_\ell} b_{hj}^d u_h u_j \\
&= \sum_{h,j\in\mathbb{Z}_\ell} c_{\frac{\ell}{d}}(j-h) u_h u_j \\
&= \sum_{s,h\in\mathbb{Z}_\ell} c_{\frac{\ell}{d}}(s) u_h u_{h+s} \\
&= \sum_{s\in\mathbb{Z}_\ell} c_{\frac{\ell}{d}}(s) \sum_{h\in\mathbb{Z}_\ell} u_h u_{h+s} \\
&= \sum_{s\in\mathbb{Z}_\ell} c_{\frac{\ell}{d}}(s) P_{\mathbf{u}}(s). \qquad \square
\end{aligned}
$$

We now present results that examine lower bounds on the dimension of the convex hull of feasible points to the LP problem to and utilize the results and ideas of Ingleton [36].

Theorem 3.4.10. *Let $\ell = p_1^{n_1} \dots p_s^{n_s}$ where $p_1, \dots, p_s$ are distinct odd primes and $n_1, \dots, n_s \in \mathbb{Z}_{\geqslant 1}$. Then*

$$
\dim(\mathrm{Conv}(\mathcal{F}_{\mathbf{u}^0}) \geqslant \sum_{j\in[s]} \sum_{i\in[n_j]} \phi(p_j^i).
$$

Proof. Let $\mathbf{u} \in \mathcal{F}_{\mathbf{u}^0}$ and $\mathbf{y} = \mathbf{u} + (1/\ell)\mathbf{1}$. To see that $\mathrm{Col}_{\mathbb{Q}}(\mathbf{P}_d) \subseteq \mathrm{Span}_{\mathbb{Q}}(\mathbb{Z}_\ell \mathbf{y})$ for each $d_{j,i} = p_1^{n_1} \dots p_j^i \dots p_s^{n_s}$, $j = 1, \dots, s$, $i = 0, \dots, n_j - 1$, of the form

$$
p_1 p_2^{n_2} \dots p_s^{n_s}, p_1^2 p_2^{n_2} \dots p_s^{n_s}, p_1^{n_1-1} p_2^{n_2} \dots p_s^{n_s}, \dots, p_1^{n_1} p_2^{n_2} \dots p_s, p_1^{n_1} p_2^{n_2} \dots p_s^2, \dots, p_1^{n_1} p_2^{n_2} \dots p_s^{n_s-1}.
$$

Assume otherwise and let $\langle \mathbf{y} | \mathbf{v}_k \rangle = 0$ for some k such that $(k, \ell) = d_{j,i}$, where $\mathbf{v}_k = \sum_{i\in\mathbb{Z}_\ell} \zeta_\ell^{ki} \mathbf{e}_i$. Then by Theorem 3.2.11, $p_j | (\ell + 1)/2$, a contradiction. Therefore,

$\mathrm{Col}_{\mathbb{Q}}(\mathbf{P}_d) \subseteq \mathrm{Span}_{\mathbb{Q}}(\mathbb{Z}_\ell \mathbf{y})$. Hence,

$$\dim_{\mathbb{Q}}(\mathrm{Span}_{Q}(\mathbb{Z}_\ell \mathbf{y})) \geqslant \sum_{j \in [s]} \sum_{i \in [n_j]} \phi(p_j^i). \qquad \square$$

Let $\mathbf{C} = \mathbf{C}_{\mathbf{u}}$ be the circulant matrix of $\mathbf{u} \in \mathbb{Q}^\ell$. Then $\mathbf{C}$ is *non-recurrent* if ℓ is the only divisor d of ℓ such that $u_i = u_j$ whenever $i \equiv j \pmod{d}$. If $\ell = p^\alpha p_1^{\alpha_1} \dots p_{m_1}^{\alpha_{m-1}}$ where $p, p_1, \dots, p_{m-1}$ are distinct primes and $\alpha, \alpha_1, \dots, \alpha_{m-1} \in \mathbb{Z}_{\geqslant 1}$, let

$$\tau(\ell, p) = 1 + \epsilon(m)\epsilon(\alpha)\phi(p) + \phi(p^\alpha) + \sum_{i \in [m-1]} \phi(p p_i^{\alpha_i}),$$

where $\epsilon(1) = 0$ and $\epsilon(k) = 1$ for $k \in \mathbb{Z}_{>1}$

Lemma 3.4.11. *(Ingleton [36]) Let $\ell = pq^\beta$, where p, q are distinct primes and $\beta \in \mathbb{Z}_{\geqslant 1}$. Let $\mathbf{C}$ be a $\ell \times \ell$ non-recurrent circulant matrix with entries from $\{-1, 1\}$. Then rank$(\mathbf{C}) \geqslant \min\{\tau(\ell, p), \tau(\ell, q)\}$.*

Note that if $\mathbf{u} \in \{-1, 1\}^\ell$ and $\langle \mathbf{1} | \mathbf{u} \rangle = -1$, then $\mathbf{C}$ is non-recurrent. This is because there is one more -1 than 1's, so that there can be no two identical rows of $\mathbf{C}$. Therefore, if $(\mathbf{u}, \mathbf{v})$ is an LP, then necessarily the circulant matrices associated with $\mathbf{u}, \mathbf{v}$ are non-recurrent.

If $\beta \geqslant 2$, then the following lemma implies that the rank is at least $\tau(\ell, q)$.

Lemma 3.4.12. *Let $\ell = pq^\beta$ be a positive integer for distinct odd primes p, q and $\beta \geqslant 2$. Then $\tau(\ell, q) < \tau(\ell, p)$.*

Proof. Note that $mn \geqslant m + n$ if and only if $(m-1)(n-1) \geqslant 1$. Now

$$\tau(n, q) = 1 + \epsilon(2)\epsilon(\beta)\phi(q) + \phi(q^\beta) + \phi(qp) = 1 + \phi(q) + \phi(q^\beta) + \phi(qp)$$

and

$$\tau(n,p) = 1 + \phi(p) + \phi(pq^{\beta}).$$

Then

$$\begin{aligned}\tau(\ell,p) - \tau(\ell,q) &= \phi(q)(q^{\beta-1}(\phi(p)-1) - (\phi(p)+1)) + \phi(p) \\ &= \phi(q)(q^{\beta-1}(p-2) - p) + \phi(p).\end{aligned}$$

We consider two cases where $p = 3$ and $p \geqslant 5$. If $p = 3$, then

$$\tau(\ell,p) - \tau(\ell,q) = \phi(q)(q^{\beta-1} - 3) + \phi(3) \geqslant \phi(q)(5^{\beta-1} - 3) + \phi(3) \geqslant 0.$$

