Legendre pairs of lengths $\ell \equiv 0 \pmod 3$

Ilias Kotsireas* & Christoph Koutschan†

October 17, 2021

Abstract

We prove a proposition that connects constant-PAF sequences and the corresponding Legendre pairs with integer PSD values. We show how to determine explicitly the complete spectrum of the $(\ell/3)$-rd value of the discrete Fourier transform for Legendre pairs of lengths $\ell \equiv 0 \pmod 3$. This is accomplished by two new algorithms based on number-theoretic arguments. As an application, we prove that Legendre pairs of the open lengths 117, 129, 133, and 147 exist by finding Legendre pairs of these lengths with a multiplier group of order at least 3. As a consequence, 85, 87, 115, 145, 159, 161, 169, 175, 177, 185, 187, 195 are the twelve integers in the range < 200 for which the question of existence of Legendre pairs remains unsolved.

Keywords: Legendre pairs, Discrete Fourier Transform, Compression, Hadamard matrix

1 Introduction

Let A denote a finite sequence $A = [a_1, \ldots, a_\ell]$ of length ℓ.
The periodic autocorrelation function (PAF) of A at lag s is defined as

$$\mathrm{PAF}(A, s) = \sum_{i=1}^{\ell} a_i\, a_{i+s}, \quad \forall\ s = 0, \ldots, \ell - 1, \tag{1}$$

where $i + s$ is taken modulo ℓ, when $i + s > \ell$.

*Corresponding author. Supported by an NSERC grant.
†Supported by the Austrian Science Fund (FWF): F5011-N15.
This paper has been published in Journal of Combinatorial Designs 29:870–887, DOI: 10.1002/jcd.21806

The discrete Fourier transform (DFT) of A at lag s is defined as

$$\mathrm{DFT}(A,s)=\sum_{i=1}^{\ell} a_i\,\omega^{s\cdot(i-1)},\quad \forall\ s=1,\ldots,\ell, \tag{2}$$

where $\omega=\cos(2\pi/\ell)+i\sin(2\pi/\ell)$ is the primitive ℓ-th root of unity, that satisfies $\omega^\ell=1$. The power spectral density (PSD) of A at lag s is defined as

$$\mathrm{PSD}(A,s)=\left|\mathrm{DFT}(A,s)\right|^2=\Re(\mathrm{DFT}(A,s))^2+\Im(\mathrm{DFT}(A,s))^2,\quad \forall\ s=1,\ldots,\ell \tag{3}$$

i.e., the PSD values are defined as the sum of squares of the real and imaginary parts of the DFT values.

Let ℓ be an odd positive integer. Two sequences $A=[a_1,\ldots,a_\ell]$ and $B=[b_1,\ldots,b_\ell]$ of length ℓ and consisting of elements from $\{-1,+1\}$, such that $a_1+\ldots+a_\ell=b_1+\ldots+b_\ell=\pm1$ form a Legendre pair of length ℓ if

$$\mathrm{PAF}(A,s)+\mathrm{PAF}(B,s)=-2,\quad \forall\ s=1,\ldots,\frac{\ell-1}{2}. \tag{4}$$

In the context of Legendre pairs, we typically work with the sole assumption that $a_1+\ldots+a_\ell=1$ and $b_1+\ldots+b_\ell=1$, without loss of generality. It is well-known, see [3], that if (A,B) form a Legendre pair of length ℓ, then we have

$$\mathrm{PSD}(A,s)+\mathrm{PSD}(B,s)=2\ell+2,\quad \forall\ s=1,\ldots,\frac{\ell-1}{2}. \tag{5}$$

The paper [3] is fundamental in the study of Legendre pairs, as it initiated the use of the PSD criterion, in the search for Legendre pairs. More specifically, the PSD criterion asserts that if, in the course of a search algorithm, an index i in the range $1,\ldots,(\ell-1)/2$ is detected, such that $\mathrm{PSD}(A,i)>2\ell+2$, then the corresponding (candidate) sequence A can be discarded from the search, because it is unsuitable to form a Legendre pair. This is due to the fact that the PSD values are always non-negative, as sums of norm squares. Given a Legendre pair of length ℓ, one can construct a Hadamard matrix of order $2\ell+2$, using a two circulant core template array found in [3].

Throughout this paper, we use the notation $\mathbb{Z}_\ell^\star$ to denote the multiplicative group $\{j\in\mathbb{Z}_\ell\mid \gcd(j,\ell)=1\}$. Let $I\subseteq\mathbb{Z}_\ell$, then an element $t\in\mathbb{Z}_\ell^\star$ is called a multiplier of I if there exists $g\in\mathbb{Z}_\ell$ such that

$$t\cdot I=I+g,$$

where $I+g:=\{i+g\mid i\in I\}$ and analogously for $t\cdot I$. We say that t is a multiplier for a sequence $A=[a_1,\ldots,a_\ell]\in\{-1,+1\}^\ell$ if it is a multiplier of $I:=\{i\in\mathbb{Z}_\ell\mid a_i=1\}$.

See [9] for more details. In this paper, we restrict our searches for Legendre pairs to sequences whose group of multipliers contains a prespecified subgroup of $\mathbb{Z}_\ell^\star$, also known as the union-of-orbits approach. In most instances considered here, we specify a subgroup of size 3, so that the search space is neither too restrictive causing no Legendre pairs to be found, nor too large causing the algorithm to get stuck in parts of the search space that contain no Legendre pairs given the current computational resources.

The rest of the paper is organized as follows. In Section 2, we present some theoretical results on the possible PSD values of sequences in Legendre pairs, under the assumption that their length ℓ is divisible by 3. These results are then exploited in Section 4, where we use them as additional filter criteria in order to speed up our exhaustive searches for Legendre pairs. With the help of considerable computational resources, we succeeded to find Legendre pairs of lengths $\ell = 117$, $\ell = 129$, and $\ell = 147$. It was unknown until now whether Legendre pairs of these lengths existed or not (see Sections 4.1 – 4.3). As an encore, in Section 4.4 we hint at the possibility of extending our ideas to lengths ℓ that are not necessarily divisible by 3 but by some other small prime, and for the first time present some examples of Legendre pairs of length $\ell = 133$.

2 Legendre pairs of length $\ell \equiv 0 \pmod 3$

Consider (A, B) a Legendre pair of length ℓ such that $\ell \equiv 0 \pmod 3$ and set $m = \ell/3$. The following lemma is proved in [4]

Lemma 1. *Let ℓ be an odd integer such that $\ell \equiv 0 \pmod 3$ and let $m = \ell/3$. Let $A = [a_1, \ldots, a_\ell]$ be a $\{-1, +1\}$-sequence. Then*

$$\mathrm{DFT}(A, m) = \left(A_1 - \frac{1}{2}A_2 - \frac{1}{2}A_3\right) + \left(\frac{\sqrt{3}}{2}A_2 - \frac{\sqrt{3}}{2}A_3\right) i,$$

$$\mathrm{PSD}(A, m) = A_1^2 + A_2^2 + A_3^2 - A_1A_2 - A_1A_3 - A_2A_3,$$

where

$$A_1 = \sum_{i=0}^{m-1} a_{3i+1}, \quad A_2 = \sum_{i=0}^{m-1} a_{3i+2}, \quad A_3 = \sum_{i=0}^{m-1} a_{3i+3}.$$

The proof of Lemma 1 is based on the exact evaluation of the roots of the cyclotomic polynomial of degree 3.

Let $\mathcal{A} = \{a_1, \ldots, a_\ell\}$, and

$$e_2(\mathcal{A}) = \sum_{i<j} a_i a_j$$

denote the second elementary symmetric function on $\mathcal{A}$. Let

$$p_1(\mathcal{A}) = \sum_{i=1}^{\ell} a_i \quad \text{and} \quad p_2(\mathcal{A}) = \sum_{i=1}^{\ell} a_i^2$$

denote the first and second power sums on $\mathcal{A}$. The following special case of the Jacobi-Trudi identity

$$e_2(\mathcal{A}) = \frac{p_1(\mathcal{A})^2}{2} - \frac{p_2(\mathcal{A})}{2} \tag{6}$$

can be found in [7].

