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

C. Koutschan, I. Kotsireas

RICAM-Report 2021-01

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

Ilias Kotsireas[*] & Christoph Koutschan[†]

January 2021

Abstract

We show how to determine explicitly the complete spectrum of the $\frac{\ell}{3}$-rd value of the Discrete Fourier Transform for Legendre pairs of lengths $\ell \equiv 0 \pmod 3$. As an application, we exhibit the first known examples of Legendre pairs of lengths 117 and 129, using the union of orbits approach. We also exhibit the first known examples of Legendre pairs of length 133. As a consequence, we provide the state-of-the-art list of thirteen integers in the range < 200 for which the question of existence of Legendre pairs remains unresolved.

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

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

where $i + s$ is taken modulo ℓ, when $i + s > \ell$.
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 $\omega = \cos\left(\frac{2\pi}{\ell}\right) + i \sin\left(\frac{2\pi}{\ell}\right)$ is the primitive ℓ-th root of unity, that satisfies $\omega^\ell = 1$.

[*] Supported by an NSERC grant

[†] Supported by the Austrian Science Fund (FWF): F5011-N15.

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 $a_1 + \ldots + a_\ell = \pm 1$ and $b_1 + \ldots + b_\ell = \pm 1$ form a Legendre pair of length ℓ if

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

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 [**?**], that if (A,B) form a Legendre pair of length ℓ, then we have

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

The paper [**?**] is a fundamental paper 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 $1,\ldots,\frac{\ell-1}{2}$ 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 emanates from the fact that the PSD values are always non-negative, as sums of 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 [**?**].

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

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

Lemma 1. *Let ℓ be an odd integer such that $\ell \equiv 0 \pmod 3$ and let $m = \frac{\ell}{3}$. Denote by $\omega = e^{2\pi i/\ell} = \cos\left(\frac{2\pi}{\ell}\right) + i\sin\left(\frac{2\pi}{\ell}\right)$ the principal ℓ-th root of unity, and let $A = [a_1,\ldots,a_\ell]$ be a $\{-1,+1\}$-sequence. Then we have that $\mathrm{DFT}(A,m)$ can be evaluated explicitly in closed form and $\mathrm{PSD}(A,m)$ is a non-negative integer. The explicit evaluations are given by*

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

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

where

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

The proof of Lemma **??** is based on the exact evaluation of the roots of the cyclotomic polynomial of degree 3.
Consider a finite set of ℓ discrete variables $\mathcal{A} = \{a_1, \dots, a_\ell\}$. Let

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

denote the second elementary symmetric function in $\mathcal{A}$. 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 in $\mathcal{A}$. 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 [**?**].

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

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

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

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

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 **??** 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 with 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 (**??**). 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 (**??**), and then:

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

■

In the sequel, we denote $\mathrm{PSD}(A,m)$ by $\widehat{A}_m$ and $\mathrm{PSD}(B,m)$ by $\widehat{B}_m$. As an additional consistency verification pertaining to Corollary **??**, one can verify that:

$$\begin{aligned} \widehat{A}_m + \widehat{B}_m &= \frac{3}{2}\left(A_1^2 + A_2^2 + A_3^2\right) - \frac{1}{2} + \frac{3}{2}\left(B_1^2 + B_2^2 + B_3^2\right) - \frac{1}{2} \\ &= \frac{3}{2}(4m+2) - 1 = \frac{3}{2}\left(4\frac{\ell}{3} + 2\right) - 1 = 2\ell + 3 - 1 = 2\ell + 2. \end{aligned}$$

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

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

Moreover, from (**??**) 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 squares are integers, we obtain that $2\widehat{A}_m + 1 \equiv 0 \pmod 3$ and $2\widehat{B}_m + 1 \equiv 0 \pmod 3$ i.e. $\widehat{A}_m \equiv 1 \pmod 3$ and $\widehat{B}_m \equiv 1 \pmod 3$. Therefore, the set of possible pairs of values $(\widehat{A}_m, \widehat{B}_m)$ can be restricted considerably. In addition, a possible pair of values $(\widehat{A}_m, \widehat{B}_m)$ has to be compatible with the linear constraints

