Legendre pairs of lengths $\ell \equiv 0 \pmod 5$

Ilias Kotsireas* Christoph Koutschan† Dursun Bulutoglu‡
David Arquette‡ Jonathan Turner‡ Kenneth Ryan§

April 8, 2024

Abstract

By assuming a type of balance for length $\ell = 87$ and non-trivial subgroups of multiplier groups of Legendre pairs (LPs) for length $\ell = 85$, we find LPs of these lengths. We then study the power spectral density (PSD) values of m compressions of LPs of length $5m$. We also formulate a conjecture for LPs of lengths $\ell \equiv 0 \pmod 5$ and demonstrate how it can be used to decrease the search space and storage requirements for finding such LPs. The newly found LPs decrease the number of integers in the range $\leqslant 200$ for which the existence question of LPs remains unsolved from 12 to 10.

Keywords: compressed vector; discrete Fourier transform; Hadamard matrix; periodic autocorrelation function; power spectral density; multiplier group

MSC 2010: 05B10; 05B20; 15B34

1 Introduction

The *periodic autocorrelation function* (PAF) of a (row) vector $\mathbf{a} \in \mathbb{C}^\ell$ indexed by $\mathbb{Z}_\ell$ is defined as $\mathrm{PAF}_{\mathbf{a}}(j) = \sum_{i=0}^{\ell-1} a_i \overline{a}_{i-j}$, where $\overline{a}_i$ is the complex conjugate of a_i. By using the PAF, we define the concept of a Legendre pair (LP) studied in [4].

*CARGO Lab, Wilfrid Laurier University, Waterloo, Ontario N2L 3C5, Canada
†Supported by the Austrian Science Fund (FWF): F5011-N15. Johann Radon Institute for Computational and Applied Mathematics (RICAM) Austrian Academy of Sciences, Linz A-4040, Austria
‡Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio 45433, USA
§West Virginia University Morgantown, West Virginia 26506, USA

Definition 1. *Let* $\mathbf{a}$ *and* $\mathbf{b}$ *be* $\{-1, 1\}$ *row vectors indexed by* $\mathbb{Z}_\ell$*. Then,* $(\mathbf{a}, \mathbf{b})$ *is an LP if*

$$\mathrm{PAF}_{\mathbf{a}}(j) + \mathrm{PAF}_{\mathbf{b}}(j) = -2 \quad \forall j \in \mathbb{Z}_\ell - \{0\}, \tag{1}$$
$$\sum_{i=0}^{\ell-1} a_i = \sum_{i=0}^{\ell-1} b_i.$$

An LP $(\mathbf{a}, \mathbf{b})$ must satisfy $\sum_{i=0}^{\ell-1} a_i = \sum_{i=0}^{\ell-1} b_i = 1$ or $\sum_{i=0}^{\ell-1} a_i = \sum_{i=0}^{\ell-1} b_i = -1$; see [1].

A *circulant shift* of a vector $\mathbf{a} \in \mathbb{C}^\ell$ by $j \in \mathbb{Z}_\ell$, denoted $c_j(\mathbf{a})$, is a transformation such that $(c_j(\mathbf{a}))_i = a_{i-j}$ for each $i \in \mathbb{Z}_\ell$. Let $\mathbf{C_a}$ be the *circulant matrix* obtained from a row vector, $\mathbf{a}$, where the $(j + 1)$th row of $\mathbf{C_a}$ is $c_j(\mathbf{a})$.

Let $\mathbf{a}, \mathbf{b} \in \{-1, 1\}^\ell$ be an LP such that $\sum_{i=0}^{\ell-1} a_i = \sum_{i=0}^{\ell-1} b_i = 1$, and $\mathbf{1}$ be the length ℓ row vector of all 1s. For a complex number $z = x + iy$, let $\bar{z} = x - iy$ be the complex conjugate of z. Then

$$\mathbf{H} = \begin{bmatrix} -1 & -1 & \mathbf{1} & \mathbf{1} \\ -1 & 1 & \mathbf{1} & -\mathbf{1} \\ \mathbf{1}^\top & \mathbf{1}^\top & \mathbf{C_b} & \mathbf{C_a} \\ \mathbf{1}^\top & -\mathbf{1}^\top & \overline{\mathbf{C_a}}^\top & -\overline{\mathbf{C_b}}^\top \end{bmatrix} \tag{2}$$

is a $(2\ell + 2) \times (2\ell + 2)$ *Hadamard matrix*, a matrix with entries in $\{\pm 1\}$ with orthogonal columns, where for a matrix $\boldsymbol{A} = (a_{ij})$, $\overline{\boldsymbol{A}} = (\overline{a_{ij}})$, which will soon become relevant. It is well known that a Hadamard matrix of order n does not exist if n is not divisible by 4 and $n > 2$. Then $4 \mid (2\ell + 2)$, implying that ℓ must be odd for an LP of length ℓ to exist. It is conjectured that an LP exists for all odd ℓ or equivalently there is an $n \times n$ Hadamard matrix constructed via LPs whenever n is a multiple of 4 [1].

An $n \times n$ matrix with entries from $\{-1, 1, -i, i\}$ with orthogonal columns with respect to the complex dot product is called a *quaternary (complex) Hadamard matrix.* The order of a quaternary Hadamard matrix must be even [6]. For even ℓ, if $\mathbf{a}, \mathbf{b} \in \{-1, 1, -i, i\}^\ell$ satisfy equation (1) in Definition 1 and equations

$$\sum_{i=0}^{\ell-1} a_i = 1 + i, \quad \sum_{i=0}^{\ell-1} b_i = 0,$$

then $\mathbf{H}$ in equation (2) with the upper left 2×2 submatrix replaced by

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

is a quaternary Hadamard matrix, and such $(\mathbf{a}, \mathbf{b})$ is called a *quaternary Legendre pair* [6]. It is conjectued that a quaternary LP exists for every even ℓ [6]. Since if a quaternary

Hadamard matrix of order n exists, then a Hadamard matrix of order $2n$ must also exist [6], proving this conjecture would also prove the *Hadamard conjecture*, i.e., a Hadamard matrix of order n exists for every n divisible by 4.

For two groups N and H, and an action of H on N, let $N \rtimes H$ be the semidirect product of N and H as defined in Rotman [8]. Let $\mathbb{Z}_\ell^\times$ be the group of units in $\mathbb{Z}_\ell$. Let $(j,k)i = ki + j$ for $(j,k) \in \mathbb{Z}_\ell \rtimes \mathbb{Z}_\ell^\times$ and $i \in \mathbb{Z}_\ell$. Then the group $\mathbb{Z}_\ell \rtimes \mathbb{Z}_\ell^\times$ acts on each vector $\mathbf{a}$ in $\mathbb{C}^\ell$ via $(j,k)a_i = a_{(j,k)^{-1}i}$. The action of $(0,k) := d_k$ for $k \in \mathbb{Z}_\ell^\times$ on $\mathbf{a}$ is called a *decimation*. Decimations and cyclic shifts do not commute. In fact, $d_r c_i (d_r)^{-1} = d_r c_i d_{r^{-1}} = c_{ir}$. Equivalently,

$$c_i d_r = d_r c_{ir^{-1}} \text{ or } d_r c_k = c_{rk} d_r.$$

The action of the group $\mathbb{Z}_\ell \rtimes \mathbb{Z}_\ell^\times$ on $\mathbf{a} \in \mathbb{C}^\ell$ is used to define an action of $(\mathbb{Z}_\ell \times \mathbb{Z}_\ell) \rtimes \mathbb{Z}_\ell^\times$ on LPs (quaternary LPs) $(\mathbf{a}, \mathbf{b})$ by $((j_1, j_2), k)(\mathbf{a}, \mathbf{b}) = ((j_1, k)\mathbf{a}, (j_2, k)\mathbf{b})$, for $(j_1, k) \in \mathbb{Z}_\ell \rtimes \mathbb{Z}_\ell^\times$ and $(j_2, k) \in \mathbb{Z}_\ell \rtimes \mathbb{Z}_\ell^\times$, see [1, 6]. Two pairs of $\{-1, 1\}$ or $\{0, 1\}$ vectors $(\mathbf{a}, \mathbf{b}), (\mathbf{a}', \mathbf{b}')$ are *equivalent* if $(\mathbf{a}, \mathbf{b})$ is in the same orbit as $(\mathbf{a}', \mathbf{b}')$ or $(\mathbf{b}', \mathbf{a}')$ under the action of $(\mathbb{Z}_\ell \times \mathbb{Z}_\ell) \rtimes \mathbb{Z}_\ell^\times$. Two pairs of $\{-1, 1, -i, i\}$ vectors $(\mathbf{a}, \mathbf{b}), (\mathbf{a}', \mathbf{b}')$ are *equivalent* if $(\mathbf{a}, \mathbf{b})$ is in the same orbit as $(\mathbf{a}', \mathbf{b}')$ under the action of $(\mathbb{Z}_\ell \times \mathbb{Z}_\ell) \rtimes \mathbb{Z}_\ell^\times$. Clearly, if $(\mathbf{a}, \mathbf{b})$ is an LP (quaternary LP), and $(\mathbf{a}', \mathbf{b}')$ is equivalent to $(\mathbf{a}, \mathbf{b})$, then $(\mathbf{a}', \mathbf{b}')$ is also an LP (quaternary LP). The following definition characterizes the inherent symmetries of a vector $\mathbf{a} \in \mathbb{C}^\ell$.

Definition 2. *For a vector $\mathbf{a} \in \mathbb{C}^\ell$, the group*

$$G_{\mathbf{a}} = \{j \in \mathbb{Z}_\ell^\times \mid (i, j)(\mathbf{a}) = \mathbf{a} \textit{ for some } i \in \mathbb{Z}_\ell\}$$

is called the multiplier group of $\mathbf{a}$, and each element of $G_{\mathbf{a}}$ is called a multiplier of $\mathbf{a}$.