If $p \geqslant 5$, then since $p - 2 \geqslant 1$,

$$q^{\beta-1}(p-2) - p \geqslant q^{\beta-1} + p - 2 - p = q^{\beta-1} - 2 \geqslant 3^{\beta-1} - 2 > 0$$

implying

$$\tau(\ell,p) - \tau(\ell,q) = \phi(q)(q^{\beta-1}(p-2) - p)) + \phi(p) > 0. \qquad \square$$

Now the following corollary follows from Lemma 3.4.12 and Theorem 3.4.10

Corollary 3.4.13. *Let $\ell = pq^{\beta}$, $\beta \geqslant 2$. Then the rank of a $\ell \times \ell$ circulant matrix is at least $\tau(\ell,q) = \phi(pq) + \phi(q) + \phi(q^{\beta})$.*

The ILP

$$\begin{aligned}
\text{minimize} \quad & \phi(p) + \sum_{i\in[\beta]} \phi(q^i) + \sum_{i\in[\beta]} x_i\phi(pq^i) \\
\text{subject to} \quad & \phi(p) + \sum_{i\in[\beta]} \phi(q^i) + \sum_{i\in[\beta]} x_i\phi(pq^i) \geqslant \phi(pq) + \phi(q) + \phi(q^{\beta}) \\
& x_i \in \{0,1\}, i \in [\beta]
\end{aligned} \tag{3.4.1}$$

aims to improve the lower bound $\tau(\ell, q)$.

3.5 Discussion

In this chapter we determined the dimension of the convex hull of feasible points to the Legendre pair problem when $\ell = p^n$ and $\ell = pq$ for p, q distinct odd primes and $n \in \mathbb{Z}_{\geqslant 1}$. Future research will be the generalization of finding the possible values this dimension for general odd ℓ. We will explore this generalization with techniques from Section 3.4.

IV. Concluding Remarks

In this research we studied the classification of OAs and the dimension of the convex hull of feasible points to the LP problem. The contribution associated with the classification of orthogonal arrays refines the work of Stufken and Tang [26] by analytically classifying of all non-OD-equivalent $\mathrm{OA}(\lambda 2^t, t+2, 2, t)$ when t is even. The classification results obtained are significantly simpler than by classification up to isomorphism as in Stufken and Tang [26]. The contribution associated with the existence of LPs determines the dimension of the convex hull of feasible points to the Legendre pair problem when $\ell = p^n$ and $\ell = pq$ for p, q distinct odd primes and $n \in \mathbb{Z}_{\geqslant 1}$ providing a better understanding of the convex hull of feasible points.

4.1 Future work

OD-equivalence operations allows for simpler classification of $\mathrm{OA}(\lambda 2^t, t+2, 2, t)$ when t is even compared to the classification carried out by isomorphism operations alone. Future research will involve classifying $\mathrm{OA}(\lambda 2^t, t+3, 2, t)$ up to OD-equivalence for even t. OD-equivalence operations contain isomorphism operations because of this we expect classifying $\mathrm{OA}(\lambda 2^t, t+3, 2, t)$ up to OD-equivalence for even t to be possible.

The determination of the dimension of the convex hull of feasible points to the LP problem when $\ell = p^n$ and $\ell = pq$ has been exhausted. The natural problem is the generalization to any odd ℓ. Possible modes of generalization are employing techniques of Ingleton [36] and bounding the dimension from below with the intent of obtaining equality. Another avenue is utilizing the discrete Fourier transform as in Fletcher *et al.* [18] and examining other inequalities or equalities that must hold in the new coordinate system if two vectors are to be Legendre pairs.

Appendix A. Chapter II Matlab Code

For any even-strength d, the following Matlab scripts: S1Script, S2Script, S3Script, and S4Script generate the complete set of solutions S1, S2, S3, and S4, respectively, corresponding to Lemmas 8, 9, 10, and 11, respectively, of Stufken and Tang [26]. The variables $y_1, y_2, y_3, y_4, \ldots, y_{m+2}$ correspond to the variables $k, u_{m+1}, u_m, u_{m-1}, \ldots, u_1$. Note that S1 and S2 in this dissertation differ from that as in Stufken and Tang [26]. The code is written in Matlab R2021a. To generate the complete solution sets as given in Theorems 2.3.5 and 2.3.6, implement scripts S1Script and S3Script.

The scripts operate as follows:

1. Specify a strength d at line 1.

2. The output of the script is a function with argument the index λ.

3. The function, with specified argument, will generate the complete set of solutions $(u_1, \ldots, u_{m+1}, k)$.

A.1 S1Script

```
1  d=2;
2  m=d+2;
3
4  str="[";
5  for j=m+2:-1:2
6      str=str+"y"+num2str(j)+",";
7  end
8  strVec=str+"y"+num2str(1)+"]";
9
10 strY=["Y1=[]"];
11 for j=2:m+2
12
13     str="Y" + num2str(j)+"={}";
14
15 strY=[strY str];
16 end
17 strY;
18
19 strYC=["Y1", "Y2{j1}"];
20 for j=3:m+2
21
```

```
    str="Y" + num2str(j)+"{j1,j2";
for i=3:j-1
    str=str+",j"+num2str(i);
end
str=str+"}";
strYC=[strYC str];
end
strYC;

strLoop=[];
for j=1:(m+2)

    str="for j"+num2str(j)+"=1:size("+strYC(j)+",2)";
    strLoop=[strLoop, str];

end
strLoop;

strVar=[];
for j=1:m+2
    str="y"+num2str(j)+"="+strYC(j)+"(j"+num2str(j)+")";
    strVar=[strVar, str];
end
strVar;

ub=["(lambda-d-1)/4", "(lambda-4*y1)/(m-1)", "-abs(y2)"];

for j=4:m+1
    str="y"+num2str(j-1);
    ub=[ub, str];

end
ub;

lb=["0", "-(lambda-4*y1)/(m+1)", "-(lambda-4*y1+y2)/m"];

for j=4:m+1
    str="-(lambda-4*y1+y2";
    for i=3:(j-1)
    str=str+"+y"+num2str(i);
    end
    str=str+")/("+ (m+3-j)+")";
    lb=[lb,str];
end

for j=4:m+2
    str="-(lambda-4*y1+y2";
    for i=3:m+1
        str=str+"+y"+num2str(i);
    end
    str=str+")";
end
lb=[lb,str];

%fileName="lambda"+num2str(lambda)+"k"+num2str(m)+"t"+num2str(d)+"S1.m";
fileName="k"+num2str(m)+"t"+num2str(d)+"S1.m";
fileID=fopen(fileName,'w');
```

```

fprintf(fileID,"function S=k"+num2str(m)+"t"+num2str(d)+"S1(lambda)\n");
fprintf(fileID, "if mod(lambda,2)==0\nerror('lambda must be odd')\nend\n");
fprintf(fileID,"d="+d+";\n m=d+2;\n");



    fprintf(fileID, strY(1)+ ";\n" );

    fprintf(fileID,"  lb="+lb(1)+";\n"+"  ub="+ub(1)+";\n");

    fprintf(fileID,strYC(1)+"=[];\nn=ceil(lb);\n while n<=ub\n"+strYC(1)+"=["+strYC(1)+",n];\nn=n+1;\nend\n");
    fprintf(fileID,"clearvars n lb ub;\n");

for j=2:m+1
    fprintf(fileID, strY(j)+ ";\n" );

    for i=1:j-1
        fprintf(fileID,strLoop(i)+"\n");
    end

    for i=1:j-1
        fprintf(fileID,"    "+strVar(i)+";\n");
    end
    fprintf(fileID,"  lb="+lb(j)+";\n"+"  ub="+ub(j)+";\n");

    fprintf(fileID,strYC(j)+"=[];\n n=ceil(lb);\nwhile n<=ub\nif mod(n,2)==1\n"+strYC(j)+"=["+strYC(j)+",n];\nn=n+1;\nelse\nn=n+1;\nend\nend\n");

    for i=1:j-1
        fprintf(fileID,"end\n");
    end
    fprintf(fileID,"clearvars n lb ub;\n");
end


fprintf(fileID,strY(m+2)+";\n");

for j=1:m+1
    fprintf(fileID,strLoop(j)+"\n");
end

for j=1:m+1
     fprintf(fileID,strVar(j)+";\n");
end

fprintf(fileID,strYC(m+2)+"="+lb(m+2)+";\n");

for j=1:m+1
    fprintf(fileID,"end\n");
end

fprintf(fileID,"S=[];\n");

```

```
for j=1:m+2
    fprintf(fileID,strLoop(j)+"\n");
end
for j=1:m+2
     fprintf(fileID,strVar(j)+";\n");
end

fprintf(fileID,"S=[S;"+strVec+"];\n");

for j=1:m+2
    fprintf(fileID,"end\n");
end

fprintf(fileID,"end");
fclose(fileID);
```

A.2 S2Script

```
d=2;
m=d+2;

str="[";
for j=m+2:-1:2
    str=str+"y"+num2str(j)+",";
end
strVec=str+"y"+num2str(1)+"]";

per=[[1 3 2], 4:m+2];

strY=["Y1=[]"];
for j=2:m+2

    str="Y" + num2str(j)+"={}";

strY=[strY str];
end
strY=strY(per)


strYC=["Y1", "Y3{j1}", "Y2{j1,j2}"];
for j=4:m+2

    str="Y" + num2str(j)+"{j1,j2,j3";
for i=4:j-1
    str=str+",j"+num2str(i);
end
str=str+"}";
strYC=[strYC str];
end
strYC


strVar=["y1=Y1(j1)", "y3=Y3{j1}(j2)", "y2=Y2{j1,j2}(j3)"];
for j=4:m+2
    str="y"+num2str(j)+"="+strYC(j)+"(j"+num2str(j)+")";
    strVar=[strVar, str];
```

```
end
strVar

strLoop=[];
for j=1:(m+2)

    str="for j"+num2str(j)+"=1:size("+strYC(j)+",2)";
    strLoop=[strLoop, str];

end
strLoop

ub=["(lambda-d-3)/4", "(lambda-4*y1-2)/(m-1)", "-abs(y3)-2", "-abs(y3)"];

for j=5:m+1
    str="y"+num2str(j-1);
    ub=[ub, str];

end
ub

lb=["0", "-(lambda-4*y1-2)/(m+1)", "(m-1)*abs(y3)-y3-(lambda-4*y1)", "-(lambda-4*y1+y2+y3)/(m-1)"];

for j=5:m+1
    str="-(lambda-4*y1+y2+y3";
    for i=4:(j-1)
    str=str+"+y"+num2str(i);
    end
    str=str+")/("+ (m+3-j)+")";
    lb=[lb,str];
end

for j=5:m+2
    str="-(lambda-4*y1+y2+y3";
    for i=4:m+1
        str=str+"+y"+num2str(i);
    end
    str=str+")";
end
lb=[lb,str]

fileName="k"+num2str(m)+"t"+num2str(d)+"S2.m";
fileID=fopen(fileName,'w');

fprintf(fileID,"function S=k"+num2str(m)+"t"+num2str(d)+"S2(lambda)\n");
fprintf(fileID, "if mod(lambda,2)==0\nerror('lambda must be odd')\nend\n");

fprintf(fileID,"d="+d+";\n m=d+2;\n");



    fprintf(fileID, strY(1)+ ";\n" );

    fprintf(fileID,"  lb="+lb(1)+";\n"+"  ub="+ub(1)+";\n");
```

```

    fprintf(fileID,strYC(1)+"=[];\nn=ceil(lb);\n while n<=ub\n"+strYC(1)+"=["+strYC(1)+",n];\nn=n+1;\nend\nclearvars n lb ub;\n");


for j=2:m+1
    fprintf(fileID, strY(j)+ ";\n" );

    for i=1:j-1
        fprintf(fileID,strLoop(i)+"\n");
    end

    for i=1:j-1
        fprintf(fileID,"    "+strVar(i)+";\n");
    end
    fprintf(fileID,"  lb="+lb(j)+";\n"+"  ub="+ub(j)+";\n");

    fprintf(fileID,strYC(j)+"=[];\n n=ceil(lb);\nwhile n<=ub\nif mod(n,2)==1\n"+strYC(j)+"=["+strYC(j)+",n];\nn=n+1;\nelse\nn=n+1;\nend\nend\n");

    for i=1:j-1
        fprintf(fileID,"end\n");
    end
    fprintf(fileID,"clearvars n lb ub;\n");
end


fprintf(fileID,strY(m+2)+";\n");

for j=1:m+1
    fprintf(fileID,strLoop(j)+"\n");
end

for j=1:m+1
     fprintf(fileID,strVar(j)+";\n");
end

fprintf(fileID,strYC(m+2)+"="+lb(m+2)+";\n");

for j=1:m+1
    fprintf(fileID,"end\n");
end

fprintf(fileID,"S=[];\n");

for j=1:m+2
    fprintf(fileID,strLoop(j)+"\n");
end
for j=1:m+2
     fprintf(fileID,strVar(j)+";\n");
end

fprintf(fileID,"S=[S;"+strVec+"];\n");

for j=1:m+2
    fprintf(fileID,"end\n");
```

```
end

fprintf(fileID,"end");

fclose(fileID);
```