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

Note that 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 (**??**) 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 (**??**). The above discussion suffices to formulate an algorithm for determining explicitly the complete spectrum of the $\frac{\ell}{3}$-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 $s = 0, \dots, m$ do
    (1) form the candidate $[\widehat{A}_m, \widehat{B}_m]$ pair $[3s+1, 2\ell+2-(3s+1)]$ ;
    (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 (??) ;
    (3) solve (up to sign) the two sum-of-squares Diophantine equations
        $A_1^2 + A_2^2 + A_3^2 = \frac{2(3s+1)+1}{3}$ and $B_1^2 + B_2^2 + B_3^2 = \frac{2(2\ell+2-(3s+1))+1}{3}$ ;
    if there are all-odd solutions of these two Diophantine equations, compatible
      with the linear constraints (??) then
        insert the pair $[3s+1, 2\ell+2-(3s+1)]$ in $\mathcal{S}$, as an element of the
          spectrum of $[\widehat{A}_m, \widehat{B}_m]$ ;
    else
        discard the pair $[3s+1, 2\ell+2-(3s+1)]$ as it cannot be an element of the
          spectrum of $[\widehat{A}_m, \widehat{B}_m]$ ;
    end
end
Output: the spectrum $\mathcal{S}$ of pairs of values $[\widehat{A}_m, \widehat{B}_m]$ for Legendre pairs $(A, B)$ of
  length $\ell = 3 \cdot m$ ;
```

Example 1. *We illustrate the algorithm with the case* $\ell = 117 = 3 \cdot 39$*, i.e.,* $m = 39$*. First we note that we have* $\widehat{A}_m + \widehat{B}_m = 2 \cdot 117 + 2 = 236$ *and in addition* $\widehat{A}_m \equiv 1 \pmod 3$ *and* $\widehat{B}_m \equiv 1 \pmod 3$*. Given that every pair of values* $(\widehat{A}_m, \widehat{B}_m)$ *determines the values of* $A_1^2 + A_2^2 + A_3^2$ *and* $B_1^2 + B_2^2 + B_3^2$ *via (**??**), we obtain the following table:*

$(\widehat{A}_m, \widehat{B}_m)$	
$(1, 235)$	$A_1^2 + A_2^2 + A_3^2 = 1, \rightsquigarrow$ *no all-odd solutions* $B_1^2 + B_2^2 + B_3^2 = 157,$
$(4, 232)$	$A_1^2 + A_2^2 + A_3^2 = 3, \rightsquigarrow [1, 1, 1]$ $B_1^2 + B_2^2 + B_3^2 = 155, \rightsquigarrow [3, 5, 11], [5, 7, 9] \rightsquigarrow$ *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:* $(A_1, A_2, A_3) = (-1, -5, 7), (B_1, B_2, B_3) = (3, 5, -7)$

The first two rows of the table indicate two different reasons why a certain $(\widehat{A}_m, \widehat{B}_m)$ *combination can be discarded. The last three rows of the table indicate the only three* $(\widehat{A}_m, \widehat{B}_m)$ *combinations that can possibly hold. The remaining* $40 - 5 = 35$ *rows of the table corresponding to all other* $(\widehat{A}_m, \widehat{B}_m)$ *combinations are omitted, but it can easily be seen that they do not lead to compatible assignments for* A_1, A_2, A_3 *and/or* B_1, B_2, B_3*. In summary, from the* 40 *possible pairs of values for* $(\widehat{A}_m, \widehat{B}_m)$*, our algorithm indicates that only* 3 *pairs of values are likely to occur in Legendre pairs of length* 117*, which allows us to add an additional layer of parallelism, when searching for such Legendre pairs.*