For $g \in \mathbb{Z}_\ell \rtimes \mathbb{Z}_\ell^\times$ written as a product of cyclic shifts and decimations and $\boldsymbol{q} \in \mathbb{C}^\ell$, the following theorem shows the connection between $G_{\boldsymbol{q}}$ and $G_{g\boldsymbol{q}}$.

Theorem 1. *Let $g \in \mathbb{Z}_\ell \rtimes \mathbb{Z}_\ell^\times$ and $\boldsymbol{q} \in \mathbb{C}^\ell$. Then $G_{g\boldsymbol{q}} = gG_{\boldsymbol{q}}g^{-1}$ and $|G_{\boldsymbol{q}}| = |G_{g\boldsymbol{q}}|$.*

Proof. Observe that $r \in G_{\boldsymbol{q}} \Leftrightarrow d_r(\boldsymbol{q}) = c_i(\boldsymbol{q})$ for some $i \in \mathbb{Z}_\ell \Leftrightarrow d_r(\boldsymbol{q}) = d_r(g^{-1}(g\boldsymbol{q})) = (d_r(g^{-1}))(g\boldsymbol{q}) = (c_i g^{-1})(g\boldsymbol{q}) = (g^{-1}c_{i'})(g\boldsymbol{q})$ for some $i' \in \mathbb{Z}_\ell$, where $c_i g^{-1} = g^{-1}c_{i'}$ for some $i' \in \mathbb{Z}_\ell$ because $\mathbb{Z}_\ell \trianglelefteq \mathbb{Z}_\ell \rtimes \mathbb{Z}_\ell^\times$. Hence, $r \in G_{\boldsymbol{q}} \Leftrightarrow gd_r(g^{-1}(g\boldsymbol{q})) = (gd_r g^{-1})(g\boldsymbol{q}) = c_{i'}(g\boldsymbol{q})$ for some $i' \in \mathbb{Z}_\ell$. This implies that $gG_{\boldsymbol{q}}g^{-1} = G_{g\boldsymbol{q}}$. Then, $|G_{\boldsymbol{q}}| = |G_{g\boldsymbol{q}}|$ as the map $x \to gxg^{-1}$ is one-to-one. ∎

The following theorem appeared as Theorem 4 in [9].

Theorem 2. *Let ℓ be odd and $\boldsymbol{b} \in \{0,1\}^\ell$ such that $\sum_{i=0}^{\ell-1} b_i = \delta$ with $\gcd(\delta, \ell) = 1$. Then there is some $i \in \mathbb{Z}_\ell$ such that $\boldsymbol{b}' = c_i(\boldsymbol{b})$, and*

$$G_{\boldsymbol{b}} \leqslant \widehat{G}_{\boldsymbol{b}'} = \{j \in \mathbb{Z}_\ell^\times \mid d_j(\boldsymbol{b}') = \boldsymbol{b}'\}.$$

The next lemma that follows from Theorem 1 and Theorem 2 shows that in Theorem 2, $G_{\boldsymbol{b}}$ is equal to $\widehat{G}_{\boldsymbol{b}'}$.

Lemma 1. *Let ℓ be odd and $\boldsymbol{b} \in \{0,1\}^\ell$, such that $\sum_{i=0}^{\ell-1} b_i = \delta$ with $\gcd(\delta, \ell) = 1$. Then there is some $i \in \mathbb{Z}_\ell$ such that $\boldsymbol{b}' = c_i(\boldsymbol{b})$, and*

$$G_{\boldsymbol{b}} = \widehat{G}_{\boldsymbol{b}'} = \{j \in \mathbb{Z}_\ell^\times \mid d_j(\boldsymbol{b}') = \boldsymbol{b}'\}.$$

The following lemma follows from Lemma 1.

Lemma 2. *Let ℓ be odd and $\boldsymbol{b} \in \{-1,1\}^\ell$ such that $\sum_{i=0}^{\ell-1} b_i = \delta'$ with $\gcd((\delta'+\ell)/2, \ell) = 1$. Then there is some $i \in \mathbb{Z}_\ell$ such that $\boldsymbol{b}' = c_i(\boldsymbol{b})$, and*

$$G_{\boldsymbol{b}} = \widehat{G}_{\boldsymbol{b}'} = \{j \in \mathbb{Z}_\ell^\times \mid d_j(\boldsymbol{b}') = \boldsymbol{b}'\}.$$

Proof. Since $(i,j)(\mathbf{a}) = \mathbf{a}$ for some $i \in \mathbb{Z}_\ell$ if and only if $(i,j)(\mathbf{a}+\mathbf{1})/2 = (\mathbf{a}+\mathbf{1})/2$ for some $i \in \mathbb{Z}_\ell$. Hence,

$$G_{\boldsymbol{b}} = G_{\frac{\boldsymbol{b}+\mathbf{1}}{2}}.$$

Since, $\sum_{i=0}^{\ell-1}(b_i+1)/2 = (\delta'+\ell)/2$ and $\gcd((\delta'+\ell)/2, \ell) = 1$, by Lemma 2 there is some $i \in \mathbb{Z}_\ell$ such that $\boldsymbol{b}' = c_i((\boldsymbol{b}+\mathbf{1})/2) = (c_i(\boldsymbol{b})+\mathbf{1})/2$, and

$$G_{\boldsymbol{b}} = G_{\frac{\boldsymbol{b}+\mathbf{1}}{2}} = \widehat{G}_{\boldsymbol{b}'} = \widehat{G}_{\frac{c_i(\boldsymbol{b})+\mathbf{1}}{2}}.$$

Now,

$$\widehat{G}_{\frac{c_i(\boldsymbol{b})+\mathbf{1}}{2}} = \widehat{G}_{c_i(\boldsymbol{b})} = \widehat{G}_{\boldsymbol{b}'}$$

follows from the definition of $\widehat{G}_{\boldsymbol{b}'}$. ∎

The following corollary simplifies the search for an LP $(\boldsymbol{a}, \boldsymbol{b})$ with multiplier groups $G_{\boldsymbol{a}}$ and $G_{\boldsymbol{b}}$.

Corollary 1. *An LP $(\boldsymbol{a}, \boldsymbol{b})$ with multiplier groups $G_{\boldsymbol{a}}$ and $G_{\boldsymbol{b}}$ exists if and only if an equivalent LP $(\boldsymbol{a}', \boldsymbol{b}')$ with multiplier groups $\widehat{G}_{\boldsymbol{a}'} = G_{\boldsymbol{a}}$ and $\widehat{G}_{\boldsymbol{b}'} = G_{\boldsymbol{b}}$ exists. Hence, a search for all non-equivalent LPs $(\boldsymbol{a}, \boldsymbol{b})$ with multiplier groups $G_{\boldsymbol{a}}$ and $G_{\boldsymbol{b}}$ can be implemented by searching for all non-equivalent LPs $(\boldsymbol{a}', \boldsymbol{b}')$ with multiplier groups $\widehat{G}_{\boldsymbol{a}'}$ and $\widehat{G}_{\boldsymbol{b}'}$.*

Proof. For an LP $(\boldsymbol{a},\boldsymbol{b})$, $\sum_{i=0}^{\ell-1} a_i = \sum_{i=0}^{\ell-1} b_i = \delta' = \pm 1$ and $\gcd((\ell \pm 1)/2, \ell) = 1$. Hence, by Lemma 2, there exits $i_1, i_2 \in \mathbb{Z}_\ell$ such that $G_u = \widehat{G}_{c_{i_1}(\boldsymbol{a})}$ and $G_v = \widehat{G}_{c_{i_2}(\boldsymbol{b})}$, and $(c_{i_1}(\boldsymbol{a}), c_{i_2}(\boldsymbol{b}))$ is an LP equivalent to $(\boldsymbol{a},\boldsymbol{b})$ with multiplier groups $\widehat{G}_{c_{i_2}(\boldsymbol{a})} = G_{\boldsymbol{a}}$, and $\widehat{G}_{c_{i_2}(\boldsymbol{b})} = G_{\boldsymbol{b}}$. ■

Our repository of LPs, provides many examples of LPs $(\boldsymbol{a},\boldsymbol{b})$, with $G_u \neq G_v$. However, for LPs $(\boldsymbol{a},\boldsymbol{b})$ in our repository with non-trivial multiplier groups, more often than not $G_u = G_v$. On the other hand, for most LPs in our repository, $G_{\boldsymbol{a}} = G_{\boldsymbol{b}} = \{1\}$.

Throughout the rest of the paper, let the row vectors $\mathbf{a}, \mathbf{b} \in \mathbb{R}^\ell$, ℓ be odd, and $w = e^{2\pi i/\ell}$. The *discrete Fourier transform* of $\mathbf{a}$ is $\mathrm{DFT}_{\mathbf{a}}(j) := \sum_{r=0}^{\ell-1} w^{jr} a_r$ and the *power spectral density* of $\mathbf{a}$ is $\mathrm{PSD}_{\mathbf{a}}(j) := |\,\mathrm{DFT}_{\mathbf{a}}(j)|^2$ for $j \in \mathbb{Z}_\ell$. It is shown in [4] that a pair of row vectors $\mathbf{a}, \mathbf{b} \in \{-1,1\}^\ell$ form an LP of length ℓ if and only if

$$\sum_{i=0}^{\ell-1} a_i = \sum_{i=0}^{\ell-1} b_i = \pm 1, \tag{3}$$

$$\mathrm{PSD}_{\mathbf{a}}(j) + \mathrm{PSD}_{\mathbf{b}}(j) = 2\ell + 2 \quad \forall j \in \mathbb{Z}_\ell - \{0\}. \tag{4}$$

If $\mathbf{a} \in \{-1,1\}^\ell$, then $(\mathbf{a}+\mathbf{1})/2 \in \{0,1\}^\ell$. It is plain to see that

$$\mathrm{PSD}_{\frac{\mathbf{a}+\mathbf{1}}{2}}(j) = \frac{\mathrm{PSD}_{\mathbf{a}}(j)}{4} \quad \forall j \in \mathbb{Z}_\ell - \{0\}, \tag{5}$$

and

$$\mathrm{PSD}_{\frac{\mathbf{a}+\mathbf{1}}{2}}(0) = |\,\mathrm{DFT}_{\frac{\mathbf{a}+\mathbf{1}}{2}}(0)|^2 = \left(\frac{\sum_{i=0}^{\ell-1} a_i + \ell}{2}\right)^2 = \left(\frac{\ell \pm 1}{2}\right)^2. \tag{6}$$

The following lemma follows from equations (3), (4), (5), and (6).