Applying Lemma 1 to a Legendre pair (A, B) of length ℓ such that $\ell \equiv 0 \pmod 3$, we obtain the following:

Corollary 1. *If $\ell \equiv 0 \pmod 3$, $m = \ell/3$, and if the two $\{-1, +1\}$-sequences $A = [a_1, \ldots, a_\ell]$ and $B = [b_1, \ldots, b_\ell]$ form a Legendre pair of length ℓ, then*

$$\begin{cases} \mathrm{PSD}(A, m) = \dfrac{3}{2}\left(A_1^2 + A_2^2 + A_3^2\right) - \dfrac{1}{2} \\ \\ \mathrm{PSD}(B, m) = \dfrac{3}{2}\left(B_1^2 + B_2^2 + B_3^2\right) - \dfrac{1}{2} \end{cases} \tag{7}$$

$$A_1^2 + A_2^2 + A_3^2 + B_1^2 + B_2^2 + B_3^2 = 4m + 2 \tag{8}$$

where

$$A_1 = \sum_{i=0}^{m-1} a_{3i+1}, \quad A_2 = \sum_{i=0}^{m-1} a_{3i+2}, \quad A_3 = \sum_{i=0}^{m-1} a_{3i+3},$$

$$B_1 = \sum_{i=0}^{m-1} b_{3i+1}, \quad B_2 = \sum_{i=0}^{m-1} b_{3i+2}, \quad B_3 = \sum_{i=0}^{m-1} b_{3i+3}.$$

Proof. Applying Lemma 1 to the sequences A, B separately we obtain

$$\mathrm{PSD}(A,m) = A_1^2 + A_2^2 + A_3^2 - \underbrace{(A_1A_2 + A_1A_3 + A_2A_3)}_{e_2(A_1,A_2,A_3)},$$
$$\mathrm{PSD}(B,m) = B_1^2 + B_2^2 + B_3^2 - \underbrace{(B_1B_2 + B_1B_3 + B_2B_3)}_{e_2(B_1,B_2,B_3)}.$$

The second elementary symmetric functions $e_2(A_1, A_2, A_3)$ and $e_2(B_1, B_2, B_3)$ are related to the first elementary symmetric functions $e_1(A_1, A_2, A_3)$ and $e_1(B_1, B_2, B_3)$ via the special case of the Jacobi-Trudi identity (6). We also know that $e_1(A_1, A_2, A_3) = A_1 + A_2 + A_3 = 1$ and $e_1(B_1, B_2, B_3) = B_1 + B_2 + B_3 = 1$. Therefore we obtain (7), and

$$\begin{aligned} A_1^2 + A_2^2 + A_3^2 + B_1^2 + B_2^2 + B_3^2 &= \frac{2\,\mathrm{PSD}(A,m)+1}{3} + \frac{2\,\mathrm{PSD}(B,m)+1}{3} \\ &= \frac{2(2\ell+2)+2}{3} = \frac{4\ell+6}{3} = 4m+2. \end{aligned} \qquad \blacksquare$$

In the sequel, we denote $\mathrm{PSD}(A,m)$ by $\widehat{A}_m$ and $\mathrm{PSD}(B,m)$ by $\widehat{B}_m$.

Corollary 1 can be used to derive additional decoupled constraints (i.e., involving A_i and B_i separately) based on (8). From (5) we know:

$$\widehat{A}_m + \widehat{B}_m = 2\ell + 2. \tag{9}$$

Moreover, from (7) we obtain:

$$A_1^2 + A_2^2 + A_3^2 = \frac{2\widehat{A}_m + 1}{3} \quad \text{and} \quad B_1^2 + B_2^2 + B_3^2 = \frac{2\widehat{B}_m + 1}{3}. \tag{10}$$

Since both these sums of three odd integer squares are integers, we obtain that $2\widehat{A}_m + 1 \equiv 9 \pmod{24}$ and $2\widehat{B}_m + 1 \equiv 9 \pmod{24}$ i.e. $\widehat{A}_m \equiv 4 \pmod{12}$ and $\widehat{B}_m \equiv 4 \pmod{12}$. Therefore, the set of possible pairs of values $\left[\widehat{A}_m, \widehat{B}_m\right]$ can be restricted considerably. In addition, a possible pair of values $\left[\widehat{A}_m, \widehat{B}_m\right]$ has to be compatible with the linear constraints

$$A_1 + A_2 + A_3 = 1 \quad \text{and} \quad B_1 + B_2 + B_3 = 1. \tag{11}$$

For a Legendre pair (A, B) of length ℓ, we must have that $A_1, A_2, A_3, B_1, B_2, B_3$ are all odd. For given fixed values of $\widehat{A}_m$, $\widehat{B}_m$, equations (10) can be solved independently as sums-of-squares Diophantine equations and typically have anywhere from 1 to 5 all-odd solutions (up to sign), for the right-hand-side values that arise in the context of

Legendre pairs of lengths $\ell < 200$. These solutions give possible triplets of values for (A_1, A_2, A_3) and (B_1, B_2, B_3) that must be compatible with the linear constraints (11). The above discussion suffices to formulate an algorithm for determining explicitly the complete spectrum of the $(\ell/3)$-rd PSD values for any Legendre pair of length ℓ divisible by three. We outline this algorithm below.

Algorithm 1: Determination of the spectrum $\mathcal{S}$

Input: An odd positive integer $\ell = 3 \cdot m$;
Initialization: $\mathcal{S} = \{\}$;
for $s = 0, \ldots, \lfloor (\ell - 1)/6 \rfloor$ **do**
  (1) form the candidate $\left[\widehat{A}_m, \widehat{B}_m\right]$ pair $[12s + 4, 2\ell + 2 - (12s + 4)]$;
  (2) compute the values of $A_1^2 + A_2^2 + A_3^2$ and $B_1^2 + B_2^2 + B_3^2$ using (10) ;
  (3) solve (up to sign) the two sum-of-squares Diophantine equations

$$A_1^2 + A_2^2 + A_3^2 = \frac{2(12s + 4) + 1}{3},$$

$$B_1^2 + B_2^2 + B_3^2 = \frac{2(2\ell + 2 - (12s + 4)) + 1}{3} \;;$$

  if *there are all-odd solutions of these two Diophantine equations, compatible with the linear constraints (11)* **then**
    insert the pair $[12s + 4, 2\ell + 2 - (12s + 4)]$ in $\mathcal{S}$, as an element of the spectrum of $\left[\widehat{A}_m, \widehat{B}_m\right]$;
  else
    discard the pair $[12s + 4, 2\ell + 2 - (12s + 4)]$ as it cannot be an element of the spectrum of $\left[\widehat{A}_m, \widehat{B}_m\right]$;
  end
end
Output: the spectrum $\mathcal{S}$ of pairs of values $\left[\widehat{A}_m, \widehat{B}_m\right]$ for Legendre pairs (A, B) of length $\ell = 3 \cdot m$;

Example 1. *We illustrate Algorithm 1 with the case $\ell = 117 = 3 \cdot 39$, i.e., $m = 39$. First, we have $\widehat{A}_m + \widehat{B}_m = 2 \cdot 117 + 2 = 236$ and in addition $\widehat{A}_m \equiv 4 \pmod{12}$ and $\widehat{B}_m \equiv 4 \pmod{12}$. Given that every pair of values $\left[\widehat{A}_m, \widehat{B}_m\right]$ determines the values of $A_1^2 + A_2^2 + A_3^2$ and $B_1^2 + B_2^2 + B_3^2$ via (10), we obtain Table 1. The first row of Table 1 indicates a reason why a certain $\left[\widehat{A}_m, \widehat{B}_m\right]$ combination can be discarded. The last three rows of Table 1 indicate the only three $\left[\widehat{A}_m, \widehat{B}_m\right]$ combinations that can possibly hold. The remaining rows of the table corresponding to all other $\left[\widehat{A}_m, \widehat{B}_m\right]$ combinations are omitted.*