3 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 **??** (provided that $\ell \equiv 0 \pmod 3$), by computing the sums A_1, A_2, A_3 and then $\mathrm{PSD}\big(A, \frac{\ell}{3}\big)$ 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 $\mathrm{PSD}(A,k) \leq 2\ell+2$ for all $1 \leq k \leq \frac{1}{2}(\ell-1)$ (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 $I = \big\{1,\ldots,\frac{1}{2}(\ell-1)\big\} \setminus \big\{\frac{\ell}{3}\big\}$ 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 timings were measured on RICAM's computing cluster `radon1`, which has 1168 Xeon E5-2630v3 (2.4Ghz) cores. For the reported computations, we employed a moderate parallelization, typically using 16 cores for one task. Since the parallelization is done by splitting the search space into pieces, it scales very well. The reported timings are given in CPU hours, i.e., as the sum of the timings of each core.

3.1 Legendre pairs of length 117

We executed Algorithm 1 for Legendre pairs of length $\ell = 117 = 3\cdot 39$ and obtained that the spectrum of possible pairs of values for $\mathrm{PSD}(A,39)$ and $\mathrm{PSD}(B,39)$ is made up of only 3 pairs:

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

as it was demonstrated in Example **??**. 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.

3.1.1 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 $\mathbb{Z}_{117}^{\star}$ 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, while we need 19 orbits of size 3 and 2 orbits of size 1, to make a block of size $19\cdot 3+2\cdot 1 = 59 = \frac{117+1}{2}$. We enumerate the $38+2$ orbits of the action of $H_1 = \{1,16,22\}$

on $\mathbb{Z}_{117}^{\star}$ as follows:

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

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 10 Legendre pairs of pairs length 117 were found, these 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 the property that their $117/3 = 39$-th PSD values are equal to $[64, 172]$. 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 and slow full PSD test (using floating-point arithmetic).

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

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

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

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

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

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

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

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

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

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

We also list the 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 $\{1, \ldots, 38\}$, ranked lexicographically from 0 to $\binom{38}{19} - 1 = 35{,}345{,}263{,}800 - 1$. See [?] for ranking and unranking algorithms for k-element subsets and other useful combinatorial structures. For example, the integer 10327421105 encodes the subset

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

of $\{1, \ldots, 38\}$, which corresponds to the index set I_A in item 1 (using the order of the 3-cosets as displayed above).

3.1.2 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 $\mathbb{Z}^{\star}_{117}$ and yields 38 1-cosets and 26 3-cosets, which gives a lot of possible combinations to build blocks of size 58 (or 59). We have note been able to construct Legendre pairs of length 117 using H_2.