Lemma 3. *Let* $\mathbf{a}, \mathbf{b} \in \{-1,1\}^\ell$ *form an LP of length* ℓ. *Then*

$$\sum_{i=0}^{\ell-1} \frac{a_i + 1}{2} = \sum_{i=0}^{\ell-1} \frac{b_i + 1}{2} = \frac{\ell \pm 1}{2},$$

$$\mathrm{PSD}_{\frac{\mathbf{a}+\mathbf{1}}{2}}(j) + \mathrm{PSD}_{\frac{\mathbf{b}+\mathbf{1}}{2}}(j) = \frac{\ell+1}{2} \quad \forall j \in \mathbb{Z}_\ell - \{0\}.$$

The following theorem from [4] determines the relation between $\mathrm{PSD}_{\mathbf{a}}(j)$ and $\mathrm{PAF}_{\mathbf{a}}(j)$.

Theorem 3. *[Wiener-Khinchin Theorem] The PSD of $\mathbf{a} \in \mathbb{R}^\ell$ is equal to the DFT of its PAF, i.e.,*

$$\mathrm{PSD}_{\mathbf{a}}(k) = \sum_{j=0}^{\ell-1} \mathrm{PAF}_{\mathbf{a}}(j) w^{jk} \quad \text{for } k \in \mathbb{Z}_\ell.$$

Moreover, the PAF of $\mathbf{a}$ is equal to the inverse DFT of $\mathbf{a}$'s PSD, i.e.,

$$\mathrm{PAF}_{\mathbf{a}}(j) = \frac{1}{\ell} \sum_{k=0}^{\ell-1} \mathrm{PSD}_{\mathbf{a}}(k) w^{-jk} \quad \text{for } j \in \mathbb{Z}_\ell.$$

The following corollary follows directly from Theorem 3 and equation (6).

Corollary 2. *Let $\mathbf{a}, \mathbf{b} \in \{-1, 1\}^\ell$ form an LP of length ℓ. Then*

$$1 = \mathrm{PSD}_{\mathbf{a}}(0) = \sum_{j=0}^{\ell-1} \mathrm{PAF}_{\mathbf{a}}(j),$$

and

$$\left(\frac{\ell \pm 1}{2}\right)^2 = \mathrm{PSD}_{\frac{\mathbf{a}+\mathbf{1}}{2}}(0) = \sum_{j=0}^{\ell-1} \mathrm{PAF}_{\frac{\mathbf{a}+\mathbf{1}}{2}}(j).$$

Throughout the paper, WLOG, we assume that $\sum_{i=0}^{\ell-1} a_i = \sum_{i=0}^{\ell-1} b_i = 1$. Also, let $e_2(\mathbf{a}) = \sum_{i<j} a_i a_j$ be the *elementary symmetric polynomial of degree* 2 and $p_2(\mathbf{a}) = \sum_i a_i^2$ be the *power sum symmetric polynomial of degree* 2.

For $\mathbf{a} = [a_0, \ldots, a_{\ell-1}]$ and $\ell = nm$ for some positive integers n, m, define $A_j = \sum_{i=0}^{m-1} a_{ni+j}$ for $j = 0, \ldots, n-1$. The vector $\mathcal{A}_m = [A_0, \ldots, A_{n-1}]$ is called the *m-compression* of $\mathbf{a}$ [2]. Throughout the paper, let $\mathcal{A}_m = [A_0, \ldots, A_{n-1}]$, $\mathcal{B}_m = [B_0, \ldots, B_{n-1}]$ be the m-compressions of $\mathbf{a}$, $\mathbf{b}$.

The following theorem from [10] shows how the DFT and the PSD of the m-compression of a vector $\mathbf{a}$ are related to the DFT and the PSD of $\mathbf{a}$.

Theorem 4. *Let $\mathbf{a}$ be a vector of length $\ell = nm$, and $\mathcal{A}_m$ be the m-compression of $\mathbf{a}$. Then $\mathrm{DFT}_{\mathcal{A}_m}(j) = \mathrm{DFT}_{\mathbf{a}}(mj)$ and $\mathrm{PSD}_{\mathcal{A}_m}(j) = \mathrm{PSD}_{\mathbf{a}}(mj)$ for $j \in \{0, \ldots, n-1\}$.*

Compression of complementary vectors has proved to be a valuable tool for finding several previously unknown complementary vectors (vectors whose PAF vectors' jth entries sum to a constant for $j \neq 0$) in the past decade [2, 5, 6, 10]. Compression-based search algorithms are based on a two-step process. In the first step, several candidate compression vectors are computed. The second step involves searching for decompressions of the candidate compressed vectors from the first step.

In Section 2, we find restrictions on the PSD values of LP vectors computed using only the 5th primitive roots of unity. We then corroborate our theoretical restrictions by computing all PSD values which are only based on the 5th primitive roots of unity for all LP vectors that we possess. Then, based on these restrictions, we develop Conjecture 1 which applies to $\ell \equiv 0 \pmod 5$ cases. We then show how this conjecture can be used to prune the search space. Moreover, we provide evidence for Conjecture 1 by confirming that it is valid for all $\ell \leqslant 85$ such that $\ell \equiv 0 \pmod 5$ (with the sole exception of $\ell = 75$).

In Section 3, we first discuss the limitations of the methods used by [10] for finding LPs of length $\ell > 77$ and how those limitations can be overcome. Then, by assuming that the sought after LP $(\boldsymbol{a}, \boldsymbol{b})$ satisfies $\{1, 69\} \leqslant \widehat{G}_{\boldsymbol{a}}$, $\{1, 69\} \leqslant \widehat{G}_{\boldsymbol{b}}$, and using the method in Section 4.1.1 of [5] with $H_1 = \{1, 69\}$, we find the first known examples of LPs of length 85 that satisfy this property. The length $\ell = 85$ has been the smallest open length case. Additionally, we show how to exploit a different concept of balance applied to LPs of composite order. As an application, we find the first examples of LPs of length 87.

In Section 4, we describe the partial searches that have been implemented for LPs of length 115.

In Section 5, we provide the current list of ten ℓ values less than 200 for which the LP existence problem remains unsolved.

2 LPs of lengths $\ell \equiv 0 \pmod 5$

For a vector of length $\ell = nm$, the following lemma expresses a sum of PAFs in terms of the PAF of the compressed vector $\mathcal{A}_m$.

Lemma 4. *Let* **a** *be a length $\ell = nm$ vector for positive odd integers n and m. Then*

$$\sum_{j=0}^{m-1} \mathrm{PAF}_a(nj+k) = \mathrm{PAF}_{\mathcal{A}_m}(k).$$

Proof.

$$\begin{aligned}
\sum_{j=0}^{m-1} \mathrm{PAF}_a(nj+k) &= \sum_{j=0}^{m-1}\sum_{i=0}^{\ell-1} a_i a_{i-nj-k} = \sum_{j=0}^{m-1}\sum_{i=0}^{m-1}\sum_{r=0}^{n-1} a_{ni+r}a_{ni-nj+r-k} \\
&= \sum_{r=0}^{n-1}\sum_{i=0}^{m-1}\sum_{j=0}^{m-1} a_{ni+r}a_{nj+r-k} = \sum_{r=0}^{n-1}\left(\sum_{i=0}^{m-1} a_{ni+r}\right)\left(\sum_{j=0}^{m-1} a_{nj+r-k}\right) \\
&= \sum_{r=0}^{n-1} A_r A_{r-k} = \mathrm{PAF}_{\mathcal{A}_m}(k).
\end{aligned}$$

■

For a vector of length $\ell = 5m$, the following lemma determines $\mathrm{PSD}_{\mathbf{a}}(rm)$ in terms of $\mathrm{PAF}_{\mathbf{a}}(j)$ for $j \in \mathbb{Z}_\ell$.