A.3 S3Script

```
d=2;
m=d+2;

str="[";
for j=m+2:-1:2
    str=str+"y"+num2str(j)+",";
end
strVec=str+"y"+num2str(1)+"]";

strY=["Y1=[]"];
for j=2:m+2

    str="Y" + num2str(j)+"={}";

strY=[strY str];
end
strY

strYC=["Y1", "Y2{j1}"];
for j=3:m+2

    str="Y" + num2str(j)+"{j1,j2";
for i=3:j-1
    str=str+",j"+num2str(i);
end
str=str+"}";
strYC=[strYC str];
end
strYC

strLoop=[];
for j=1:(m+2)

    str="for j"+num2str(j)+"=1:size("+strYC(j)+",2)";
    strLoop=[strLoop, str];

end
strLoop

strVar=[];
for j=1:m+2
    str="y"+num2str(j)+"="+strYC(j)+"(j"+num2str(j)+")";
    strVar=[strVar, str];
end
strVar

ub=["lambdaE/2", "(lambdaE-2*y1)/(m-1)", "-abs(y2)"];

```

```
for j=4:m+1
    str="y"+num2str(j-1);
    ub=[ub, str];

end
ub;

lb=["0", "-(lambdaE-2*y1)/(m+1)", "-(lambdaE-2*y1+y2)/m"];

for j=4:m+1
    str="-(lambdaE-2*y1+y2";
    for i=3:(j-1)
    str=str+"+y"+num2str(i);
    end
    str=str+")/("+ (m+3-j)+")";
    lb=[lb,str];
end

for j=4:m+2
    str="-(lambdaE-2*y1+y2";
    for i=3:m+1
        str=str+"+y"+num2str(i);
    end
    str=str+")";
end
lb=[lb,str];

fileName="k"+num2str(m)+"t"+num2str(d)+"S3.m";
fileID=fopen(fileName,'w');

fprintf(fileID,"function S=k"+num2str(m)+"t"+num2str(d)+"S3(lambda)\n");
fprintf(fileID, "if mod(lambda,2)==1\nerror('lambda must be even')\nend\n");
fprintf(fileID,"lambdaE=lambda/2;\nd="+d+";\n m=d+2;\n");

for j=1:m+1
    fprintf(fileID, strY(j)+ ";\n" );
    for i=1:j-1
        fprintf(fileID,strLoop(i)+"\n");
    end
    for i=1:j-1
        fprintf(fileID,"    "+strVar(i)+";\n");
    end
    fprintf(fileID,"  lb="+lb(j)+";\n"+"  ub="+ub(j)+";\n");

    fprintf(fileID,strYC(j)+"=[];\n n=ceil(lb);\n while n<=ub\n"+strYC(j)+"=["+strYC(j)+",n];\nn=n+1;\nend\n");
    for i=1:j-1
        fprintf(fileID,"end\n");
    end
    fprintf(fileID,"clearvars n lb ub;\n");
end

fprintf(fileID,strY(m+2)+";\n");

for j=1:m+1
    fprintf(fileID,strLoop(j)+"\n");
```

```
end

for j=1:m+1
     fprintf(fileID,strVar(j)+";\n");
end

fprintf(fileID,strYC(m+2)+"="+lb(m+2)+";\n");

for j=1:m+1
    fprintf(fileID,"end\n");
end

fprintf(fileID,"S=[];\n");

for j=1:m+2
    fprintf(fileID,strLoop(j)+"\n");
end
for j=1:m+2
     fprintf(fileID,strVar(j)+";\n");
end

fprintf(fileID,"S=[S;"+strVec+"];\n");

for j=1:m+2
    fprintf(fileID,"end\n");
end

fprintf(fileID,"end");
fclose(fileID);
```

A.4 S4Script

```
d=2;
m=d+2;

str="[";
for j=m+2:-1:2
    str=str+"y"+num2str(j)+",";
end
strVec=str+"y"+num2str(1)+"]";

per=[[1 3 2], 4:m+2];

strY=["Y1=[]"];
for j=2:m+2

    str="Y" + num2str(j)+"={}";

strY=[strY str];
end
strY=strY(per);


strYC=["Y1", "Y3{j1}", "Y2{j1,j2}"];
for j=4:m+2