$\left[\widehat{A}_m, \widehat{B}_m\right]$	
$(4, 232)$	$A_1^2 + A_2^2 + A_3^2 = 3, \rightsquigarrow [1, 1, 1]$ $B_1^2 + B_2^2 + B_3^2 = 155, \rightsquigarrow [3, 5, 11], [5, 7, 9] \rightsquigarrow$ no compatible assignments
$(28, 208)$	$A_1^2 + A_2^2 + A_3^2 = 19, \rightsquigarrow [1, 3, 3]$ $B_1^2 + B_2^2 + B_3^2 = 139, \rightsquigarrow [3, 3, 11], [3, 7, 9]$ compatible assignments: $(A_1, A_2, A_3) = (1, -3, 3), (B_1, B_2, B_3) = (3, 7, -9)$
$(64, 172)$	$A_1^2 + A_2^2 + A_3^2 = 43, \rightsquigarrow [3, 3, 5]$ $B_1^2 + B_2^2 + B_3^2 = 115, \rightsquigarrow [3, 5, 9]$ compatible assignments: $(A_1, A_2, A_3) = (3, 3, -5), (B_1, B_2, B_3) = (-3, -5, 9)$
$(112, 124)$	$A_1^2 + A_2^2 + A_3^2 = 75, \rightsquigarrow [1, 5, 7], [5, 5, 5]$ $B_1^2 + B_2^2 + B_3^2 = 83, \rightsquigarrow [1, 1, 9], [3, 5, 7]$ compatible assignments: $(A_1, A_2, A_3) = (-1, -5, 7), (B_1, B_2, B_3) = (3, 5, -7)$

Table 1: Some computations using Algorithm 1 for the spectrum of $\left[\widehat{A}_m, \widehat{B}_m\right]$ for $m = 39$.

The omitted rows do not lead to compatible assignments for A_1, A_2, A_3 and/or B_1, B_2, B_3. Only 3 pairs of values are not ruled out to occur in Legendre pairs of length 117. This allows us to add an additional layer of parallelism when searching for such Legendre pairs.

If H is a subgroup of $\mathbb{Z}_\ell^\star$ of size 3, then H is cyclic and all of its elements must be $1 \pmod 3$. Moreover, if H is a subgroup of $\mathbb{Z}_\ell^\star$ with all its members equal to $1 \pmod 3$, then each orbit of H consists of elements that are equal to each other $\pmod 3$. The consequence is that each orbit contributes to exactly one of the three quantities A_1, A_2, A_3 that were defined in Lemma 1. We can exploit this observation to further confine the potential values for $\widehat{A}_m$ and $\widehat{B}_m$. The following algorithm is formulated under the assumption that the chosen orbits indicate the positions of the $+1$'s, but since $\widehat{A}_m$ is a sum-of-squares in the A_i, it works also in situations where the chosen orbits mark the positions of the -1's.

Algorithm 2: Determination of PSD values $\widehat{A}_m$ compatible with the H orbits

Input: An odd positive integer $\ell = 3 \cdot m$, a subgroup H of $\mathbb{Z}_\ell^\star$ s.t. $h \equiv 1 \pmod 3$ for all $h \in H$, and non-negative integers $c_1, \ldots, c_t$ indicating the number of chosen orbits of sizes $s_1, \ldots, s_t$, respectively ;

for $i = 1, \ldots, t$ **do**
  for $j \in \{0, 1, 2\}$ **do**
    $n_{i,j}$ = number of orbits of size s_i with elements $\equiv j \pmod 3$;
  end
end

$$T = \big\{(k_{1,1}, \ldots, k_{t,1}, k_{1,2}, \ldots, k_{t,2}) \;\big|\; 0 \le k_{1,1} \le \min\{c_1, n_{1,1}\}, \ldots, 0 \le k_{t,1} \le \min\{c_t, n_{t,1}\}, 0 \le k_{1,2} \le \min\{c_1, n_{1,2}\}, \ldots, 0 \le k_{t,2} \le \min\{c_t, n_{t,2}\}, 0 \le c_1 - k_{1,1} - k_{1,2} \le n_{1,0}, \ldots, 0 \le c_t - k_{t,1} - k_{t,2} \le n_{t,0}\big\} ;$$

$\mathcal{C} = \{\}$;

for $(k_{1,1}, \ldots, k_{t,1}, k_{1,2}, \ldots, k_{t,2}) \in T$ **do**
  $A_1 = -m + 2 \cdot \sum_{i=1}^t s_i \cdot k_{i,1}$;
  $A_2 = -m + 2 \cdot \sum_{i=1}^t s_i \cdot k_{i,2}$;
  $A_3 = -m + 2 \cdot \sum_{i=1}^t s_i \cdot (c_i - k_{i,1} - k_{i,2})$;
  $P = A_1^2 + A_2^2 + A_3^2 - A_1A_2 - A_1A_3 - A_2A_3$;
  $\mathcal{C} = \mathcal{C} \cup \{P\}$;
end

Output: the set $\mathcal{C}$ of potential values for $\widehat{A}_m$ that are compatible with the choice of $c_1, \ldots, c_t$ orbits of H ;

Example 2. *Continuing Example 1 for $\ell = 117$, we apply Algorithm 2 in order to show that $\big[\widehat{A}_{39}, \widehat{B}_{39}\big] = [112, 124]$ cannot appear when we employ the subgroup $H_1 = \{1, 16, 22\}$ for conducting a search with the orbits method. The subgroup H_1 induces 2 orbits of size $s_1 = 1$, and 38 orbits of size $s_2 = 3$. For such a search one may choose $c_1 = 2$ orbits of size 1 and $c_2 = 19$ orbits of size 3. By looking at the orbits (they are listed explicitly below in Section 4.1.1), we find $n_{2,0} = 12$ orbits whose elements are divisible by 3, and similarly $n_{2,1} = n_{2,2} = 13$. Moreover, $n_{1,0} = 2$ and $n_{1,1} = n_{1,2} = 0$, which eventually implies $k_{1,1} = k_{1,2} = 0$. Let $k_{2,1}$ (resp. $k_{2,2}$) denote the number of chosen 3-orbits whose elements are $1 \pmod 3$ (resp. $2 \pmod 3$). Then we obtain*

$$A_1 = 6 \cdot k_{2,1} - 39, \quad A_2 = 6 \cdot k_{2,2} - 39, \quad A_3 = 2 \cdot 2 + 6 \cdot (19 - k_{2,1} - k_{2,2}) - 39.$$

Letting $k_{2,1}$ and $k_{2,2}$ range over all admissible values, i.e.,

$$0 \le k_{2,1} \le 13 \ \wedge\ 0 \le k_{2,2} \le 13 \ \wedge\ 0 \le 19 - k_{2,1} - k_{2,2} \le 12,$$

we get all possible values for A_1, A_2, A_3 and determine the potential values

$$\widehat{A}_{39} = \mathrm{PSD}(A, 39) = A_1^2 + A_2^2 + A_3^2 - A_1A_2 - A_1A_3 - A_2A_3.$$

to be

$$28,\ 64,\ 100,\ 172,\ 208,\ 244,\ 316,\ 388,\ 496, \ldots, 4132,\ 4348,\ 4564.$$

This list excludes the possibility of finding a Legendre pair with $\left[\widehat{A}_{39}, \widehat{B}_{39}\right] = [112, 124]$. Note that this result does not change if we set $c_1 = 1$ and $c_2 = 19$ (a situation where the chosen orbits indicate the positions of the -1's).

3 Compression and constant-PAF sequences

The term "constant-PAF sequences" is taken to mean sequences all of whose PAF values are equal to the same constant. We refer the reader to [2] for the definition and properties of compression of Legendre pairs. It has been observed experimentally in the current paper, as well as in [10], that some Legendre pairs of composite length $\ell = n \cdot m$ have the properties that:

- their m-compression is made up from two constant-PAF sequences of length n
- some of the PSD values of the resulting Legendre pairs of length ℓ are integers.

In this section, we prove a proposition that elucidates the connection between these two aforementioned facts.