Lemma 5. *Let $m \in \mathbb{Z}_{\geqslant 1}$, $r \in \{1, \ldots, 4\}$, and $\mathbf{a}$ be a vector of length $\ell = 5m$. Then*

$$\mathrm{PSD}_{\mathbf{a}}(rm) = \sum_{j=0}^{m-1} \mathrm{PAF}_{\mathbf{a}}(5j) - \sum_{k=1}^{2} \frac{1 + (-1)^{k+\lfloor \frac{r}{2} \rfloor}\sqrt{5}}{2} \sum_{j=0}^{m-1} \mathrm{PAF}_{\mathbf{a}}(5j+k).$$

Proof. Let $w = e^{2\pi i/\ell}$, $w' = w^m$. By Theorem 3,

$$\begin{aligned}
\mathrm{PSD}_{\mathbf{a}}(rm) &= \sum_{j=0}^{\ell-1} \mathrm{PAF}_{\mathbf{a}}(j) w^{rmj} = \sum_{j=0}^{\ell-1} \mathrm{PAF}_{\mathbf{a}}(j)(w')^{rj} = \sum_{k=0}^{4} \sum_{j=0}^{m-1} \mathrm{PAF}_{\mathbf{a}}(5j+k)(w')^{rk} \\
&= \sum_{j=0}^{m-1} \mathrm{PAF}_{\mathbf{a}}(5j) + \sum_{k=1}^{2} 2\cos\left(\frac{2\pi rk}{5}\right) \sum_{j=0}^{m-1} \mathrm{PAF}_{\mathbf{a}}(5j+k) \\
&= \sum_{j=0}^{m-1} \mathrm{PAF}_{\mathbf{a}}(5j) + \sum_{k=1}^{2} \left(\frac{-1 + (-1)^{\lfloor (rk \bmod 5)/2 \rfloor}\sqrt{5}}{2}\right) \sum_{j=0}^{m-1} \mathrm{PAF}_{\mathbf{a}}(5j+k),
\end{aligned}$$

from which the assertion follows directly. ■

Corollary 3. *For a pair of vectors $(\mathbf{a}, \mathbf{b})$ of length $\ell = 5m$, the LP constraints*

$$\mathrm{PSD}_{\mathbf{a}}(rm) + \mathrm{PSD}_{\mathbf{b}}(rm) = 2\ell + 2$$

are satisfied for $r \in \{1, \ldots, 4\}$ if and only if

$$\sum_{j=0}^{m-1} \Big(\mathrm{PAF}_{\mathbf{a}}(5j) + \mathrm{PAF}_{\mathbf{b}}(5j)\Big) - \sum_{j=0}^{m-1} \sum_{k=1}^{2} \frac{\mathrm{PAF}_{\mathbf{a}}(5j+k) + \mathrm{PAF}_{\mathbf{b}}(5j+k)}{2} = 2\ell + 2,$$

and

$$\sum_{j=0}^{m-1} \sum_{k=1}^{2} (-1)^k \Big(\mathrm{PAF}_{\mathbf{a}}(5j+k) + \mathrm{PAF}_{\mathbf{b}}(5j+k)\Big) = 0.$$

The following corollary follows from Lemmas 4 and 5.

Corollary 4. *Let $\mathbf{a}$ be a vector of length $5m$ for some $m \in \mathbb{Z}_{\geqslant 1}$. Let the m-compression of $\mathbf{a}$ be $\mathcal{A}_m = [A_0, A_1, A_2, A_3, A_4]$. Then,*

$$\mathrm{PSD}_{\mathbf{a}}(rm) = p_2(\mathcal{A}_m) - \frac{1}{2} e_2(\mathcal{A}_m) + (-1)^{\lfloor \frac{r}{2} \rfloor} \sqrt{5} \left(\frac{\mathrm{PAF}_{\mathcal{A}_m}(1) - \mathrm{PAF}_{\mathcal{A}_m}(2)}{2}\right) \tag{7}$$

for $r = 1, \ldots, 4$.

Proposition 1. *Let* $(\mathbf{a}, \mathbf{b})$ *be an LP of length* $\ell = 5m$ *with* m *odd. Then there exist integers* $n_1, n_2 \in \mathbb{Z}_{\geqslant 0}$ *with* $n_1 + n_2 = 2\ell + 2$ *and* $x \in \mathbb{Z}$ *such that*

$$\begin{aligned} \mathrm{PSD}_{\mathbf{a}}(rm) &= n_1 + (-1)^{\lfloor \frac{r}{2} \rfloor}\sqrt{5}x, \\ \mathrm{PSD}_{\mathbf{b}}(rm) &= n_2 - (-1)^{\lfloor \frac{r}{2} \rfloor}\sqrt{5}x \end{aligned} \tag{8}$$

for $r = 1, \ldots, 4,$ *where*

$$x = \frac{\mathrm{PAF}_{\mathcal{A}_m}(1) - \mathrm{PAF}_{\mathcal{A}_m}(2)}{2} = -\frac{\mathrm{PAF}_{\mathcal{B}_m}(1) - \mathrm{PAF}_{\mathcal{B}_m}(2)}{2}. \tag{9}$$

Proof. Equations (8) directly follow from equation (7) and the fact that an LP $(\mathbf{a}, \mathbf{b})$ of length $\ell = 5m$ satisfies $\mathrm{PSD}_{\mathbf{a}}(rm) + \mathrm{PSD}_{\mathbf{b}}(rm) = 2\ell + 2$ for $r = 1, \ldots, 4$. Since by our general assumption the vectors $\mathbf{a}, \mathbf{b}$ satisfy $\sum_{i=0}^{\ell-1} a_i = \sum_{i=0}^{\ell-1} b_i = 1$, the same holds true for their m-compressions, that is $\sum_{i=0}^{4} A_i = \sum_{i=0}^{4} B_i = 1$. Consequently, $\left(\sum_{i=0}^{4} A_i\right)^2 = p_2(\mathcal{A}_m) + 2e_2(\mathcal{A}_m) = 1$, and analogously for $\mathcal{B}_m$. Then by Corollary 4,

$$\begin{aligned} n_1 &= p_2(\mathcal{A}_m) - \frac{1}{2}e_2(\mathcal{A}_m) = \frac{1}{4}\Big(5p_2(\mathcal{A}_m) - 1\Big), \\ n_2 &= p_2(\mathcal{B}_m) - \frac{1}{2}e_2(\mathcal{B}_m) \ = \frac{1}{4}\Big(5p_2(\mathcal{B}_m) - 1\Big). \end{aligned} \tag{10}$$

This shows that n_1 and n_2 are integers, because $p_2(\mathcal{A}_m)$ is the sum of five odd squares and hence equals 1 mod 4. To see that x is an integer, note that an odd m implies that $\mathrm{PAF}_{\mathcal{A}_m}(k)$ and $\mathrm{PAF}_{\mathcal{B}_m}(k)$ for $k = 1, 2$ are all odd. Equations (9) follow from Corollary 4 and equations (8).

We will next prove that $0 \leqslant n_1$. By symmetry, this will also give us $0 \leqslant n_2$. By equations (7) and (10)

$$\frac{4n_1}{25} = \frac{p_2(\mathcal{A}_m)}{5} - \frac{1}{25} = \frac{p_2(\mathcal{A}_m)}{5} - \left(\frac{\sum_{i=0}^{4} A_i}{5}\right)^2.$$

Hence, $4n_1/25$ is the population variance of the numbers in $\{A_0, A_1, A_2, A_3, A_4\}$ implying that $0 \leqslant n_1$. ∎

Experimental evidence gathered for $\ell = 5, 15, 25, 35, 45, 55, 65, 85$ indicates there are LPs of these orders such that

$$\begin{aligned} n_1 &= \frac{1}{4}\Big(5p_2(\mathcal{A}_m) - 1\Big) = \ell + 1 = 5m + 1, \\ n_2 &= \frac{1}{4}\Big(5p_2(\mathcal{B}_m) - 1\Big) = \ell + 1 = 5m + 1. \end{aligned} \tag{11}$$

Solving equations (11) for $p_2(\mathcal{A}_m)$ and $p_2(\mathcal{B}_m)$, we get that equations (11) are equivalent to

$$p_2(\mathcal{A}_m) = p_2(\mathcal{B}_m) = 4m + 1.$$

The next two lemmas determine restrictions on n_1, n_2, and x in Proposition 1.

Lemma 6. *Each of n_1, n_2, and x in Proposition 1 must be even.*

Proof. By symmetry, it suffices to prove the result for n_1 and x. Let $\mathbf{a}$ be as in Proposition 1. By replacing $\mathbf{a}$ with $(\mathbf{a}+\mathbf{1})/2$ in Lemma 5, and by equation (5) we get that

$$\mathrm{PSD}_{\frac{\mathbf{a}+\mathbf{1}}{2}}(m) = \frac{\alpha_1}{2} + \frac{\alpha_2}{2}\sqrt{5} = \frac{n_1 + \sqrt{5}x}{4},$$

for some $\alpha_1, \alpha_2 \in \mathbb{Z}$. Hence, by the linear independence of 1 and $\sqrt{5}$ in the field extension $\mathbb{Q}[\sqrt{5}]$, we have $\alpha_1 = n_1/2$ and $\alpha_2 = x/2$, implying that both n_1 and x must be even. ■

Lemma 7. *Let n_1, n_2, and x be as in Proposition 1. Then $n_i + x \equiv 0 \pmod 4$ for $i = 1, 2$.*

Proof. By symmetry, it suffices to prove the result for n_1 and x. Let $w' = e^{2\pi i/5}$ and $\mathbf{a}$ be as in Proposition 1. Then, by the proof of Lemma 5,

$$\mathrm{PSD}_{\mathbf{a}}(m) = \sum_{k=0}^{4}\sum_{j=0}^{m-1} \mathrm{PAF}_{\mathbf{a}}(5j+k)(w')^k = n_1 + \sqrt{5}x.$$

Now, by equation (5),

$$\mathrm{PSD}_{\frac{\mathbf{a}+\mathbf{1}}{2}}(m) = \sum_{k=0}^{4}\sum_{j=0}^{m-1} \mathrm{PAF}_{\frac{\mathbf{a}+\mathbf{1}}{2}}(5j+k)(w')^k = \frac{n_1 + \sqrt{5}x}{4}.$$