```

```
    str="Y" + num2str(j)+"{j1,j2,j3";
for i=4:j-1
    str=str+",j"+num2str(i);
end
str=str+"}";
strYC=[strYC str];
end
strYC;


strVar=["y1=Y1(j1)", "y3=Y3{j1}(j2)", "y2=Y2{j1,j2}(j3)"];
for j=4:m+2
    str="y"+num2str(j)+"="+strYC(j)+"(j"+num2str(j)+")";
    strVar=[strVar, str];
end
strVar;

strLoop=[];
for j=1:(m+2)

    str="for j"+num2str(j)+"=1:size("+strYC(j)+",2)";
    strLoop=[strLoop, str];

end
strLoop;

ub=["(lambdaE-1)/2", "(lambdaE-2*y1-1)/(m-1)", "-abs(y3)-1", "-abs(y3)"];

for j=5:m+1
    str="y"+num2str(j-1);
    ub=[ub, str];

end
ub;

lb=["0", "-(lambdaE-2*y1-1)/(m+1)", "(m-1)*abs(y3)-y3-(lambdaE-2*y1)", "-(lambdaE-2*y1+y2+y3)/(m-1)"];

for j=5:m+1
    str="-(lambdaE-2*y1+y2+y3";
    for i=4:(j-1)
    str=str+"+y"+num2str(i);
    end
    str=str+")/("+ (m+3-j)+")";
    lb=[lb,str];
end

for j=5:m+2
    str="-(lambdaE-2*y1+y2+y3";
    for i=4:m+1
        str=str+"+y"+num2str(i);
    end
    str=str+")";
end
lb=[lb,str];

fileName="k"+num2str(m)+"t"+num2str(d)+"S4.m";
```

```
fileID=fopen(fileName,'w');

fprintf(fileID,"function S=k"+num2str(m)+"t"+num2str(d)+"S4(lambda)\n");
fprintf(fileID, "if mod(lambda,2)==1\nerror('lambda must be even')\nend\n");
fprintf(fileID,"lambdaE=lambda/2;\nd="+d+";\n m=d+2;\n");

fprintf(fileID, strY(1)+ ";\n" );

fprintf(fileID,"  lb="+lb(1)+";\n"+"  ub="+ub(1)+";\n");

fprintf(fileID,strYC(1)+"=[];\nn=ceil(lb);\n while n<=ub\n"+strYC(1)+"=["+strYC(1)+",n];\nn=n+1;\nend\nclearvars n lb ub;\n");


for j=2:m+1
    fprintf(fileID, strY(j)+ ";\n" );

    for i=1:j-1
        fprintf(fileID,strLoop(i)+"\n");
    end

    for i=1:j-1
        fprintf(fileID,"    "+strVar(i)+";\n");
    end
    fprintf(fileID,"  lb="+lb(j)+";\n"+"  ub="+ub(j)+";\n");

    fprintf(fileID,strYC(j)+"=[];\n n=ceil(lb);\nwhile n<=ub\n"+strYC(j)+"=["+strYC(j)+",n];\nn=n+1;\nend\n");

    for i=1:j-1
        fprintf(fileID,"end\n");
    end
    fprintf(fileID,"clearvars n lb ub;\n");
end


fprintf(fileID,strY(m+2)+";\n");

for j=1:m+1
    fprintf(fileID,strLoop(j)+"\n");
end

for j=1:m+1
     fprintf(fileID,strVar(j)+";\n");
end

fprintf(fileID,strYC(m+2)+"="+lb(m+2)+";\n");

for j=1:m+1
    fprintf(fileID,"end\n");
end

fprintf(fileID,"S=[];\n");

for j=1:m+2
```

```
    fprintf(fileID,strLoop(j)+"\n");
end
for j=1:m+2
     fprintf(fileID,strVar(j)+";\n");
end

fprintf(fileID,"S=[S;"+strVec+"];\n");

for j=1:m+2
    fprintf(fileID,"end\n");
end

fprintf(fileID,"end");
fclose(fileID);
```

A.5 OA generation and verification

```
%Specify number of factors k
k=4

%Initialize solution u=(u_1,u_2,u_3,u_4,u_5)

%Just an example of using S3Script to generate solutions
%(u_1,u_2,u_3,u_4,u_5,p)
lambda=4;
X=k4t2EvenLambdaS3(lambda)


%Here we choose the solution for Example 4 in Appendix B.
u=X(1,1:end-1);

%Create full factorial 2^k x k
F=ff2n(k);

%Write in Yates ordering
I=k:-1:1;
Yates=F(:,I);
Yates=-2*Yates+1

%Construct J-vector
L=ones(k,k)-eye(k);


x=k-1:-1:0;
y=2.^x;

li=L*y'+1;
li=[li; 2^k];




%Construct the J-vector
J=zeros(1,2^k);

J(1)=2^t*lambda;
```

```
%If lambda is odd
%J(li)=2^t*u;

%If lambda is even
J(li)=2^(t+1)*u;


H=hadamard(2^k);

%Construct the frequency vector
x=2^(-k)*H*J'
I=find(x)
size(I,1);


%Construct the orthogonal array
OA=[];
for i=1:size(I,1)
    s=I(i);
    for j=1:x(s)
    OA=[OA; Yates(s,:)];
    end
end
OA

%Verify OA is an orthogonal array of strength t

columns=1:k;

for j=0:2^k
C=nchoosek(columns,j);

    for i=1:size(C,1)
     l=C(i,:);
     A=OA(:,l);
     d=prod(A,2);
     sum(d);
     if sum(d)~=0
         l
         sum(d)
     end

    end
end
```

Appendix B. Chapter II Examples

Example 1. Consider the 4×2 arrays $\boldsymbol{X}, \boldsymbol{Y}$ and $\boldsymbol{Z}$

$$\underset{\boldsymbol{X}}{\begin{bmatrix} 1 & 1 \\ -1 & 1 \\ 1 & -1 \\ -1 & -1 \end{bmatrix}} \qquad \underset{\boldsymbol{Y}}{\begin{bmatrix} -1 & -1 \\ 1 & -1 \\ -1 & 1 \\ 1 & 1 \end{bmatrix}} \qquad \underset{\boldsymbol{Z}.}{\begin{bmatrix} 1 & -1 \\ 1 & 1 \\ -1 & -1 \\ -1 & 1 \end{bmatrix}}$$

Since $\boldsymbol{X}, \boldsymbol{Y}$, and $\boldsymbol{Z}$ are full factorials, they are OA$(4, 2, 2, 2)$s. Observe that $\boldsymbol{Y}$ is obtained by permuting levels in both columns of $\boldsymbol{X}$, while $\boldsymbol{Z}$ is obtained by permuting both columns of $\boldsymbol{X}$ and permuting levels within the the first column of $\boldsymbol{X}$.

Since

$$\{\text{rows of } \boldsymbol{X}\} = \{\text{rows of } \boldsymbol{Y}\} = \{\text{rows of } \boldsymbol{Z}\},$$

$\boldsymbol{X}, \boldsymbol{Y}$, and $\boldsymbol{Z}$ are isomorphic.

Example 2. Consider the following OA$(4, 2, 2, 2)$s $\boldsymbol{X}$ and $\boldsymbol{Y}$

$$\underset{\boldsymbol{X}}{\begin{bmatrix} 1 & 1 \\ -1 & 1 \\ 1 & -1 \\ -1 & -1 \end{bmatrix}} \qquad \underset{\boldsymbol{Y}.}{\begin{bmatrix} 1 & 1 \\ -1 & -1 \\ 1 & -1 \\ -1 & 1 \end{bmatrix}}$$

Note that $\boldsymbol{Y} = R_1(\boldsymbol{X})$. Since $\{\text{rows of } \boldsymbol{X}\} = \{\text{rows of } \boldsymbol{Y}\}$, $\boldsymbol{X}$ and $\boldsymbol{Y}$ are OD-equivalent.

Example 3. Consider the OA$(4, 2, 2, 2)$ $\boldsymbol{X}$

$$\begin{bmatrix} 1 & 1 \\ -1 & 1 \\ 1 & -1 \\ -1 & -1 \end{bmatrix}$$

$\boldsymbol{X}$.