3.1.3 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 $\mathbb{Z}^{\star}_{117}$ and yields 8 1-cosets and 36 3-cosets, which gives 3 possible combinations to build blocks of size 59:

(a) $8 \cdot 1 + 17 \cdot 3 = 59$ with search space of size 8,597,496,600 (8.5 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 (266 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 (138 CPU hours); there are 36,699,600 sequences passing the PSD test.

We did not find any Legendre pairs of length 117 via the subgroup H_3.

3.1.4 Legendre pairs of length 117 via H_4

The subgroup $H_4 = \{1, 61, 94\}$ of order 3 of $\mathbb{Z}^{\star}_{117}$ acts on $\mathbb{Z}^{\star}_{117}$ 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, while we need 19 orbits of size 3 and 2 orbits of size 1, to make a block of size $19 \cdot 3 + 2 \cdot 1 = 59 = \frac{117+1}{2}$. We find 9 Legendre pairs of length 117, composed out of 18 different sequences. These are shown below in LexRank form:

$(8221110983, 12044164377)$, $(12702071296, 15372978390)$, $(23944768832, 15178414396)$,
$(20338660993, 90051589)$, $(7146518669, 23738703053)$, $(3073133857, 30770050335)$,
$(32540516078, 3097218289)$, $(33749219312, 4797783684)$, $(5422010999, 7269176966)$.

Interestingly, among these nine pairs, there are 5 pairs with $[\mathrm{PSD}(A, 39), \mathrm{PSD}(B, 39)]$ equal to $[64, 172]$ (as it was the case for the first subgroup H_1), but there are also 4 pairs with $[\mathrm{PSD}(A, 39), \mathrm{PSD}(B, 39)]$ equal to $[28, 208]$.

3.2 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:

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

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

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

which acts on $\mathbb{Z}^{\star}_{129}$ and yields a search space of size: $\binom{2}{2} \cdot \binom{42}{21} = 538{,}257{,}874{,}440$, because there are 42 orbits of size 3 and 2 orbits of size 1, while we need 21 orbits of size 3 and 2 orbits of size 1, to make a block of size $21 \cdot 3 + 2 \cdot 1 = 65 = \frac{129+1}{2}$. We enumerate the $42 + 2$ orbits of the action of $H = \{1, 49, 79\}$ on $\mathbb{Z}^{\star}_{129}$ as follows:

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

We conducted an exhaustive search for Legendre pairs of order 129 using this subgroup in 431 CPU hours. The search was done in parallel on 16 processors and yielded output files of total size 80 Gigabytes, i.e., more than 500 million sequences passing the PSD test, among them 112 Legendre pairs of length 129 were found.

However, these 112 Legendre pairs contain some redundancy due to symmetries. Assume that two sequences $A = [a_1, \ldots, a_\ell]$ and $B = [b_1, \ldots, b_\ell]$ form a Legendre pair. Define the sequences $\tilde{A} = [a_{\ell-1}, a_{\ell-2}, \ldots, a_2, a_1, a_\ell]$ and $\tilde{B} = [b_{\ell-1}, b_{\ell-2}, \ldots, b_2, b_1, b_\ell]$. Then we obtain three other Legendre pairs: $(A, \tilde{B})$, $(\tilde{A}, B)$, and $(\tilde{A}, \tilde{B})$, which are also found by the exhaustive search, because the set of cosets is invariant under $i \mapsto \ell - i$.

3.3 Legendre pairs of length 133