Since $\mathrm{PAF}_{(\mathbf{a}+\mathbf{1})/2}(5j+k) = \mathrm{PAF}_{(\mathbf{a}+\mathbf{1})/2}(-5j-k)$ for $k \in \{1, 2\}$,

$$\mathrm{PSD}_{\frac{\mathbf{a}+\mathbf{1}}{2}}(m) = S_0 + S_1\left(w' + \overline{w'}\right) + S_2\left((w')^2 + \left(\overline{w'}\right)^2\right),$$

where $S_0 = \sum_{j=0}^{m-1} \mathrm{PAF}_{(\mathbf{a}+\mathbf{1})/2}(5j)$ and $S_i = \sum_{j=0}^{m-1} \mathrm{PAF}_{(\mathbf{a}+\mathbf{1})/2}(5j+i)$ for $i = 1, 2$. Observe that $S_0, S_1, S_2 \in \mathbb{Z}_{\geqslant 1}$. Then, since $(w')^2 + \left(\overline{w'}\right)^2 = \left(w' + \overline{w'}\right)^2 - 2 \in \mathbb{Z}\left[w' + \overline{w'}\right]$,

$$\mathrm{PSD}_{\frac{\mathbf{a}+\mathbf{1}}{2}}(m) = S_0 + S_1\left(w' + \overline{w'}\right) + S_2\left((w')^2 + \left(\overline{w'}\right)^2\right) \in \mathbb{Z}\left[w' + \overline{w'}\right].$$

Then since $\sqrt{5} = 2w' + 2\overline{w'} + 1$,

$$\mathrm{PSD}_{\frac{\mathbf{a}+\mathbf{1}}{2}}(m) = \frac{n_1 + \sqrt{5}x}{4} = \frac{n_1 + x + 2x\left(w' + \overline{w'}\right)}{4} \in \mathbb{Z}\left[w' + \overline{w'}\right].$$

Hence, $n_1 + x \equiv 0 \pmod 4$. ■

The following general lemma will be used to find another restriction on n_1 and n_2 in Proposition 1.

Lemma 8. *Let* $\mathbf{a}$ *be a vector of length* $\ell = mn$ *for some positive integers* m *and* n*. Then*

$$\sum_{k=0}^{n-1} \mathrm{PSD}_{\mathbf{a}}(km) = n \sum_{x=0}^{m-1} \mathrm{PAF}_{\mathbf{a}}(xn) = n \, \mathrm{PAF}_{\mathcal{A}_m}(0).$$

Proof. Since $\mathrm{PSD}_a(km) = \mathrm{PSD}_{\mathcal{A}_m}(k)$, by applying the inverse Fourier transform to $[\mathrm{PSD}_{\mathcal{A}_m}(0) \ldots \mathrm{PSD}_{\mathcal{A}_m}(n-1)]$, we get $[\mathrm{PAF}_{\mathcal{A}_m}(0), \ldots, \mathrm{PAF}_{\mathcal{A}_m}(n-1)]$, which at 0 is what the lemma claims (cf. Theorem 3). ■

The following lemma provides an additional restriction on the values of n_1, n_2 in Proposition 1.

Lemma 9. *Let* $\mathbf{a}, \mathbf{b}, n_1,$ *and* n_2 *be as in Proposition 1. Then* $n_i \equiv 6 \pmod{10}$ *for* $i = 1, 2$.

Proof. By symmetry, it suffices to prove the result for $i = 1$. By Lemma 8 and Proposition 1

$$\sum_{k=0}^{4} \mathrm{PSD}_{\mathbf{a}}(km) = 1 + 4n_1 = 5 \left(\sum_{x=0}^{m-1} \mathrm{PAF}_{\mathbf{a}}(5x) \right) \equiv 0 \pmod{5}.$$

Alternatively, we can employ $p_2(\mathcal{A}_m) = 4s + 1$ (see the proof of Proposition 1) to deduce that $n_1 = \big(5p_2(\mathcal{A}_m) - 1\big)/4 = 5s + 1$ for some integer s. Now the result follows from the Chinese remainder theorem since n_1 must be even by Lemma 6. ■

The following corollary provides upper and lower bounds on n_1, n_2 in Proposition 1.

Corollary 5. *Let* $\ell = 5m$*, and let* $\mathbf{a}$, $\mathbf{b}$, n_1*, and* n_2 *be as in Proposition 1. Then* $6 \leqslant n_i \leqslant 2\ell - 4$ *for* $i = 1, 2$.

Proof. By Proposition 1, we get $0 \leqslant n_i \leqslant 2\ell + 2 = 10m + 2$ for $i = 1, 2$. By Lemma 9, we get $6 \leqslant n_i \leqslant 2\ell - 4 = 10m - 4$ for $i = 1, 2$. ■

The lower bound for n_i in Corollary 5 is achieved by taking $\mathcal{A}_m = [1, 1, 1, -1, -1]$.

The following corollary now follows from Proposition 1, Corollary 5, and Lemma 7.

Corollary 6. *Let* $\ell = 5m$*, and let* $\mathbf{a}$, $\mathbf{b}$, n_1, n_2*, and* x *be as in Proposition 1. Then there exist non-negative integers* k_1, k_2 *such that* $n_i = 10k_i + 6$ *for* $i = 1, 2$, $k_1 + k_2 = m - 1$*, and* $2k_i + 2 \equiv x$ *(mod 4).*

Corollary 6 summarizes all the constraints obtained in this section regarding n_1, n_2, and x in equation (8). In fact, all the constraints regarding n_1, n_2, and x that appear before Corollary 6 are implied by Corollary 6.

Exhaustive searches for $\ell = 5, 15, 25$ have revealed that most LPs of these lengths have $n_1 = n_2 = \ell+1$, where n_1, n_2 are as in Proposition 1. The case $n_1 = n_2 = \ell+1$ corresponds to taking $k_1 = k_2 = (m-1)/2$ in Corollary 6. Non-exhaustive searches for larger odd values of ℓ which are multiples of 5 have revealed the same pattern, i.e., the standard relationship $\mathrm{PSD}_{\mathbf{a}}(m) + \mathrm{PSD}_{\mathbf{b}}(m) = 2\ell + 2$ is materialized (often, but not always) in the same manner. These observations give rise to the following conjecture.

Conjecture 1. *For every odd positive integer* $\ell \equiv 0 \pmod 5$*, there exists at least one LP* $(\mathbf{a}, \mathbf{b})$ *of length* $\ell = 5m$ *such that*

$$\begin{aligned}\mathrm{PSD}_{\mathbf{a}}(rm) &= \ell + 1 + (-1)^{\lfloor \frac{r}{2} \rfloor}\sqrt{5}x \\ \mathrm{PSD}_{\mathbf{b}}(rm) &= \ell + 1 - (-1)^{\lfloor \frac{r}{2} \rfloor}\sqrt{5}x\end{aligned} \tag{12}$$

for $r = 1, \ldots, 4$*, and for some nonnegative integer* $x \equiv -(\ell+1) \equiv \ell + 1 \pmod 4$.

By formula (8), Conjecture 1 holds for one r if and only if $n_1 = n_2$. Again, by formula (8), if Conjecture 1 holds for one r, then it also holds for the other rs. Conjecture 1 states that for each odd positive $\ell \equiv 0 \pmod 5$, there exists a length ℓ LP $(\mathbf{a}, \mathbf{b})$ such that $n_1 = n_2 = \ell+1$ in Proposition 1. That is, the constant $2\ell+2$ can be distributed in a "balanced" manner between $\mathrm{PSD}_{\mathbf{a}}(rm)$ and $\mathrm{PSD}_{\mathbf{b}}(rm)$ for $r \in \{1, \ldots, 4\}$. On the other hand, there exist LPs $(\mathbf{a}, \mathbf{b})$ of length $\ell = 5m$ which do not satisfy $n_1 = n_2$. Table 1 provides computational evidence for Conjecture 1. Cases $m = 1, 3, 5$ are based on complete—and the remaining cases are based on partial—classifications of all non-equivalent LPs, where equivalent LPs satisfying Conjecture 1 have the same x value. This is because

$$\mathrm{PSD}_{(j_1,k)\mathbf{a}}(rm) = \mathrm{PSD}_{\mathbf{a}}(krm)$$

for each $(j_1, k) \in \mathbb{Z}_\ell \rtimes \mathbb{Z}_\ell^\times$ and $r \in \{1, \ldots, 4\}$.

The following proposition provides necessary and sufficient constraints on the m-compressed vectors $(\mathcal{A}_m, \mathcal{B}_m)$ of an LP $(\mathbf{a}, \mathbf{b})$ of length $\ell = 5m$ to satisfy equations (12).

Proposition 2. *The* m*-compressed vectors* $\mathcal{A}_m = [A_0, \ldots, A_4]$ *and* $\mathcal{B}_m = [B_0, \ldots, B_4]$ *of an LP* $(\mathbf{a}, \mathbf{b})$ *of length* $\ell = 5m$ *satisfy the conditions in Conjecture 1 if and only if*

$$p_2(\mathcal{A}_m) = \mathrm{PAF}_{\mathcal{A}_m}(0) = p_2(\mathcal{B}_m) = \mathrm{PAF}_{\mathcal{B}_m}(0) = 4m + 1. \tag{13}$$

Proof. This result follows from Proposition 1 and equation (10). ■

m	$\ell = 5m$	x
1	5	2
3	15	$0, 4$
5	25	$2, 6, 10$
7	35	$0, 8, 16$
9	45	$2, 6, 10, 14, 18$
11	55	$4, 8, 12, 20, 24$
13	65	14
17	85	18

Table 1: Computationally verified cases for Conjecture 1 with their corresponding x value(s)

Equations (13) in Proposition 2 drastically reduce the search space for an LP $(\mathbf{a}, \mathbf{b})$ satisfying the conditions in Conjecture 1. For such an LP, we are only interested in all-odd solutions to equations (13) since A_i, B_i are odd numbers for $i = 0, \ldots, 4$. Another consequence of Proposition 2 is that the alphabet of the possible m-compressed vectors $(\mathcal{A}_m, \mathcal{B}_m)$ is also significantly truncated. More specifically, while the full alphabet for candidate m-compressed vectors is

$$\{-m, -(m-2), \ldots, -1, +1, \ldots, (m-2), m\},$$

by Proposition 2, A_i is an odd integer with $|A_i| \leqslant \sqrt{4m-3} < 2\sqrt{m}$ for $i \in \mathbb{Z}_\ell$.