Proposition 1. *Let $A = [a_1, \ldots, a_\ell]$ and $B = [b_1, \ldots, b_\ell]$ be a Legendre pair of composite length $\ell = n \cdot m$. Let $\mathcal{A} = [A_1, \ldots, A_n]$, $\mathcal{B} = [B_1, \ldots, B_n]$, where*

$$A_j = \sum_{i=0}^{m-1} a_{ni+j} \quad \text{and} \quad B_j = \sum_{i=0}^{m-1} b_{ni+j}$$

for $j = 1, \ldots, n$, i.e. $(\mathcal{A}, \mathcal{B})$ is the m-compression of (A, B).
If the m-compression of (A, B) is made up from two constant-PAF sequences of length n:

$$\mathrm{PAF}(\mathcal{A}, 1) = \mathrm{PAF}(\mathcal{A}, 2) = \cdots = \mathrm{PAF}(\mathcal{A}, \frac{n-1}{2})$$

$$\mathrm{PAF}(\mathcal{B}, 1) = \mathrm{PAF}(\mathcal{B}, 2) = \cdots = \mathrm{PAF}(\mathcal{B}, \frac{n-1}{2})$$

(where $\mathrm{PAF}(\mathcal{A},1)+\mathrm{PAF}(\mathcal{B},1)=(-2)\cdot m$*), then the PSD values at integer multiples of* m *of* A *and* B *are integers, with the explicit evaluations*

$$\mathrm{PSD}(A,m\cdot s)=p_2(\mathcal{A})-\mathrm{PAF}(\mathcal{A},1),\quad s=1,2,\ldots,\frac{n-1}{2}$$

$$\mathrm{PSD}(B,m\cdot s)=p_2(\mathcal{B})-\mathrm{PAF}(\mathcal{B},1),\quad s=1,2,\ldots,\frac{n-1}{2}$$

(where $\mathrm{PSD}(A,m\cdot s)+\mathrm{PSD}(B,m\cdot s)=2\cdot\ell+2$*).*

Proof. We use the fact that the PSD remains invariant under m-compression, see [2]. We also use the Wiener-Khinchin theorem, see [3], that states that the PSD of a sequence is equal to the DFT of its periodic autocorrelation function. We also use the fact that certain sums of roots of unity vanish identically. For every $s=1,2,\ldots,(n-1)/2$ and ω the primitive n-th root of unity we have:

$$\begin{aligned}\mathrm{PSD}(A,m\cdot s) &= \mathrm{PSD}(\mathcal{A},s)\\ &= \sum_{j=0}^{n-1}\mathrm{PAF}(\mathcal{A},j)\,\omega^{js}\\ &= \mathrm{PAF}(\mathcal{A},0)+\mathrm{PAF}(\mathcal{A},1)\left(\sum_{j=1}^{n-1}\omega^{js}\right)\\ &= p_2(\mathcal{A})-\mathrm{PAF}(\mathcal{A},1).\end{aligned}$$

The assertion $\mathrm{PSD}(B,m\cdot s)=p_2(\mathcal{B})-\mathrm{PAF}(\mathcal{B},1)$ is proved in a completely analogous manner. ■

We remark that the roles of n and m in Proposition 1 are not interchangeable. Proposition 1 will be illustrated in the next section.

4 Computational results

We have implemented the systematic traversal of the search space in the `C` language, gaining (not surprisingly) a considerable speed-up compared to our prototype implementations in Maple and Mathematica. For each sequence A in the search space, we first apply Lemma 1 (provided that $\ell\equiv 0 \pmod 3$), by computing the sums A_1,A_2,A_3 and then $\mathrm{PSD}(A,\ell/3)$ in exact arithmetic. If a sequence passes this test (or if $\ell\not\equiv 0 \pmod 3$), our program continues with the full PSD test, i.e., it checks whether $\mathrm{PSD}(A,k)\le 2\ell+2$ for all $1\le k\le(\ell-1)/2$ (note that we can exploit early termination here). The DFT is computed in floating point arithmetic using double precision. For each sequence passing this second test, we write the two sequences $\big(\mathrm{PSD}(A,k)\big)_{k\in I}$ and $\big(2\ell+2-\mathrm{PSD}(A,k)\big)_{k\in I}$ with $I=\{1,\dots,(\ell-1)/2\}\setminus\{\ell/3\}$ into an output file. Since the PSD values are floating point numbers, we convert them to integers and, in order to save disk space, hash them modulo 16. The results are then saved as hexadecimal strings of length $|I|$. A Legendre pair corresponds to two lines in the output file whose two strings match pairwise (but in reverse order). Due to the hashing there is the possibility to find matches which do not correspond to Legendre pairs, but the probability that this happens is negligible and such false candidates can easily be sorted out in a post-processing step.

All times were measured on RICAM's computing cluster `radon1`, which has 1168 Xeon E5-2630v3 (2.4Ghz) threads. For the reported computations, we employed a moderate parallelization, typically using 16 threads for one task. Since the parallelization is done by splitting the search space into pieces, it scales very well. The reported times are given in CPU hours, i.e., as the sum of the times of each thread.

4.1 Legendre pairs of length 117

We executed Algorithm 1 for Legendre pairs of length $\ell=117=3\cdot 39$ and obtained

$$\big[\mathrm{PSD}(A,39),\mathrm{PSD}(B,39)\big]\in\big\{[28,208],[64,172],[112,124]\big\},$$

as in Example 1. There are four subgroups of order 3 in $\mathbb{Z}_{117}^{\star}$

$$H_1=\{1,16,22\},\quad H_2=\{1,40,79\},\quad H_3=\{1,55,100\},\quad H_4=\{1,61,94\}.$$

In the following subsections we investigate these subgroups separately, by considering only sequences whose multiplier group contains the respective subgroup.

4.1.1 Legendre pairs of length 117 via H_1

The subgroup $H_1=\{1,16,22\}$ of order 3 of $\mathbb{Z}_{117}^{\star}$ acts on $\mathbb{Z}_{117}$ and yields 38 orbits of size 3 and 2 orbits of size 1. We list the $38+2$ orbits of the action of $H_1=\{1,16,22\}$ on $\mathbb{Z}_{117}$

as follows:

$$
\begin{array}{lll}
H_1 \cdot 1 = \{1, 16, 22\}, & H_1 \cdot 2 = \{2, 32, 44\}, & H_1 \cdot 3 = \{3, 48, 66\}, \\
H_1 \cdot 4 = \{4, 64, 88\}, & H_1 \cdot 5 = \{5, 80, 110\}, & H_1 \cdot 6 = \{6, 15, 96\}, \\
H_1 \cdot 7 = \{7, 37, 112\}, & H_1 \cdot 8 = \{8, 11, 59\}, & H_1 \cdot 9 = \{9, 27, 81\}, \\
H_1 \cdot 10 = \{10, 43, 103\}, & H_1 \cdot 12 = \{12, 30, 75\}, & H_1 \cdot 13 = \{13, 52, 91\}, \\
H_1 \cdot 14 = \{14, 74, 107\}, & H_1 \cdot 17 = \{17, 23, 38\}, & H_1 \cdot 18 = \{18, 45, 54\}, \\
H_1 \cdot 19 = \{19, 67, 70\}, & H_1 \cdot 20 = \{20, 86, 89\}, & H_1 \cdot 21 = \{21, 102, 111\}, \\
H_1 \cdot 24 = \{24, 33, 60\}, & H_1 \cdot 25 = \{25, 49, 82\}, & H_1 \cdot 26 = \{26, 65, 104\}, \\
H_1 \cdot 28 = \{28, 31, 97\}, & H_1 \cdot 29 = \{29, 53, 113\}, & H_1 \cdot 34 = \{34, 46, 76\}, \\
H_1 \cdot 35 = \{35, 68, 92\}, & H_1 \cdot 36 = \{36, 90, 108\}, & H_1 \cdot 40 = \{40, 55, 61\}, \\
H_1 \cdot 41 = \{41, 71, 83\}, & H_1 \cdot 42 = \{42, 87, 105\}, & H_1 \cdot 47 = \{47, 50, 98\}, \\
H_1 \cdot 51 = \{51, 69, 114\}, & H_1 \cdot 56 = \{56, 62, 77\}, & H_1 \cdot 57 = \{57, 84, 93\}, \\
H_1 \cdot 58 = \{58, 106, 109\}, & H_1 \cdot 63 = \{63, 72, 99\}, & H_1 \cdot 73 = \{73, 85, 115\}, \\
H_1 \cdot 79 = \{79, 94, 100\}, & H_1 \cdot 95 = \{95, 101, 116\}, & \\
H_1 \cdot 39 = \{39\}, & H_1 \cdot 78 = \{78\}. &
\end{array}
$$

Subsequently, we distinguish two cases:

- Case (I): make use of 2 orbits of size 1 and 19 orbits of size 3, to make a subset of size $2 \cdot 1 + 19 \cdot 3 = 59 = (117+1)/2$. The search space is of size: $\binom{2}{2} \cdot \binom{38}{19} = 35{,}345{,}263{,}800$.
- Case (II): make use of 1 orbit of size 1 and 19 orbits of size 3, to make a subset of size $1 \cdot 1 + 19 \cdot 3 = 58 = (117-1)/2$. The search space is of size: $\binom{2}{1} \cdot \binom{38}{19} = 70{,}690{,}527{,}600$. In order to have sequences whose entries sum up to 1, these orbits have to encode the positions of the -1's.