Observe that $\forall \ell \subseteq [2] \ni 1 \leqslant |\ell| \leqslant 2,\ J_\ell = 0$,

$$\begin{aligned}
J_{\{1\}} &= 1 + (-1) + 1 + (-1) = 0, \\
J_{\{2\}} &= 1 + 1 + (-1) + (-1) = 0, \\
J_{\{1,2\}} &= (1)(1) + (-1)(1) + (1)(-1) + (-1)(-1) = 0.
\end{aligned}$$

Let us verify this by the equation $\mathbf{J} = \mathbf{H}^\top \mathbf{x}$. Since $\boldsymbol{X}$ is a full factorial, $\mathbf{x} = \mathbf{1}$. Then

$$\mathbf{J} = \mathbf{H}^\top \mathbf{x} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 4 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

in agreement with above.

The next example will construct an OA from the solution set as given in Theorem 2.3.6.

Example 4. Consider $\mathrm{OA}(4\lambda, 4, 2, 2)$ when $\lambda = 4$. The three non-OD-equivalent solutions are $(u_1, u_2, u_3, u_4, u_5, p) = (-1, -1, 0, 0, 0, 0), (-2, 0, 0, 0, 0, 0)$, and $(0, 0, 0, 0, 0, 1)$.

Let us construct the OA to the particular solution $(u_1, u_2, u_3, u_4, u_5, p) = (-1, -1, 0, 0, 0, 0)$. Since λ is even, the J-characteristics are $J_{\ell_j} = 2^{t+1} u_j = 8u_j,\ j = 1, \ldots, 5$. Then, the J-vector is

$$\mathbf{J} = [J_{\ell_1}, J_{\ell_2}, J_{\ell_3}, J_{\ell_4}, J_{\ell_5}] = [-8, -8, 0, 0, 0]$$

To determine the frequency vector $\mathbf{x}$, we need need the full J-vector of all 16 coordinates. As we are using Yates ordering, the full J-vector is

$$\mathbf{J} = [J_\varnothing, J_1, J_2, J_{12}, J_3, J_{13}, J_{23}, J_{123}, J_4, J_{14}, J_{24}, J_{124}, J_{34}, J_{134}, J_{234}, J_{1234}]^\top,$$

where J_{12} means $J_{\{1,2\}}$, similarly for the other coordinates. Since $\ell_1 = \{1,2,3\}, \ell_2 = \{1,2,4\}, \ell_3 = \{1,3,4\}, \ell_4 = \{2,3,4\}$ and $\ell_5 = \{1,2,3,4\}$,

$$\mathbf{J} = [16, 0, 0, 0, 0, 0, 0, -8, 0, 0, 0, -8, 0, 0, 0, 0]^\top.$$

By Lemma 2.2.1, $\mathbf{x} = 2^{-k}\mathbf{HJ} = 2^{-4}\mathbf{HJ}$, where

$$\mathbf{H} = \begin{bmatrix}
+&+&+&+&+&+&+&+&+&+&+&+&+&+&+&+\\
+&-&+&-&+&-&+&-&+&-&+&-&+&-&+&-\\
+&+&-&-&+&+&-&-&+&+&-&-&+&+&-&-\\
+&-&-&+&+&-&-&+&+&-&-&+&+&-&-&+\\
+&+&+&+&-&-&-&-&+&+&+&+&-&-&-&-\\
+&-&+&-&-&+&-&+&+&-&+&-&-&+&-&+\\
+&+&-&-&-&-&+&+&+&+&-&-&-&-&+&+\\
+&-&-&+&-&+&+&-&+&-&-&+&-&+&+&-\\
+&+&+&+&+&+&+&+&-&-&-&-&-&-&-&-\\
+&-&+&-&+&-&+&-&-&+&-&+&-&+&-&+\\
+&+&-&-&+&+&-&-&-&-&+&+&-&-&+&+\\
+&-&-&+&+&-&-&+&-&+&+&-&-&+&+&-\\
+&+&+&+&-&-&-&-&-&-&-&-&+&+&+&+\\
+&-&+&-&-&+&-&+&-&+&-&+&+&-&+&-\\
+&+&-&-&-&-&+&+&-&-&+&+&+&+&-&-\\
+&-&-&+&-&+&+&-&-&+&+&-&+&-&-&+
\end{bmatrix}$$

and $+, -$ mean $1, -1$, respectively. Then

$$\mathbf{x} = [0, 2, 2, 0, 1, 1, 1, 1, 1, 1, 1, 1, 2, 0, 0, 2]^\top.$$

The $2^4 \times 4$ full factorial array, with Yates ordering, $\mathbf{F}$, as given on page 7, is

$$\begin{bmatrix} + + + + \\ - + + + \\ + - + + \\ - - + + \\ + + - + \\ - + - + \\ + - - + \\ - - - + \\ + + + - \\ - + + - \\ + - + - \\ - - + - \\ + + - - \\ - + - - \\ + - - - \\ - - - - \end{bmatrix}.$$

Therefore, up to a row permutation, the OA given by $(u_1, u_2, u_3, u_4, u_5, p) = (-1, -1, 0, 0, 0, 0)$ is

$$\begin{bmatrix} - + + + \\ - + + + \\ + - + + \\ + - + + \\ + + - + \\ - + - + \\ + - - + \\ - - - + \\ + + + - \\ - + + - \\ + - + - \\ - - + - \\ + + - - \\ + + - - \\ - - - - \\ - - - - \end{bmatrix}.$$

Appendix C. Chapter III Examples

Example 1. The regular $\mathbb{C}$-representation of $\mathbb{Z}_3$ is $V = \mathrm{Span}_{\mathbb{C}}\{\mathbf{e}_i\}_{i\in\mathbb{Z}_\ell}$ with the homomorphism

$$R\colon \mathbb{Z}_3 \to \mathrm{GL}(V)$$

acting on the basis as $R(j)\mathbf{e}_i \mapsto \mathbf{e}_{i+j},\ i,j \in \mathbb{Z}_3$.

There are three irreducible $\mathbb{C}$-subrepresentations $(R_k, V_k), k \in \mathbb{Z}_3$ of V. For a fixed k, the homomorphism acts as follows

$$\begin{aligned} R_k(j)\colon V_k &\to V_k \\ \mathbf{v} &\mapsto \zeta^{jk}\mathbf{v} \end{aligned}$$

where $\zeta = e^{2\pi i/3}$. Each $V_k = \mathrm{Span}_{\mathbb{C}}\{\mathbf{v}_k\}$, where $\mathbf{v}_k = \sum_{j\in\mathbb{Z}_3} \overline{\zeta}^{jk}\mathbf{e}_j, k \in \mathbb{Z}_3$.