We used the subgroup of order 3, $H = \{1, 11, 121\}$, which acts on $\mathbb{Z}^{\star}_{133}$ and 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 five new Legendre pairs of length 133 were discovered (as before, we display their lexicographic rank for a 22-subset of the 44 cosets 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. $(272147218211, 279717372516)$

We note that 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 [?]. The order 268 was the smallest open order for Hadamard matrices until 1985, when such matrices were constructed in [?].

We note that these five Legendre pairs have the property that their PSD values at integer multiples of the prime factor 19 of $\ell = 133$, are integers. More specifically, using the above numbering we have that:

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

The following proposition is an attempt to ascertain the cause of this property.

Proposition 1. *If the 19-compression* $(\mathcal{A}, \mathcal{B})$ *of a Legendre pair* (A, B) *of order* $\ell = 133$ *exhibits the constancy property:*

$$\mathrm{PAF}(\mathcal{A}, 1) = \mathrm{PAF}(\mathcal{A}, 2) = \mathrm{PAF}(\mathcal{A}, 3) = \widehat{A^{19}}$$

$$\mathrm{PAF}(\mathcal{B}, 1) = \mathrm{PAF}(\mathcal{B}, 2) = \mathrm{PAF}(\mathcal{B}, 3) = \widehat{B^{19}}$$

(where the constants $\widehat{A^{19}}$ *and* $\widehat{B^{19}}$ *must sum to* $(-2) \cdot 19 = -38$*), then the PSD values at integer multiples of* 19 *of* A *and* B *are integers, with the explicit evaluations:*

$$\mathrm{PSD}(A, 19 \cdot s) = p_2(\mathcal{A}) - \widehat{A^{19}}, \quad s = 1, 2, 3$$

$$\mathrm{PSD}(B, 19 \cdot s) = p_2(\mathcal{B}) - \widehat{B^{19}}, \quad s = 1, 2, 3$$

(where the constants $\mathrm{PSD}(A, 19 \cdot s)$ *and* $\mathrm{PSD}(B, 19 \cdot s)$ *must sum to* $2 \cdot 133 + 2 = 268$*).*

Proof. We remark that $\mathrm{DFT}(A, 19)$ and $\mathrm{DFT}(B, 19)$ are linear combinations of ω^0, $\omega^{1 \cdot 19}$, …, $\omega^{6 \cdot 19}$, where $\omega = e^{2\pi i/133}$ is the principal 133-rd root of unity. More specifically we have

$$\mathrm{DFT}(A, 19) = \sum_{s=0}^{\ell-1} a_{s+1} \omega^{s \cdot 19} = A_1 \, \omega^0 + A_2 \, \omega^{1 \cdot 19} + \cdots + A_7 \, \omega^{6 \cdot 19}$$

and

$$\mathrm{DFT}(B, 19) = \sum_{s=0}^{\ell-1} b_{s+1} \omega^{s \cdot 19} = B_1 \, \omega^0 + B_2 \, \omega^{1 \cdot 19} + \cdots + B_7 \, \omega^{6 \cdot 19}$$

where

$$A_1 = \sum_{i=0}^{\ell-1} a_{7i+1}, \ \ldots, \ A_7 = \sum_{i=0}^{\ell-1} a_{7i+7}, \ B_1 = \sum_{i=0}^{\ell-1} b_{7i+1}, \ \ldots, \ B_7 = \sum_{i=0}^{\ell-1} b_{7i+7},$$

i.e. $A_1, \ldots, A_7$ are the elements of the 19-compression of A and $B_1, \ldots, B_7$ are the elements of the 19-compression of B; see [**?**] for the definition and properties of compression of complementary sequences in general. Next we remark that $\omega^{19}, \ldots, \omega^{114}$ are the roots of the cyclotomic polynomial $\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$, which admit the explicit expressions:

$$\cos\left(\tfrac{2\pi}{7}\right) + i \sin\left(\tfrac{2\pi}{7}\right), \quad -\cos\left(\tfrac{3\pi}{7}\right) + i \sin\left(\tfrac{3\pi}{7}\right), \quad -\cos\left(\tfrac{\pi}{7}\right) + i \sin\left(\tfrac{\pi}{7}\right),$$