For case (I), we conducted an exhaustive search for Legendre pairs of order 117 using the subgroup $\{1, 16, 22\}$ in 31 CPU hours. The search yielded 69,735,984 candidate sequences passing the PSD test, among them 192 Legendre pairs of lengths 117 were found. These pairs occur in 48 four-cycles (bipartite complete graphs $K_{2,2}$): by a four-cycle we mean four sequences A, B, C, D forming four Legendre pairs (A, B), (B, C), (C, D), and (D, A). However, these 192 Legendre pairs contain some redundancy due to symmetries. Denote by σ the cyclic (forward) shift and by ρ the reverting of a sequence, and assume that (A, B) is a Legendre pair. Then also $\big(A, \rho^i(\sigma^j(B))\big)$ is a Legendre pair for any choice of i and j, because the sequence of PAF values is invariant under shifting and reverting, i.e., $\mathrm{PAF}(B, s) = \mathrm{PAF}(\rho^i(\sigma^j(B)), s)$ for any s. Note that most of these pairs will not be found during this exhaustive search, because they are not compatible with the imposed orbit structure. The only operation that is compatible is $A \mapsto \rho(\sigma(A))$, because the set of orbits is invariant under $i \mapsto \ell - i$. Thus, we can design four Legendre pairs from the four sequences

$$A, \quad \rho(\sigma(A)), \quad B, \quad \rho(\sigma(B)).$$

Ten out of the 192 Legendre pairs are given below in the form $(A_k, B_k), k = 1, \ldots, 10$. Moreover, all 10 Legendre pairs of length 117 shown below, have $117/3 = 39$-th PSD values equal to $[64, 172]$. Among the remaining Legendre pairs of length 117, some also have $117/3 = 39$-th PSD values equal to $[28, 208]$. Algorithm 2 explains why there are no pairs with $[112, 124]$, see Example 2. Taking advantage of this property computationally, results in significant gains in CPU time, because we first use this property as a fast filtering mechanism (using exact arithmetic), before applying the computationally expensive full PSD test (using floating-point arithmetic). We also used the PSD constancy property over the orbits, see [2], in order to compute solely one PSD value per orbit.

In the following list, each Legendre pair (A, B) is given by two index sets I_A and I_B. The positions k where the sequence A equals 1, i.e., $a_k = 1$, are given by $\bigcup_{i \in I_A} H_1 \cdot i$, and the sequence A equals -1 at all other positions. Analogously, the index set I_B encodes the $\{-1, +1\}$-sequence B.

1. $I_{A_1} = \{1, 3, 4, 7, 8, 13, 14, 17, 19, 24, 28, 29, 36, 39, 40, 47, 51, 56, 63, 78, 95\}$
   $I_{B_1} = \{2, 5, 7, 9, 13, 14, 18, 19, 20, 24, 34, 36, 39, 40, 42, 47, 56, 58, 73, 78, 79\}$

2. $I_{A_2} = \{1, 4, 8, 10, 12, 18, 20, 29, 34, 35, 36, 39, 40, 47, 56, 57, 58, 63, 73, 78, 95\}$
   $I_{B_2} = \{3, 5, 6, 7, 8, 9, 10, 12, 13, 14, 18, 19, 20, 26, 28, 39, 40, 41, 47, 56, 78\}$

3. $I_{A_3} = \{1, 2, 4, 6, 7, 8, 10, 14, 18, 29, 34, 36, 39, 47, 51, 56, 63, 73, 78, 79, 95\}$
   $I_{B_3} = \{2, 3, 5, 7, 10, 12, 13, 14, 20, 24, 26, 28, 34, 36, 39, 40, 41, 47, 56, 63, 78\}$

4. $I_{A_4} = \{2, 3, 6, 7, 9, 19, 21, 26, 29, 34, 39, 40, 41, 47, 56, 58, 63, 73, 78, 79, 95\}$
   $I_{B_4} = \{1, 2, 3, 4, 5, 14, 17, 18, 25, 26, 29, 35, 36, 39, 40, 56, 57, 58, 63, 73, 78\}$

5. $I_{A_5} = \{2, 3, 9, 10, 17, 18, 19, 20, 25, 34, 36, 39, 41, 47, 56, 57, 58, 73, 78, 79, 95\}$
   $I_{B_5} = \{1, 2, 4, 8, 9, 13, 14, 17, 21, 26, 29, 39, 40, 42, 56, 57, 58, 63, 73, 78, 95\}$

6. $I_{A_6} = \{1, 2, 4, 5, 6, 8, 13, 17, 18, 19, 21, 34, 36, 39, 40, 41, 47, 51, 56, 73, 78\}$
   $I_{B_6} = \{2, 4, 7, 8, 9, 10, 13, 18, 24, 25, 29, 35, 39, 40, 51, 56, 63, 73, 78, 79, 95\}$

7. $I_{A_7} = \{2, 5, 6, 7, 8, 10, 13, 17, 18, 20, 21, 36, 39, 40, 41, 51, 58, 73, 78, 79, 95\}$
   $I_{B_7} = \{3, 4, 5, 7, 10, 14, 17, 18, 26, 28, 29, 35, 36, 39, 40, 41, 57, 63, 78, 79, 95\}$

8. $I_{A_8} = \{3, 4, 5, 7, 8, 18, 21, 24, 25, 28, 29, 34, 39, 40, 41, 42, 47, 56, 73, 78, 95\}$
   $I_{B_8} = \{3, 9, 14, 17, 19, 21, 25, 28, 29, 34, 35, 39, 40, 47, 51, 57, 58, 73, 78, 79, 95\}$

9. $I_{A_9} = \{1, 2, 4, 6, 7, 9, 10, 12, 13, 14, 18, 28, 29, 34, 35, 39, 41, 42, 56, 78, 95\}$
   $I_{B_9} = \{5, 6, 8, 9, 10, 13, 14, 19, 20, 25, 28, 34, 36, 39, 41, 51, 56, 58, 63, 73, 78\}$

10. $I_{A_{10}} = \{1, 2, 5, 7, 8, 9, 19, 20, 24, 29, 35, 36, 39, 40, 51, 58, 63, 73, 78, 79, 95\}$
    $I_{B_{10}} = \{5, 7, 9, 10, 13, 14, 17, 20, 21, 26, 28, 35, 39, 40, 42, 56, 57, 63, 78, 79, 95\}$

We also list the above 10 Legendre pairs of pairs length 117 in a more succinct manner, using the lexicographic ranks of the subsets encoding the positions of $+1's$:

$$\begin{array}{ll}
(10327421105, 25363140085), & (15300082821, 29082145926), \\
(5172847060, 20669267508), & (21265971921, 810444739), \\
(22124932714, 6023154169), & (4370665803, 24003646556), \\
(24634133277, 27568254144), & (27457918899, 31248697558), \\
(5218049000, 33814036464), & (6896605532, 34222709639).
\end{array}$$

More specifically, these are the 19-element subsets of $\{1, \dots, 38\}$, ranked lexicographically from 0 to $\binom{38}{19} - 1 = 35{,}345{,}263{,}800 - 1$. See [5] for ranking and unranking algorithms for k-element subsets and other useful combinatorial structures. For example, the integer 10327421105 encodes the subset

$$\{1, 3, 4, 7, 8, 12, 13, 14, 16, 19, 22, 23, 26, 27, 30, 31, 32, 35, 38\} \subset \{1, \dots, 38\},$$

which corresponds to I_{A_1} (using the order of the orbits as displayed above).