Example 2. Continuing Example 1, the group $\mathbb{Z}_3$ has three characters, χ_0, χ_1 and χ_2. By definition, $\chi_k(i) = \mathrm{Tr}(R_k(j)) = \mathrm{Tr}(\left[\zeta^{jk}\right]) = \zeta^{jk}, j,k \in \mathbb{Z}_3$. For a fixed $i \in \mathbb{Z}_3$, consider the sum $S_i = \chi_1(i) + \chi_2(i) = \zeta^i + \zeta^{2i}$. If $i = 0$, then $S_0 = 2$. For $i \neq 0$, since $1 + \zeta + \zeta^2 = 0$, $S_1 = S_2 = -1$. Note that the sum S_i is always rational for $i \in \mathbb{Z}_3$.

Example 3. Let $\ell = 3$. Since the only divisors of 3 are 1 and 3, by Theorem 3.2.6, the regular $\mathbb{Q}$-representation of $\mathbb{Z}_3$ is

$$\mathbb{Q}^{\mathbb{Z}_3} = \mathrm{Col}_{\mathbb{Q}}(\mathbf{P}_1) \ominus \mathrm{Col}_{\mathbb{Q}}(\mathbf{P}_3).$$

We calculate $\mathbf{P}_1$. By definition, $\mathbf{P}_1 = \frac{1}{3}\sum_{i\in\mathbb{Z}_3}\sum_{\chi\in\mathcal{O}_1}\overline{\chi(i)}\mathbf{M}_{R(i)}$. Since $(1,3) = (2,3) = 1$, $\mathcal{O}_1 = \{\chi_1, \chi_2\}$. Also, the matrix $\mathbf{M}_{R(i)}$ in the standard basis $\mathbf{e}_0, \mathbf{e}_1, \mathbf{e}_2$ is

$$\mathbf{M}_{R(0)} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \mathbf{M}_{R(1)} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \mathbf{M}_{R(2)} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}.$$

Therefore,

$$\begin{aligned}
\mathbf{P}_1 &= \frac{1}{3} \sum_{i \in \mathbb{Z}_3} \sum_{\chi \in \mathcal{O}_1} \overline{\chi(i)} \mathbf{M}_{R(i)} \\
&= \frac{1}{3} \sum_{i \in \mathbb{Z}_3} \left(\overline{\chi_1(i)} + \overline{\chi_2(i)} \right) \mathbf{M}_{R(i)} \\
&= \frac{1}{3} \left(\left(\overline{\chi_1(0)} + \overline{\chi_2(0)} \right) \mathbf{M}_{R(0)} + \left(\overline{\chi_1(1)} + \overline{\chi_2(1)} \right) \mathbf{M}_{R(1)} + \left(\overline{\chi_1(2)} + \overline{\chi_2(2)} \right) \mathbf{M}_{R(2)} \right) \\
&= \frac{1}{3} \left(2\mathbf{M}_{R(0)} - \mathbf{M}_{R(1)} - \mathbf{M}_{R(2)} \right) \\
&= \frac{1}{3} \begin{bmatrix} 2 & -1 & -1 \\ -1 & 2 & -1 \\ -1 & -1 & 2 \end{bmatrix}.
\end{aligned}$$

A similar calculation gives

$$\mathbf{P}_3 = \frac{1}{3} \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}.$$

Since $\dim_{\mathbb{Q}}(\mathrm{Col}_{\mathbb{Q}}(\mathbf{P}_1)) = \mathrm{Tr}(\mathbf{P}_1) = 2$, $\mathrm{Col}_{\mathbb{Q}}(\mathbf{P}_1)$ is a two-dimensional irreducible $\mathbb{Q}$-subrepresentation of $\mathbb{Q}^{\mathbb{Z}_3}$, similarly $\mathrm{Col}_{\mathbb{Q}}(\mathbf{P}_3)$ is a one-dimensional irreducible $\mathbb{Q}$-subrepresentation of $\mathbb{Q}^{\mathbb{Z}_3}$.

Bibliography

1. R. T. Johnson, G. T. Hutto, J. R. Simpson, and D. C. Montgomery, "Designed experiments for the defense community," *Quality Engineering*, vol. 24, no. 1, pp. 60–79, 2012.

2. G. Hutto and J. Higdon, "Survey of design of experiments (DOE) projects in developmental test CY07-08," *American Institute of Aeronautics and Astronautics 2009*, vol. 1706, 2009.

3. A. A. Tucker, G. T. Hutto, and C. H. Dagli, "Application of design of experiments to flight test: a case study," *Journal of Aircraft*, vol. 47, no. 2, pp. 458–463, 2008.

4. R. F. Gunst and R. L. Mason, "Fractional factorial design," *Wiley Interdisciplinary Reviews: Computational Statistics*, vol. 1, no. 2, pp. 234–244, 2009.

5. R. Mee, *A comprehensive guide to factorial two-level experimentation.* Springer New York, NY: Springer Science & Business Media, 2009.

6. A. Hedayat, N. Sloane, and J. Stufken, *Orthogonal Arrays: Theory and Applications.* New York, NY, USA: Springer-Verlag, 1999.

7. C. S. Cheng, "Some projection properties of orthogonal arrays," *Annals of Statistics*, vol. 23, no. 4, pp. 1223–1233, 1995.

8. R. L. Plackett and J. P. Burman, "The design of optimum multifactorial experiments," *Biometrika*, vol. 33, no. 4, pp. 305–325, 1946.

9. K. J. Horadam, "Hadamard matrices and their applications," in *Hadamard Matrices and Their Applications.* Princeton University press, 2012.

10. A. Hedayat and W. D. Wallis, "Hadamard matrices and their applications," *Annals of Statistics*, pp. 1184–1238, 1978.

11. J. Seberry, B. J. Wysocki, and T. A. Wysocki, "On some applications of Hadamard matrices," *Metrika*, vol. 62, no. 2, pp. 221–239, 2005.

12. R. C. Bose and K. A. Bush, "Orthogonal arrays of strength two and three," *Annals of Mathematical Statistics*, vol. 23, no. 4, pp. 508–524, 1952.

13. A. Hedayat, J. Stufken, and G. Su, "On difference schemes and orthogonal arrays of strength t," *Journal of Statistical Planning and Inference*, vol. 56, no. 2, pp. 307–324, 1996.