Next, we show Conjecture 1 cannot be ruled out by the necessary constraints (13) and $\sum_{i=0}^{4} A_i = \sum_{i=0}^{4} B_i = 1$ for LPs of lengths $\ell = 5, 15, 25, 35, 45, 55, 65, 75, 85, 95, 105, 115$. In Table 2, we summarize the all-odd solutions to (13) for odd ℓ such that $\ell = 5m$ and $m \in \{1, \ldots, 23\}$. In the last column, we record the all-odd solutions (up to sign changes and permutations) of the five sums of squares Diophantine equations of the fourth column. Since the linear equations $\sum_{i=0}^{4} A_i = \sum_{i=0}^{4} B_i = 1$ must also be satisfied, some of these all-odd solutions are ruled out, and this is indicated by boldface. Conjecture 1 has practical value as it can be used to prune the search space when $\ell \equiv 0 \pmod 5$ by only decompressing m-compressions which are compatible with the all-odd solutions in Table 2.

3 Finding LPs of lengths $\ell = 85$ and $\ell = 87$

The orbit of a vector $\boldsymbol{b}$ under circulant shifts and decimations is called the *decimation class* of $\boldsymbol{b}$ [9]. Since $(\mathbb{Z}_\ell \times \mathbb{Z}_\ell) \rtimes \mathbb{Z}_\ell^\times$ acts on LPs, the search space for LPs is drastically reduced by

ℓ	m	$\mathrm{PSD}_{\mathbf{a}}(rm)$ $\mathrm{PSD}_{\mathbf{b}}(rm)$	$\sum_{i=0}^{4} A_i^2$ $\sum_{i=0}^{4} B_i^2$	All-odd solutions
5	1	$5+1\pm(-1)^{\lfloor\frac{r}{2}\rfloor}\sqrt{5}x$	$4\cdot 1+1=5$	$[1,1,1,1,1]$
15	3	$15+1\pm(-1)^{\lfloor\frac{r}{2}\rfloor}\sqrt{5}x$	$4\cdot 3+1=13$	$[1,1,1,1,3]$
25	5	$25+1\pm(-1)^{\lfloor\frac{r}{2}\rfloor}\sqrt{5}x$	$4\cdot 5+1=21$	$[1,1,1,3,3]$
35	7	$35+1\pm(-1)^{\lfloor\frac{r}{2}\rfloor}\sqrt{5}x$	$4\cdot 7+1=29$	$[1,1,1,1,5]$, $[1,1,3,3,3]$
45	9	$45+1\pm(-1)^{\lfloor\frac{r}{2}\rfloor}\sqrt{5}x$	$4\cdot 9+1=37$	$[1,1,1,3,5]$, $[1,3,3,3,3]$
55	11	$55+1\pm(-1)^{\lfloor\frac{r}{2}\rfloor}\sqrt{5}x$	$4\cdot 11+1=45$	$[1,1,3,3,5]$, $[\mathbf{3},\mathbf{3},\mathbf{3},\mathbf{3},\mathbf{3}]$
65	13	$65+1\pm(-1)^{\lfloor\frac{r}{2}\rfloor}\sqrt{5}x$	$4\cdot 13+1=53$	$[\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{7}]$, $[1,1,1,5,5]$, $[1,3,3,3,5]$
75	15	$75+1\pm(-1)^{\lfloor\frac{r}{2}\rfloor}\sqrt{5}x$	$4\cdot 15+1=61$	$[1,1,1,3,7]$, $[1,1,3,5,5]$, $[3,3,3,3,5]$
85	17	$85+1\pm(-1)^{\lfloor\frac{r}{2}\rfloor}\sqrt{5}x$	$4\cdot 17+1=69$	$[1,1,3,3,7]$, $[1,3,3,5,5]$
95	19	$95+1\pm(-1)^{\lfloor\frac{r}{2}\rfloor}\sqrt{5}x$	$4\cdot 19+1=77$	$[1,1,1,5,7]$, $[\mathbf{1},\mathbf{1},\mathbf{5},\mathbf{5},\mathbf{5}]$, $[1,3,3,3,7]$, $[3,3,3,5,5]$
105	21	$105+1\pm(-1)^{\lfloor\frac{r}{2}\rfloor}\sqrt{5}x$	$4\cdot 21+1=85$	$[\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{9}]$, $[1,1,3,5,7]$, $[1,3,5,5,5]$, $[3,3,3,3,7]$
115	23	$115+1\pm(-1)^{\lfloor\frac{r}{2}\rfloor}\sqrt{5}x$	$4\cdot 23+1=93$	$[\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{9}]$, $[1,3,3,5,7]$, $[3,3,5,5,5]$

Table 2: All-odd solutions to equations (13)

searching only across decimation class representatives [4]. In fact, to classify $\{0,1\}$ LPs up to equivalence, in light of Lemma 3, Fletcher et al. [4] exhaustively generated a set of all decimation class representatives $\boldsymbol{b} \in \{0,1\}^\ell$ for odd $\ell \leqslant 47$ such that $\sum_{i=0}^{\ell-1} b_i = (\ell+1)/2$. By Lemma 3, they then deleted the class representatives $\boldsymbol{b}$ such that $\mathrm{PSD}_{\boldsymbol{b}}(j) > (\ell+1)/2$ for some $j \in \mathbb{Z}_\ell \backslash \{0\}$. Then, among all the decimations of a given vector $\boldsymbol{b}$, they selected the decimations $d_k(\boldsymbol{b})$ with $|\mathrm{PSD}_{d_k(\boldsymbol{b})}(1) - (\ell+1)/4|$ of greatest value to be the representatives of $\boldsymbol{b}$'s decimation class, where the decimation class of $\boldsymbol{b}$ is allowed to have multiple different decimation class representatives. In the second step, they sorted the list of class representative $\boldsymbol{b}$s according to

$$\mathrm{PSD}_{\boldsymbol{b}}(1) - \frac{\ell+1}{4}.$$

In the last step, they located pairs of class representatives $\boldsymbol{a}, \boldsymbol{b}$ that satisfied

$$\mathrm{PSD}_{\boldsymbol{a}}(1) - \frac{\ell+1}{4} + \mathrm{PSD}_{\boldsymbol{b}}(1) - \frac{\ell+1}{4} = 0. \tag{14}$$

To confirm that the LP property was satisfied by all the resulting pairs, they also deleted pairs $(\boldsymbol{a}, \boldsymbol{b})$ satisfying equation (14) that did not satisfy the equations involving the PSDs of $\boldsymbol{a}$ and $\boldsymbol{b}$ as in Lemma 3. In the end, Fletcher et al. [4] classified all LPs of length less than or equal to 47 up to equivalence using this method. A similar method that additionally exploited simultaneous decompressions of candidate compressed vectors was implemented in [10]. This method found an LP of length 77 for the first time.

For lengths $\ell = 55$ and 77, Table 3 reports the decimation class counts for the number of decimation classes of length ℓ, $\{0, 1\}$ vectors with $(\ell + 1)/2$ ones reported in [9], and the solution times for the simultaneous decompression-based searches reported in [10].

Length ℓ	Number of Decimation Classes	Exhaustive Search (CPU Hours)	One Solution (CPU Hours)
55	$1.738341231644e + 12$	101,542.4	—
77	$2.945564382817e + 18$	—	182,280

Table 3: Decimation class counts in [9] and solution times for simultaneous decompression-based searches in [10]

Assuming that the number of compressed pairs and the time required for decompression scales linearly on average with the number of decimation classes, we expect the Table 4 time requirements for an exhaustive search or partial search to first solution if the method in [10] is used for lengths $\ell = 85$ and $\ell = 87$.

Length ℓ	Number of Decimation Classes	Exhaustive Search (CPU Hours)	One Solution (CPU Hours)
85	$6.100692175209e + 20$	$3.563621e + 13$	37,752,839
87	$2.693812140345e + 21$	$1.573547e + 14$	166,700,847

Table 4: Expected time needed for an exhaustive search and partial search to first solution using the method in [10]

These time estimates are optimistic as experiments suggest that the growth rate is superlinear in the number of decimation classes. This growing magnitude of complexity precluded Turner *et al.* [10] from investigating larger open LP problems. Partial searches for LPs using the compression method for $\ell > 77$ only remain viable by reducing the number of complementary compressed vectors, or rather selecting the complementary compressions with higher likelihood of producing an LP. Alternatively, by Corollary 1 we can search for an LP $(\boldsymbol{a}, \boldsymbol{b})$ that has multiplier groups $\widehat{G}_{\boldsymbol{a}}$ and $\widehat{G}_{\boldsymbol{b}}$ both containing some non trivial elements of $\mathbb{Z}_n^{\times}$. This would reduce the search space drastically and can bring $\ell > 77$ cases within computational reach if such an LP exists. For $\ell = 3m$, $m \in \{39, 43, 49\}$, Kotsireas and Koutschan [5] used a method that exploits such a property along with a method that reduces the possible values of $\mathrm{PSD}_{\mathbf{a}}(m)$ and keeps only the vectors whose $\mathrm{PSD}_{\mathbf{a}}(m)$ are within the reduced set, and found the first examples of LPs of lengths 117, 129, and 147. Kotsireas and Koutschan [5] also found an LP of length 133 by solely restricting the search to LPs $(\boldsymbol{a}, \boldsymbol{b})$ whose multiplier groups $\widehat{G}_{\boldsymbol{a}}$ and $\widehat{G}_{\boldsymbol{b}}$ both contained the group $G = \{1, 11, 121\} < \mathbb{Z}_{133}^{\times}$.