For case (II), we conducted an exhaustive search for Legendre pairs of order 117 using the subgroup $\{1, 16, 22\}$. The search yielded 139,471,968 candidate sequences passing the PSD test, among them 768 Legendre pairs of lengths 117 were found. These 768 Legendre pairs occur in 48 $K_{4,4}$ bipartite graphs. Similar to case (I), we can explain this phenomenon via the underlying symmetries.

Recall the notations σ and ρ for the cyclic shift and reverting of a sequence. In case (I) we chose both 1-orbits, and therefore all sequences A in the search space satisfied $A_{39} = A_{78} = 1$ and $A_{117} = -1$. In contrast, we choose in case (II) only one 1-orbit and hence the sequences in the search space have $(A_{39}, A_{78}, A_{117})$ equal to $(-1, 1, 1)$ or $(1, -1, 1)$. A sequence of the first type ($A_{39} = -1$) can be mapped to one of the second type ($A_{78} = -1$) by σ^{39}, notably without leaving the search space, because the set of orbits is invariant under $i \mapsto i + 39 \pmod{117}$. Hence one finds the following four sequences with identical PAF values in the search space of case (II):

$$A, \quad \sigma^{39}(A), \quad \rho(\sigma(A)), \quad \rho(\sigma^{40}(A)).$$

Combining any of these four sequences with any of the four sequences with complementary PAF sequence forms a Legendre pair. This explains the occurrence of $K_{4,4}$ bipartite graphs.

Also note that for any sequence A with $A_{39} = -1$ in case (II), we find the sequence $\sigma^{-39}(A)$ in the search space of case (I). Ignoring the symmetries, i.e., picking one representative from each class, yields 48 Legendre pairs which are non-equivalent under shifting and reverting.

4.1.2 Legendre pairs of length 117 via H_2

The subgroup $H_2 = \{1, 40, 79\}$ of order 3 of $\mathbb{Z}^\star_{117}$ acts on $\mathbb{Z}_{117}$ and yields 38 size 1 orbits and 26 size 3 orbits, which gives a lot of possible combinations to build subsets of size 58 (or 59). We have not been able to construct Legendre pairs of length 117 using H_2, possibly because we did not implement an exhaustive search in this case.

4.1.3 Legendre pairs of length 117 via H_3

The subgroup $H_3 = \{1, 55, 100\}$ of order 3 of $\mathbb{Z}^\star_{117}$ acts on $\mathbb{Z}_{117}$ and yields 8 size 1 orbits and 36 size 3 orbits, which gives 3 possible combinations to build subsets of size 59:

(a) $8 \cdot 1 + 17 \cdot 3 = 59$ with search space of size 8,597,496,600 (2.7 CPU hours); there are 2,812,308 sequences passing the PSD test.

(b) $5 \cdot 1 + 18 \cdot 3 = 59$ with search space of size 508,207,576,800 (95 CPU hours); there are 50,685,120 sequences passing the PSD test.

(c) $2 \cdot 1 + 19 \cdot 3 = 59$ with search space of size 240,729,904,800 (49 CPU hours); there are 36,699,600 sequences passing the PSD test.

In addition, there are also 3 possible combinations to build blocks of size 58:

(d) $7 \cdot 1 + 17 \cdot 3 = 58$ with search space of size 68,779,972,800 (13.5 CPU hours); there are 10,485,600 sequences passing the PSD test.

(e) $4 \cdot 1 + 18 \cdot 3 = 58$ with search space of size 635,259,471,000 (119 CPU hours); there are 63,356,400 sequences passing the PSD test.

(f) $1 \cdot 1 + 19 \cdot 3 = 58$ with search space of size 68,779,972,800 (22 CPU hours); there are 22,498,464 sequences passing the PSD test.

No Legendre pair of length 117 whose multiplier group contains H_3 exists.

4.1.4 Legendre pairs of length 117 via H_4

The subgroup $H_4 = \{1, 61, 94\}$ of order 3 of $\mathbb{Z}_{117}^\star$ acts on $\mathbb{Z}_{117}$ and yields a search space of size: $\binom{2}{2} \cdot \binom{38}{19} = 35{,}345{,}263{,}800$, because there are 38 orbits of size 3 and 2 orbits of size 1, and we need 19 orbits of size 3 and 2 orbits of size 1 to make a subset of size $19 \cdot 3 + 2 \cdot 1 = 59 = (117 + 1)/2$. We found 240 Legendre pairs of length 117 via an exhaustive search. Some of them are shown below in LexRank form:

$$
\begin{array}{lll}
(8221110983, 12044164377), & (12702071296, 15372978390), & (23944768832, 15178414396), \\
(20338660993, 90051589), & (7146518669, 23738703053), & (3073133857, 30770050335), \\
(32540516078, 3097218289), & (33749219312, 4797783684), & (5422010999, 7269176966).
\end{array}
$$

Among the 240 pairs, there are 144 pairs with $[\mathrm{PSD}(A, 39), \mathrm{PSD}(B, 39)]$ equal to $[64, 172]$ and 96 pairs with $[\mathrm{PSD}(A, 39), \mathrm{PSD}(B, 39)]$ equal to $[28, 208]$.

A search with block size 58 delivered 960 Legendre pairs of length 117. Analogous to subgroup H_1, any of these pairs can be obtained from others by shifting and reverting one or both sequences. Hence, we can extract 60 Legendre pairs using H_4 which are non-equivalent under shifting and reverting.

4.2 Legendre pairs of length 129

We executed Algorithm 1 for Legendre pairs of length $\ell = 129 = 3 \cdot 43$ and obtained that the spectrum of possible pairs of values for $\mathrm{PSD}(A, 43)$ and $\mathrm{PSD}(B, 43)$ is made up of only 5 pairs:

$$\big[\mathrm{PSD}(A, 43), \mathrm{PSD}(B, 43)\big] \in \big\{[4, 256], [16, 244], [52, 208], [64, 196], [112, 148]\big\}.$$

There is one subgroup of order 3 in $\mathbb{Z}_{129}^\star$

$$H = \{1, 49, 79\}$$

acting on $\mathbb{Z}_{129}$ and yielding a search space of size $\binom{2}{2} \cdot \binom{42}{21} = 538{,}257{,}874{,}440$. Since there are 42 orbits of size 3 and 2 orbits of size 1, we need 21 orbits of size 3 and 2 orbits of size 1, to make a subset of size $21 \cdot 3 + 2 \cdot 1 = 65 = (129 + 1)/2$. The $42 + 2$ orbits of the action of $H = \{1, 49, 79\}$ on $\mathbb{Z}_{129}$ are

$$
\begin{array}{lll}
H \cdot 1 = \{1, 49, 79\}, & H \cdot 2 = \{2, 29, 98\}, & H \cdot 3 = \{3, 18, 108\}, \\
H \cdot 4 = \{4, 58, 67\}, & H \cdot 5 = \{5, 8, 116\}, & H \cdot 6 = \{6, 36, 87\}, \\
H \cdot 7 = \{7, 37, 85\}, & H \cdot 9 = \{9, 54, 66\}, & H \cdot 10 = \{10, 16, 103\}, \\
H \cdot 11 = \{11, 23, 95\}, & H \cdot 12 = \{12, 45, 72\}, & H \cdot 13 = \{13, 121, 124\}, \\
H \cdot 14 = \{14, 41, 74\}, & H \cdot 15 = \{15, 24, 90\}, & H \cdot 17 = \{17, 53, 59\}, \\
H \cdot 19 = \{19, 28, 82\}, & H \cdot 20 = \{20, 32, 77\}, & H \cdot 21 = \{21, 111, 126\}, \\
H \cdot 22 = \{22, 46, 61\}, & H \cdot 25 = \{25, 40, 64\}, & H \cdot 26 = \{26, 113, 119\}, \\
H \cdot 27 = \{27, 33, 69\}, & H \cdot 30 = \{30, 48, 51\}, & H \cdot 31 = \{31, 100, 127\}, \\
H \cdot 34 = \{34, 106, 118\}, & H \cdot 35 = \{35, 38, 56\}, & H \cdot 39 = \{39, 105, 114\}, \\
H \cdot 42 = \{42, 93, 123\}, & H \cdot 44 = \{44, 92, 122\}, & H \cdot 47 = \{47, 101, 110\}, \\
H \cdot 50 = \{50, 80, 128\}, & H \cdot 52 = \{52, 97, 109\}, & H \cdot 55 = \{55, 88, 115\}, \\
H \cdot 57 = \{57, 84, 117\}, & H \cdot 60 = \{60, 96, 102\}, & H \cdot 62 = \{62, 71, 125\}, \\
H \cdot 63 = \{63, 75, 120\}, & H \cdot 65 = \{65, 89, 104\}, & H \cdot 68 = \{68, 83, 107\}, \\
H \cdot 70 = \{70, 76, 112\}, & H \cdot 73 = \{73, 91, 94\}, & H \cdot 78 = \{78, 81, 99\}, \\
H \cdot 43 = \{43\}, & H \cdot 86 = \{86\}. &
\end{array}
$$

We conducted an exhaustive search for Legendre pairs of order 129 using the subgroup $H = \{1, 49, 79\}$ in 431 CPU hours. The search was done in parallel on 16 threads and yielded output files of total size 80 gigabytes, containing more than 460 million sequences which passed the PSD test; among them 112 Legendre pairs of length 129 were found. Analogous to $\ell = 117$, this list can be condensed to 28 pairs, where the remaining ones are obtained by symmetry.