14. D. Bulutoglu and F. Margot, "Classification of orthogonal arrays by integer programming," *Journal of Statistical Planning and Inference*, vol. 138, no. 3, pp. 654–666, 2008.

15. J. J. Sylvester, "Thoughts on inverse orthogonal matrices, simultaneous sign successions, and tessellated pavements in two or more colours, with applications to Newton's rule, ornamental tile-work, and the theory of numbers," *London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science*, vol. 34, no. 232, pp. 461–475, 1867.

16. R. E. Paley, "On orthogonal matrices," *Journal of Mathematics and Physics*, vol. 12, no. 1-4, pp. 311–320, 1933.

17. K. Arasu, D. Bulutoglu, and J. Hollon, "Legendre G-array pairs and the theoretical unification of several G-array families," *Journal of Combinatorial Designs*, vol. 28, no. 11, pp. 814–841, 2020.

18. R. J. Fletcher, M. Gysin, and J. Seberry, "Application of the discrete Fourier transform to the search for generalised Legendre pairs and Hadamard matrices," *Australasian Journal of Combinatorics*, vol. 23, pp. 75–86, 2001.

19. J. S. Turner, I. S. Kotsireas, D. A. Bulutoglu, and A. J. Geyer, "A Legendre pair of length 77 using complementary binary matrices with fixed marginals," *Designs, Codes and Cryptography*, vol. 89, no. 6, pp. 1321–1333, 2021.

20. D. Bulutoglu, I. Kotsireas, C. Koutschan, and J. Turner, "Legendre pairs of lengths $\ell \equiv 0 \pmod 5$," *arXiv e-prints*, 2021.

21. I. Kotsireas and C. Koutschan, "Legendre pairs of lengths $\ell \equiv 0 \pmod 3$," *Journal of Combinatorial Designs*, vol. 29, no. 12, pp. 870–887, 2021.

22. D. A. Bulutoglu and K. J. Ryan, "Integer programming for classifying orthogonal arrays," *Australasian Journal of Combinatorics*, vol. 70, no. 3, pp. 362–385, 2018.

23. D. S. Krotov, "On the $\mathrm{OA}(1536, 13, 2, 7)$ and related orthogonal arrays," *Discrete Mathematics*, vol. 343, no. 2, p. 111659, 2020.

24. D. S. Krotov and K. V. Vorob'ev, "On unbalanced boolean functions with best correlation immunity," *Electronic Journal of Combinatorics*, pp. P1–45, 2020.

25. S. Yamamoto, S. Kuriki, and M. Sato, "On existence and construction of some 2-symbol orthogonal arrays," *TRU Mathematics*, vol. 20, no. 2, pp. 317–331, 1984.

26. J. Stufken and B. Tang, "Complete enumeration of two-level orthogonal arrays of strength d with $d + 2$ constraints," *Annals of Statistics*, vol. 35, no. 2, pp. 793–814, 2007.

27. A. J. Geyer, D. A. Bulutoglu, and K. J. Ryan, “Finding the symmetry group of an LP with equality constraints and its application to classifying orthogonal arrays,” *Discrete Optimization*, vol. 32, pp. 93–119, 2019.

28. J. Seberry and M. Mitrouli, “Some remarks on Hadamard matrices,” *Cryptography and Communications*, vol. 2, no. 2, pp. 293–306, 2010.

29. D. A. Bulutoglu and D. M. Kaziska, “Erratum to “improved wlp and gwp lower bounds based on exact integer programming”[j. statist. plann. inference 140 (2010) 1154–1161],” *Journal of Statistical Planning and Inference*, vol. 7, no. 141, pp. 2500–2501, 2011.

30. J. J. Rotman, *Advanced Modern Algebra.* Boston, MI, USA: American Mathematical Society, 2010, vol. 114.

31. D. A. Bulutoglu, “Finding the dimension of a non-empty orthogonal array polytope,” *Discrete Optimization*, vol. 45, p. 100727, 2022.

32. J. P. Serre, *Linear representations of finite groups.* New York, NY, USA: Springer-Verlag, 1977, vol. 42.

33. T. Lam and K. Leung, “On vanishing sums of roots of unity,” *Journal of Algebra*, vol. 224, no. 1, pp. 91–109, 2000.

34. G. Sivek, “On vanishing sums of distinct roots of unity,” *Integers*, vol. 10, pp. 365–368, 2010.

35. T. M. Apostol, *Introduction to analytic number theory.* Springer Science & Business Media, 1998.

36. A. Ingleton, “The rank of circulant matrices,” *Journal of the London Mathematical Society*, vol. 1, no. 4, pp. 445–460, 1956.

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704–0188

1. REPORT DATE *(DD–MM–YYYY)*
22–08–2022

2. REPORT TYPE
Dissertation

3. DATES COVERED *(From — To)*
Sept 2019 — Sept 2022

4. TITLE AND SUBTITLE
Orthogonal Arrays and Legendre Pairs

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

6. AUTHOR(S)
Kilpatrick, Kristopher N., Capt, USAF

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER
AFIT-ENC-DS-22-S-004

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Department of Mathematics and Statistics
2950 Hobson Way
WPAFB OH 45433-7765

10. SPONSOR/MONITOR'S ACRONYM(S)
AFIT/ENC

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
DISTRIBUTION STATEMENT A:
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Well-designed experiments greatly improve test and evaluation. Efficient experiments reduce the cost and time of running tests while improving the quality of the information obtained. Orthogonal Arrays (OAs) and Hadamard matrices are used as designed experiments to glean as much information as possible about a process with limited resources. However, constructing OAs and Hadamard matrices in general is a very difficult problem. Finding Legendre pairs (LPs) results in the construction of Hadamard matrices. This research studies the classification problem of OAs and the existence problem of LPs. In doing so, it makes two contributions to the discipline. First, it improves upon previous classification results of 2-symbol OAs of even-strength t and $t+2$ columns. Second, it presents previously unknown impossible values for the dimension of the convex hull of all feasible points to the LP problem improving our understanding of its feasible set.

15. SUBJECT TERMS
Orthogonal Arrays, Hadamard Matrices, Legendre Pair, OD-Equivalence, Representation Theory

16. SECURITY CLASSIFICATION OF: a. REPORT	b. ABSTRACT	c. THIS PAGE	17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
U	U	U	UU	69	Dr. Dursun A. Bulutoglu, AFIT/ENC

19b. TELEPHONE NUMBER *(include area code)*
(937)255-3636 x4704; dursun.bulutoglu@us.af.mil

Standard Form 298 (Rev. 8–98)
Prescribed by ANSI Std. Z39.18