3.1 LPs of length $\ell = 85$

We used the method in Section 4.1.1 in [5] with $H_1 = \{1, 69\}$ and Corollary 1 to restrict the search space for LPs of length $\ell = 85$ by assuming that the sought after LP $(\boldsymbol{a}, \boldsymbol{b})$ has multiplier groups $\widehat{G}_{\boldsymbol{a}}$ and $\widehat{G}_{\boldsymbol{b}}$ satisfying $H_1 = \{1, 69\} \leqslant \widehat{G}_{\boldsymbol{a}}$ and $H_1 = \{1, 69\} \leqslant \widehat{G}_{\boldsymbol{b}}$. This method found the first known examples of LPs of length $\ell = 85$. This had been the smallest previously unknown length case for LPs. The subgroup $H_1 = \{1, 69\}$ of $\mathbb{Z}_{85}^{\times}$ acts on $\mathbb{Z}_{85}$ and yields 16 orbits of size 1 and 34 orbits of size 2. We searched for an LP of length $\ell = 85$ which could be obtained by combining the orbits of the subgroup H_1. This restriction has the benefit of reducing the search space provided that such an LP exists. We chose 12 orbits of size 1 and 15 orbits of size 2 to make blocks of size $12 \cdot 1 + 15 \cdot 2 = 42$. Here, each block of size 42 consists of positions of -1s determining the vectors $\boldsymbol{a}$ and $\boldsymbol{b}$. Therefore, the size of the search space was $\binom{16}{12} \cdot \binom{34}{15} = 1820 \cdot 1{,}855{,}967{,}520 = 3{,}377{,}860{,}886{,}400$. This search was not exhaustive and was interrupted after traversing 2.6% of the search space. This took about 100 hours of CPU time. This search was done on 64 compute nodes, each with two 8-core Intel Haswell CPUs (Xeon E5-2630v3, 2.4Ghz) and 128 GB RAM. For this search, we implemented the same PSD test in Section 4 of [5] without checking if the PSD value at $\ell/3$ is from a finite list of candidates, and used the same method as in Section 4 of [5] to identify LPs among vectors that passed the PSD test. However, this search did not take advantage of Conjecture 1 by only keeping the vectors $\mathbf{a}$ that satisfied $\mathrm{PAF}_{\mathcal{A}_{17}}(0) = 69$ for the 17 compression $\mathcal{A}_{17}$ of $\mathbf{a}$ as Conjecture 1 had not yet been formulated at the time of the search. Our search yielded 4 equivalent (1 non-equivalent) LPs of length $\ell = 85$ made out of 6 different vectors. Their lexicographic rank encodings as subsets of size 12 out of 16 and 15 out of 34 are

$$
\begin{aligned}
&\big(\{12, 1321116338\},\ \{42, 1275934280\}\big),\\
&\big(\{12, 1843909851\},\ \{42, 606586783\}\big),\\
&\big(\{42, 1275934280\},\ \{9, 1555522731\}\big),\\
&\big(\{42, 606586783\},\ \{9, 788215097\}\big).
\end{aligned}
$$

See [7] for lexicographic ranking and unranking algorithms for subsets of size k. For the first LP $(\mathbf{a}, \mathbf{b})$ of length $\ell = 85$ shown above, its lexicographic rank encoding $\big(\{12, 13211163 38\}, \{42, 1275934280\}\big)$ is decoded as follows.

- In the space of $\binom{16}{12} = 1820$ 12-subsets of $\{1, \ldots, 16\}$, decode

$$\begin{aligned} 12 \text{ as } \mathbf{a}_{\text{ones}} &= \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 14, 15\}, \\ 42 \text{ as } \mathbf{b}_{\text{ones}} &= \{1, 2, 3, 4, 5, 6, 7, 8, 10, 11, 14, 15\}. \end{aligned}$$

- In the space of $\binom{34}{15} = 1,855,967,520$ 15-subsets of $\{1, \ldots, 34\}$, decode

$$\begin{aligned} 1321116338 \text{ as } \mathbf{a}_{\text{twos}} &= \{3, 4, 5, 7, 10, 11, 22, 24, 25, 27, 28, 29, 30, 31, 34\}, \\ 1275934280 \text{ as } \mathbf{b}_{\text{twos}} &= \{2, 8, 10, 11, 12, 15, 19, 21, 23, 25, 26, 28, 29, 33, 34\}. \end{aligned}$$

- Enumerate the 16 orbits of size 1 in increasing order as $O_1 = \{\{5\}, \{10\}, \{15\}, \{20\}, \{25\}, \{30\}, \{35\}, \{40\}, \{45\}, \{50\}, \{55\}, \{60\}, \{65\}, \{70\}, \{75\}, \{80\}\}$.
- Enumerate the 34 orbits of size 2 in increasing order of their smallest element as $O_2 = \{\{1, 69\}, \{2, 53\}, \{3, 37\}, \{4, 21\}, \{6, 74\}, \{7, 58\}, \{8, 42\}, \{9, 26\}, \{11, 79\}, \{12, 63\}, \{13, 47\}, \{14, 31\}, \{16, 84\}, \{17, 68\}, \{18, 52\}, \{19, 36], \{22, 73], \{23, 57\}, \{24, 41\}, \{27, 78\}, \{28, 62\}, \{29, 46\}, \{32, 83\}, \{33, 67\}, \{34, 51\}, \{38, 72\}, \{39, 56\}, \{43, 77\}, \{44, 61\}, \{48, 82\}, \{49, 66\}, \{54, 71\}, \{59, 76\}, \{64, 81\}\}$.
- Make the block of size 42 of the indices of the positions of the -1 elements in $\mathbf{a}$, by combining 12 elements of O_1 whose indices are given by $\mathbf{a}_{\text{ones}}$ and 15 elements of O_2 whose indices are given by $\mathbf{a}_{\text{twos}}$. This yields the following $\mathbf{a}$-block of size 42: $\{5, 10, 15, 20, 25, 30, 35, 40, 45, 50, 70, 75, 3, 37, 4, 21, 6, 74, 8, 42, 12, 63, 13, 47, 29, 46, 33, 67, 34, 51, 39, 56, 43, 77, 44, 61, 48, 82, 49, 66, 64, 81\}$.
- Make the block of size 42 of the indices of the positions of the -1 elements in $\mathbf{b}$, by combining 12 elements of O_1 whose indices are given by $\mathbf{b}_{\text{ones}}$ and 15 elements of O_2 whose indices are given by $\mathbf{b}_{\text{twos}}$. This yields the following $\mathbf{b}$-block of size 42: $\{5, 10, 15, 20, 25, 30, 35, 40, 50, 55, 70, 75, 2, 53, 9, 26, 12, 63, 13, 47, 14, 31, 18, 52, 24, 41, 28, 62, 32, 83, 34, 51, 38, 72, 43, 77, 44, 61, 59, 76, 64, 81\}$.
- The above $\mathbf{a}$-block and $\mathbf{b}$-block (both of size 42) yield an LP for $\ell = 85$.

For the first LP $(\mathbf{a}, \mathbf{b})$ of length $\ell = 85$ shown above, the 17-compressions are

$$\mathcal{A}_{17} = [1, 3, 3, 1, -7], \ \ \mathcal{B}_{17} = [3, 1, 1, 3, -7].$$

These possess the properties required by Proposition 2. That is,

$$\text{PAF}_{\mathcal{A}_{17}}(0) = \text{PAF}_{\mathcal{B}_{17}}(0) = 4 \cdot 17 + 1 = 69.$$

As a consequence, the coefficients of $\sqrt{5}$ in $\mathrm{PSD}_{\mathbf{a}}(17r)$ and $\mathrm{PSD}_{\mathbf{b}}(17r)$ cancel out for $r = 1, \ldots, 4$. Specifically,

$$\mathrm{PSD}_{\mathbf{a}}(17r) = 85 + 1 + (-1)^{\lfloor \frac{r}{2} \rfloor}\sqrt{5} \cdot 18$$

$$\mathrm{PSD}_{\mathbf{b}}(17r) = 85 + 1 - (-1)^{\lfloor \frac{r}{2} \rfloor}\sqrt{5} \cdot 18.$$

Remark 1. *We did not use Conjecture 1 or Corollary 6 in our search for an LP of length* 85 *because neither Conjecture 1 nor Corollary 6 had been formulated when we implemented our search. However, the LP we found happened to satisfy equations (12) in Conjecture 1.*

3.2 LPs of length $\ell = 87$

Next, we describe our search method for LPs $(\mathbf{a}, \mathbf{b})$ of length $\ell = 87$. First we need the following theorem which is a special case of Theorem 3 in [2].

Theorem 5. *Let* $(\mathbf{a}, \mathbf{b})$ *be an LP of length* $\ell = dm$. *Then the* m*-compressed vectors* $(\mathcal{A}_m, \mathcal{B}_m)$ *satisfy*

$$\mathrm{PAF}_{\mathcal{A}_m}(0) + \mathrm{PAF}_{\mathcal{B}_m}(0) = 2\ell - 2\left(\frac{\ell}{d} - 1\right) = 2\ell + 2 - \frac{2\ell}{d},$$

$$\mathrm{PAF}_{\mathcal{A}_m}(j) + \mathrm{PAF}_{\mathcal{B}_m}(j) = -\frac{2\ell}{d}, \quad \forall j \in \mathbb{Z}_d - \{0\}.$$

By Theorem 5, the 3-compressed vectors $(\mathcal{A}_3, \mathcal{B}_3)$ of an LP $(\mathbf{a}, \mathbf{b})$ of length $\ell = 87$ must contain 14 elements with absolute value equal to 3 and $2 \cdot 29 - 14 = 44$ elements with absolute value equal to 1. Experimental evidence from the study of other lengths which are divisible by 3 indicates that $\mathcal{A}_3$ and $\mathcal{B}_3$ which have an equal number of elements with absolute value equal to 3 are more likely to yield LPs. Hence, we computed approximately six thousand candidate 3-compressions satisfying the following constraints.