Here are two Legendre pairs of length 129, given by index sets I_A, I_B:

1. $I_A = \{1, 2, 5, 13, 17, 19, 21, 22, 25, 26, 27, 34, 39, 43, 50, 55, 60, 62, 63, 68, 73, 78, 86\}$
   $I_B = \{1, 3, 11, 12, 13, 17, 21, 26, 31, 34, 35, 42, 43, 47, 50, 52, 57, 60, 62, 68, 70, 78, 86\}$

2. $I_A = \{1, 2, 5, 13, 17, 19, 21, 22, 25, 26, 27, 34, 39, 43, 50, 55, 60, 62, 63, 68, 73, 78, 86\}$
   $I_B = \{1, 2, 3, 4, 5, 6, 10, 11, 12, 17, 19, 20, 21, 22, 27, 30, 34, 43, 50, 57, 70, 73, 86\}$

Both the above Legendre pairs of length 129 have $\left[\widehat{A}_{43}, \widehat{B}_{43}\right] = [148, 112]$. In fact, all the 112 Legendre pairs of length 129 that we found have this property. This is partly explained by applying Algorithm 2, where

$$4,\ 76,\ 112,\ 148,\ 256,\ 292,\ 364,\ 400, \ldots$$

are returned as potential values for $\widehat{A}_{43}$ and $\widehat{B}_{43}$, leaving only two possible pairs, namely $[4, 256]$ and $[112, 148]$.

4.3 Legendre pairs of length 147

We executed Algorithm 1 for Legendre pairs of length $\ell = 147 = 3 \cdot 49$ and obtained that the spectrum of possible pairs of values for $\mathrm{PSD}(A, 49)$ and $\mathrm{PSD}(B, 49)$ is made up of only 6 pairs

$$\big[\mathrm{PSD}(A, 49), \mathrm{PSD}(B, 49)\big] \in \big\{[4, 292], [28, 268], [52, 244], [100, 196], [124, 172], [148, 148]\big\}.$$

Algorithm 2 further shows that in fact only two of the above six pairs (namely the first and the last one) are compatible with the particular orbit structure induced by the subgroup H of order 3 in $\mathbb{Z}_{147}^{\star}$

$$H = \{1, 67, 79\}$$

acting on $\mathbb{Z}_{147}$. This information prevents us from conducting redundant computations and helps us target the search more narrowly. The 50 orbits of the action of $H = \{1, 67, 79\}$ on $\mathbb{Z}_{147}$ are

$$\begin{array}{lll}
H \cdot 1 = \{1, 67, 79\}, & H \cdot 2 = \{2, 11, 134\}, & H \cdot 3 = \{3, 54, 90\}, \\
H \cdot 4 = \{4, 22, 121\}, & H \cdot 5 = \{5, 41, 101\}, & H \cdot 6 = \{6, 33, 108\}, \\
H \cdot 7 = \{7, 28, 112\}, & H \cdot 8 = \{8, 44, 95\}, & H \cdot 9 = \{9, 15, 123\}, \\
H \cdot 10 = \{10, 55, 82\}, & H \cdot 12 = \{12, 66, 69\}, & H \cdot 13 = \{13, 136, 145\}, \\
H \cdot 14 = \{14, 56, 77\}, & H \cdot 16 = \{16, 43, 88\}, & H \cdot 17 = \{17, 20, 110\}, \\
H \cdot 18 = \{18, 30, 99\}, & H \cdot 19 = \{19, 31, 97\}, & H \cdot 21 = \{21, 42, 84\}, \\
H \cdot 23 = \{23, 53, 71\}, & H \cdot 24 = \{24, 132, 138\}, & H \cdot 25 = \{25, 58, 64\}, \\
H \cdot 26 = \{26, 125, 143\}, & H \cdot 27 = \{27, 45, 75\}, & H \cdot 29 = \{29, 32, 86\}, \\
H \cdot 34 = \{34, 40, 73\}, & H \cdot 35 = \{35, 119, 140\}, & H \cdot 36 = \{36, 51, 60\}, \\
H \cdot 37 = \{37, 127, 130\}, & H \cdot 38 = \{38, 47, 62\}, & H \cdot 39 = \{39, 114, 141\}, \\
H \cdot 46 = \{46, 106, 142\}, & H \cdot 48 = \{48, 117, 129\}, & H \cdot 49 = \{49\}, \\
H \cdot 50 = \{50, 116, 128\}, & H \cdot 52 = \{52, 103, 139\}, & H \cdot 57 = \{57, 93, 144\}, \\
H \cdot 59 = \{59, 104, 131\}, & H \cdot 61 = \{61, 115, 118\}, & H \cdot 63 = \{63, 105, 126\}, \\
H \cdot 65 = \{65, 92, 137\}, & H \cdot 68 = \{68, 80, 146\}, & H \cdot 70 = \{70, 91, 133\} \\
H \cdot 72 = \{72, 102, 120\}, & H \cdot 74 = \{74, 107, 113\}, & H \cdot 76 = \{76, 94, 124\}, \\
H \cdot 78 = \{78, 81, 135\}, & H \cdot 83 = \{83, 89, 122\}, & H \cdot 85 = \{85, 100, 109\}, \\
H \cdot 87 = \{87, 96, 111\}, & H \cdot 98 = \{98\}. &
\end{array}$$

Here is a Legendre pair (A, B) of length $\ell = 147$, given by two index sets I_A and I_B. The positions k where the sequence A equals 1, i.e., $a_k = 1$, are given by $\bigcup_{i \in I_A} H \cdot i$, and the sequence A equals -1 at all other positions. Analogously, the index set I_B encodes the $\{-1, +1\}$-sequence B:

$$I_A = \{1, 2, 3, 5, 7, 8, 10, 14, 16, 17, 19, 21, 27, 35, 38, 39, 49, 52, 57, 61, 70, 72, 74, 83, 87, 98\},$$

$$I_B = \{1, 2, 6, 7, 9, 10, 12, 16, 17, 19, 23, 24, 26, 35, 39, 46, 48, 49, 50, 59, 65, 68, 70, 78, 85, 98\}.$$

The LexRank encoding of the Legendre pair (A, B) of length $\ell = 147$ is

$$(2279447240326, 6981583007090).$$

This Legendre pair (A, B) of length $\ell = 147$ has $\left[\widehat{A}_{49},\ \widehat{B}_{49}\right] = [148, 148]$, the second pair of values predicted by Algorithms 1 and 2.

We also give three Legendre pairs of length $\ell = 147$ with $\left[\widehat{A}_{49},\ \widehat{B}_{49}\right] = [4, 292]$, the first pair of values predicted by Algorithms 1 and 2:

1. $(1685512212865, 3612702197526)$,
2. $(2926263388957, 265692014998)$,
3. $(4357037511235, 3728601853735)$.

We remark that the combination of Algorithms 1 and 2 was of critical importance, in order to traverse the first portion (15%) of the huge search space of 32 trillion elements and find the Legendre pairs of length $\ell = 147$.

4.4 Legendre pairs of length 133

We used the subgroup of order 3, $H = \{1, 11, 121\}$, acting on $\mathbb{Z}_{133}$. This yields a search space of size $\binom{44}{22}$ = 2,104,098,963,720 elements. The computation was stopped after 20% of the search space was traversed, in 707 hours of CPU time. The output files grew to a total size of 108 gigabytes and 5 new Legendre pairs of length 133 were discovered (we display their lexicographic rank for a 22-subset of the 44 orbits of size 3, but this time these indices give the positions of the -1's):

1. $(128572618842, 210086022915)$,
2. $(17644506807, 41167368128)$,
3. $(179364459458, 27235734754)$,
4. $(213277890206, 251235525902)$,
5. $(272147218211, 279717372516)$.

These five Legendre pairs can be used to make Hadamard matrices of order $2 \cdot 133 + 2 = 268$, via the two circulant core template array in [3]. The order 268 was the smallest open order for Hadamard matrices until 1985 [6].

These five Legendre pairs have integer PSD values at integer multiples of the prime factor 19 of $\ell = 133$. More specifically, using the above numbering we have

1. $\left[\widehat{A}_{19}, \widehat{B}_{19}\right] = \left[\widehat{A}_{38}, \widehat{B}_{38}\right] = \left[\widehat{A}_{57}, \widehat{B}_{57}\right] = [176, 92]$,

2. $\left[\widehat{A}_{19}, \widehat{B}_{19}\right] = \left[\widehat{A}_{38}, \widehat{B}_{38}\right] = \left[\widehat{A}_{57}, \widehat{B}_{57}\right] = [92, 176]$,

3. $\left[\widehat{A}_{19}, \widehat{B}_{19}\right] = \left[\widehat{A}_{38}, \widehat{B}_{38}\right] = \left[\widehat{A}_{57}, \widehat{B}_{57}\right] = [36, 232]$,

4. $\left[\widehat{A}_{19}, \widehat{B}_{19}\right] = \left[\widehat{A}_{38}, \widehat{B}_{38}\right] = \left[\widehat{A}_{57}, \widehat{B}_{57}\right] = [92, 176]$,

5. $\left[\widehat{A}_{19}, \widehat{B}_{19}\right] = \left[\widehat{A}_{38}, \widehat{B}_{38}\right] = \left[\widehat{A}_{57}, \widehat{B}_{57}\right] = [92, 176]$.

Using Proposition 1 with $\ell = 133, m = 19, n = 7$, we are able to ascertain the cause of this property.

- For the 3rd Legendre pair of length 133 we found, using the notations of Proposition 1 we have:

$$\begin{array}{rl} \mathcal{A} = [1,1,1,1,1,1,-5], & \mathrm{PAF}(\mathcal{A},1) = \mathrm{PAF}(\mathcal{A},2) = \mathrm{PAF}(\mathcal{A},3) = -5, \\ \mathcal{B} = [-1,-1,5,-1,5,5,-11], & \mathrm{PAF}(\mathcal{B},1) = \mathrm{PAF}(\mathcal{B},2) = \mathrm{PAF}(\mathcal{B},3) = -33. \end{array}$$

  Therefore, by applying Proposition 1, we obtain (note that $-5 - 33 = 2 \cdot (-19)$)

$$\begin{array}{c} \mathrm{PSD}(A,19) = \mathrm{PSD}(A,38) = \mathrm{PSD}(A,57) = p_2(\mathcal{A}) - \mathrm{PAF}(\mathcal{A},1) = 31 + 5 = 36, \\ \mathrm{PSD}(B,19) = \mathrm{PSD}(B,38) = \mathrm{PSD}(B,57) = p_2(\mathcal{B}) - \mathrm{PAF}(\mathcal{B},1) = 199 + 33 = 232. \end{array}$$

- For the 5th Legendre pair of length 133 we found, using the notations of Proposition 1 we have:

$$\begin{array}{rl} \mathcal{A} = [1,1,-3,1,-3,-3,7], & \mathrm{PAF}(\mathcal{A},1) = \mathrm{PAF}(\mathcal{A},2) = \mathrm{PAF}(\mathcal{A},3) = -13, \\ \mathcal{B} = [-5,-5,5,-5,5,5,1], & \mathrm{PAF}(\mathcal{B},1) = \mathrm{PAF}(\mathcal{B},2) = \mathrm{PAF}(\mathcal{B},3) = -25. \end{array}$$

  Therefore, by applying Proposition 1, we obtain (note that $-13 - 25 = 2 \cdot (-19)$)

$$\begin{array}{c} \mathrm{PSD}(A,19) = \mathrm{PSD}(A,38) = \mathrm{PSD}(A,57) = p_2(\mathcal{A}) - \mathrm{PAF}(\mathcal{A},1) = 79 + 13 = 92, \\ \mathrm{PSD}(B,19) = \mathrm{PSD}(B,38) = \mathrm{PSD}(B,57) = p_2(\mathcal{B}) - \mathrm{PAF}(\mathcal{B},1) = 151 + 25 = 176. \end{array}$$

5 Conclusion

We prove a proposition that connects constant-PAF sequences and the corresponding Legendre pairs with integer PSD values. We update the list of open lengths for Legendre pairs, in [1]. In particular, we furnish the first ever examples of Legendre pairs of the four open lengths $117, 129, 133, 147$. In the case of the three open lengths $117, 129, 147$, we make extensive use of two new algorithms. Our first algorithm yields the determination of the complete spectrum of the (resp. 39-th, 43-rd, 49-th) value of the discrete Fourier transform for Legendre pairs. In fact, our algorithm yields the complete spectrum of the $(\ell/3)$-rd value of the discrete Fourier transform for Legendre pairs of lengths $\ell \equiv 0 \pmod 3$. Our second algorithm exploits the particular orbit structure induced by specific subgroups of their multiplier group, to disqualify certain elements of the spectrum determined by the first algorithm. The combination of both algorithms for Legendre pairs of lengths $\ell \equiv 0 \,(\mathrm{mod}\ 3)$ was a decisive factor in discovering Legendre pairs of the three open lengths $117, 129, 147$. A Legendre pair of length $\ell = 77$ was reported in 2020 in [8], see [10]. Therefore, the state-of-the-art list of twelve integers in the range < 200 for which the question of existence of Legendre pairs is still unsolved is

$$85, 87, 115, 145, 159, 161, 169, 175, 177, 185, 187, 195.$$

For $\ell = 87$, the order-7 subgroup $\{1, 7, 16, 25, 49, 52, 82\}$, and both subgroups of order 4 (namely, $\{1, 17, 28, 41\}$ and $\{1, 28, 46, 70\}$) did not yield any solutions by exhaustive search. We also tried some of the subgroups of order 2 (there are three of them: $\{1, 28\}, \{1, 59\}, \{1, 86\}$), which admit many possible combinations of their associated subsets, some of whose search spaces being beyond our computational resources, but without success. Therefore, even twenty years after the fundamental paper [3] for Legendre pairs appeared, there are still interesting questions and open problems to ponder in this area.

Acknowledgment We are grateful for the detailed and pertinent referee comments that contributed to improving our paper. In particular, one of the referees provided a generalized version of our original Proposition 1 and a significantly simplified version of its proof.

References

[1] N. A. Balonin and D. Z. Djokovic. Three new lengths for cyclic Legendre pairs. https://arxiv.org/abs/2010.02829.

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

[3] 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.

[4] I. S. Kotsireas, C. Koukouvinos, and J. Seberry. Weighing matrices and string sorting. *Ann. Comb.*, 13(3):305–313, 2009.

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

[6] K. Sawade. A Hadamard matrix of order 268. *Graphs Combin.*, 1(2):185–187, 1985.

[7] B. Sturmfels. *Algorithms in Invariant Theory.* Texts and Monographs in Symbolic Computation. Springer-Verlag, Vienna, 1993.

[8] J. S. Turner. personal communication. Dec 7, 2020.

[9] J. S. Turner, D. Bulutoglu, D. Baczkowski, and A. Geyer. Counting the decimation classes of binary vectors with relatively prime length and density. *J. of Algebraic Comb.*, 2021 (to appear).

[10] J. S. Turner, I. S. Kotsireas, D. Bulutoglu, and A. Geyer. A Legendre pair of length 77 using complementary binary matrices with fixed marginals. *Des. Codes Cryptogr.*, 89(6):1321–1333, 2021.