1. The vectors $\mathcal{A}_3, \mathcal{B}_3 \in \{-3, -1, +1, +3\}^{29}$ contain 14 elements with absolute value equal to 3 and 44 elements with absolute value equal to 1.

2. $\mathrm{PAF}_{\mathcal{A}_3}(s) + \mathrm{PAF}_{\mathcal{B}_3}(s) = (-2) \cdot 3 = -6$ for $s = 1, \ldots, 28$.

3. $\mathrm{PSD}_{\mathcal{A}_3}(s) + \mathrm{PSD}_{\mathcal{B}_3}(s) = 2\ell + 2 = 2 \cdot 87 + 2 = 176$ for $s = 1, \ldots, 28$.

4. $\sum_{i=0}^{28} A_i = \sum_{i=0}^{28} B_i = 1$.

5. Each of $\mathcal{A}_3$ and $\mathcal{B}_3$ contains 7 elements with absolute value equal to 3 and 22 elements with absolute value equal to 1.

Among the above constraints, only constraint 5 is not necessary for a length 87 LP to exist. However, imposing constraint 5 was essential in greatly reducing the search space to a part where solutions are most likely to exist. Subsequently, we ran our `C` 3-uncompression code for approximately two thousand candidate 3-compressions and discovered the following two LPs of order $\ell = 87$:

$$
\begin{aligned}
\mathbf{a} = [&-1,-1,-1,-1,1,-1,-1,-1,1,1,-1,1,-1,1,-1,1,1,-1,-1,1,1,-1,-1,1,-1,1,-1,1,1,\\
&-1,-1,1,1,1,-1,-1,-1,-1,-1,1,-1,-1,1,-1,-1,-1,1,1,1,1,-1,-1,-1,1,-1,1,1,\\
&1,-1,1,1,-1,-1,-1,-1,1,1,1,1,1,1,-1,-1,1,1,1,-1,1,1,1,1,1,-1,1,-1,1,-1],\\
\mathbf{b} = [&-1,-1,-1,-1,-1,-1,-1,-1,1,1,1,1,-1,1,1,-1,1,1,-1,1,-1,1,1,1,1,-1,-1,1,1,\\
&-1,1,1,-1,1,-1,-1,1,-1,-1,1,1,1,-1,1,-1,1,1,-1,-1,1,-1,-1,1,1,1,1,1,-1,-1,\\
&-1,1,1,1,-1,-1,1,-1,1,-1,-1,1,-1,1,-1,-1,-1,1,-1,-1,1,1,1,-1,1,-1,1,-1],\\
\mathbf{a} = [&-1,-1,-1,-1,1,-1,-1,-1,1,1,1,1,1,1,-1,1,-1,-1,-1,1,1,1,-1,1,-1,-1,-1,1,\\
&1,-1,-1,1,1,1,-1,-1,-1,1,-1,-1,1,-1,1,-1,-1,1,1,1,1,1,-1,-1,1,1,1,-1,1,1,-1,\\
&1,1,-1,-1,-1,-1,1,-1,1,1,-1,-1,-1,-1,1,1,1,-1,1,1,-1,1,-1,-1,1,1,1,-1],\\
\mathbf{b} = [&-1,1,-1,1,1,-1,-1,1,1,1,1,1,1,-1,1,-1,1,1,1,-1,-1,1,-1,1,-1,1,-1,1,-1,\\
&-1,-1,1,-1,-1,-1,-1,-1,-1,-1,1,-1,1,1,1,-1,1,-1,-1,1,-1,-1,1,1,1,-1,-1,\\
&1,1,-1,-1,1,-1,1,-1,-1,1,-1,1,-1,1,-1,-1,1,-1,-1,1,-1,-1,1,1,1,1,1,1,1,1,-1].
\end{aligned}
$$

Both of the above LPs of length $\ell = 87$ 3-compress to

$$
\begin{aligned}
\mathcal{A}_3 &= [-3,-1,1,-1,1,-3,-3,-1,1,1,1,1,-1,1,-3,1,1,1,-1,3,3,-1,-1,1,-1,1,-1,3,1],\\
\mathcal{B}_3 &= [-3,-1,1,-1,1,-3,-3,1,-1,1,1,1,1,-1,3,-3,1,1,-1,-1,-1,1,1,3,1,1,-1,3,-1].
\end{aligned}
$$

There are seven ± 3s in each of the two vectors $\mathcal{A}_3$ and $\mathcal{B}_3$, and this "balanced" configuration yields LPs of length $\ell = 87$. Based on the analysis at the beginning of this section, we can make the following claim.

Claim 1. *Without imposing constraint 5, a successful outcome of our search for a length 87 LP would not have been possible.*

4 Searching for LPs of length $\ell = 115$

By using Corollary 1, two non-exhaustive searches for an LP $(\boldsymbol{a}, \boldsymbol{b})$ of length 115 with multiplier groups $\widehat{G}_{\boldsymbol{a}}$ and $\widehat{G}_{\boldsymbol{b}}$ both containing the subgroup $\{1, 91\}$ were performed. The first search was done before Conjecture 1 was formulated, hence it did not use it. For the first search, the combinations of 0 cosets of size 1 and 29 cosets of size 2 were considered, yielding a search space of size $\binom{4}{0} \cdot \binom{55}{29} = 3{,}560{,}597{,}348{,}629{,}860$. The computation was aborted after almost 4% of the search space were traversed. This took about $4,359$ days of CPU time, and the output files took up 76 GB of disk space. The second search was done with the implementation of Conjecture 1. This time, combinations of 4 cosets of size 1 and 27 cosets of size 2 were considered, yielding a search space of size $\binom{4}{4} \cdot \binom{55}{27} =$ 3,824,345,300,380,220. This computation was aborted after 3,436 CPU days, when slightly more than 10% of the search space was traversed. The output files occupied about 64 GB of disk space. For both of the searches, the same PSD test in Section 4 of [5] without checking if the PSD value at $\ell/3$ is from a finite list of candidates, was implemented. Both searches used the same method as in Section 4 of [5] to identify LPs among vectors that passed the PSD test. The comparison of the two partial searches shows the significant gain (both time-wise and space-wise) that is obtained from implementing Conjecture 1. Neither the first, nor the second search yielded an LP of length 115. Both of the searches were done on 64 compute nodes, each with two 8-core Intel Haswell CPUs (Xeon E5-2630v3, 2.4Ghz) and 128 GB RAM.

5 Conclusion and future research

Recently, LPs of length 77 were found in [10], and lengths $117, 129, 133, 147$ were found in [5] for the first time. In this paper, we find LPs of (the previously open) lengths $85, 87$. This reduces the list of integers less than 200 for which the existence of LPs problem remains open to the following ten values:

$$115, 145, 159, 161, 169, 175, 177, 185, 187, 195.$$

An LP $(\mathbf{a}, \mathbf{b})$ as defined in this article corresponds to a difference family in $\mathbb{Z}_\ell$ [1]. In [3], previously known theory to search for difference families in $\mathbb{Z}_\ell$ was generalized to search for difference families in finite abelian groups. A possible direction for future research is generalizing the theory in this paper to difference families in finite abelian groups, i.e., by the structure theorem of finite abelian groups, groups of the form $\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_m}$, where d_i divides d_{i+1} for $i = 1, \ldots, m-1$, and $d_m \equiv 0 \pmod 5$.

Acknowledgments

The views expressed in this article are those of the authors, and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the U.S. Government. Christoph Koutschan was supported by the Austrian Science Fund (FWF): F5011-N15. The authors thank three referees for carefully reading the paper and providing comments that significantly improved the paper.

Data Deposition Information: No data sets have been used.

References

[1] K. T. Arasu, D. A. Bulutoglu, and J. Hollon. Legendre G-array pairs and the theoretical unification of several G-array families. *J. Comb. Des.*, 28(11):814–841, 2020.

[2] D. Z. Djokovic and I. S. Kotsireas. Compression of periodic complementary sequences and applications. *Des. Codes Cryptogr.*, 74(2):365–377, 2015.

[3] D. Z. Djokovic and I. S. Kotsireas. Computational methods for difference families in finite abelian groups. *Spec. Matrices*, 7:127–141, 2019.

[4] R. J. Fletcher, M. Gysin, and J. Seberry. Application of the discrete Fourier transform to the search for generalised Legendre pairs and Hadamard matrices. *Australas. J. Combin.*, 23:75–86, 2001.

[5] I. S. Kotsireas and C. Koutschan. Legendre pairs of lengths $\ell \equiv 0 \pmod 3$. *J. Comb. Des.*, 29(12):870–887, 2021.

[6] I. S. Kotsireas and A. Winterhorf. Quaternary Legendre pairs. pages 1–16. The fields institute for research in mathematical sciences, Totonto, ON, Canada, 2023.

[7] D. L. Kreher and D. R. Stinson. *Combinatorial Algorithms. Generation, Enumeration, and Search.* CRC Press, Taylor & Francis, Boca Raton, FL, 1st edition, 1998.

[8] J. J. Rotman. *Advanced Modern Algebra*, volume 180. American Mathematical Society, Providence, RI, 3rd edition, 2015. Part 2.

[9] J. S. Turner, D. A. Bulutoglu, D. Baczkowski, and A. J. Geyer. Counting the decimation classes of binary vectors with relatively prime length and density. *J. Algebr. Comb.*, 55:61–87, 2022.

[10] 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. *Des. Codes Cryptogr.*, 89(6):1321–1333, 2021.