$$-\cos\left(\tfrac{\pi}{7}\right) - i \sin\left(\tfrac{\pi}{7}\right), \quad -\cos\left(\tfrac{3\pi}{7}\right) - i \sin\left(\tfrac{3\pi}{7}\right), \quad \cos\left(\tfrac{2\pi}{7}\right) - i \sin\left(\tfrac{2\pi}{7}\right).$$

By substituting these explicit expressions into the formula for the DFT$(A, 19)$ and separating the real and imaginary parts we obtain that

$$\begin{aligned}
&\Re(\mathrm{DFT}(A,19)) = \\
&\quad A_1 + \cos\left(\tfrac{2\pi}{7}\right)A_2 - \cos\left(\tfrac{3\pi}{7}\right)A_3 - \cos\left(\tfrac{\pi}{7}\right)A_4 - \cos\left(\tfrac{\pi}{7}\right)A_5 - \cos\left(\tfrac{3\pi}{7}\right)A_6 + \cos\left(\tfrac{2\pi}{7}\right)A_7, \\
&\Im(\mathrm{DFT}(A,19)) = \\
&\quad \sin\left(\tfrac{2\pi}{7}\right)A_2 + \sin\left(\tfrac{3\pi}{7}\right)A_3 + \sin\left(\tfrac{\pi}{7}\right)A_4 - \sin\left(\tfrac{\pi}{7}\right)A_5 - \sin\left(\tfrac{3\pi}{7}\right)A_6 - \sin\left(\tfrac{2\pi}{7}\right)A_7.
\end{aligned}$$

Taking the sum of the squares of $\Re(\mathrm{DFT}(A, 19))$ and $\Im(\mathrm{DFT}(A, 19))$, expanding and applying trigonometric simplification in Maple, we obtain the following expression for the power spectral density of A at lag 19:

$$\begin{aligned}
\mathrm{PSD}(A,19) &= A_1^2 + A_2^2 + A_3^2 + A_4^2 + A_5^2 + A_6^2 + A_7^2 + \\
&\quad + 2\big(A_1A_2 + A_2A_3 + A_3A_4 + A_4A_5 + A_5A_6 + A_6A_7 + A_7A_1\big)\sin\left(\tfrac{3\pi}{14}\right) \\
&\quad - 2\big(A_1A_3 + A_2A_4 + A_3A_5 + A_4A_6 + A_5A_7 + A_6A_1 + A_7A_2\big)\sin\left(\tfrac{\pi}{14}\right) \\
&\quad - 2\big(A_1A_4 + A_2A_5 + A_3A_6 + A_4A_7 + A_5A_1 + A_6A_2 + A_7A_3\big)\cos\left(\tfrac{\pi}{7}\right) \\
&= p_2(\mathcal{A}) + 2\sin\left(\tfrac{3\pi}{14}\right)\cdot \mathrm{PAF}(\mathcal{A},1) - 2\sin\left(\tfrac{\pi}{14}\right)\cdot \mathrm{PAF}(\mathcal{A},2) - 2\cos\left(\tfrac{\pi}{7}\right)\cdot \mathrm{PAF}(\mathcal{A},3) \\
&= p_2(\mathcal{A}) - \widehat{A^{19}}
\end{aligned}$$

where $\mathcal{A} = [A_1, \ldots, A_7]$ and where we made use of the trigonometric identity,

$$\sin\left(\tfrac{\pi}{14}\right) + \cos\left(\tfrac{\pi}{7}\right) - \sin\left(\tfrac{3\pi}{14}\right) = \frac{1}{2}.$$

Similarly, $\mathrm{PSD}(B, 19) = p_2(\mathcal{B}) - \widehat{B^{19}}$, so clearly $\mathrm{PSD}(A, 19)$ and $\mathrm{PSD}(B, 19)$ are integers. The above reasoning can also be applied to the other two integer multiples of 19, namely 38 and 57. ■

For the 3rd Legendre pair of length 133 we found, it can be seen that

$$\mathcal{A} = [1, 1, 1, 1, 1, 1, -5], \quad \mathcal{B} = [-1, -1, 5, -1, 5, 5, -11], \quad \widehat{A^{19}} = -5, \quad \widehat{B^{19}} = -33.$$

Therefore, by applying Proposition **??**, we obtain:

$$\begin{aligned}
\mathrm{PSD}(A, 19) &= p_2(\mathcal{A}) - \widehat{A^{19}} = 31 + 5 = 36, \\
\mathrm{PSD}(B, 19) &= p_2(\mathcal{B}) - \widehat{B^{19}} = 199 + 33 = 232.
\end{aligned}$$

For the 5th Legendre pair of length 133 we found, it can be seen that

$$\mathcal{A} = [1, 1, -3, 1, -3, -3, 7], \quad \mathcal{B} = [-5, -5, 5, -5, 5, 5, 1], \quad \widehat{A^{19}} = -13, \quad \widehat{B^{19}} = -25.$$

Therefore, by applying Proposition **??**, we obtain:

$$\begin{aligned} \mathrm{PSD}(A, 19) &= p_2(\mathcal{A}) - \widehat{A^{19}} = 79 + 13 = 92, \\ \mathrm{PSD}(B, 19) &= p_2(\mathcal{B}) - \widehat{B^{19}} = 151 + 25 = 176. \end{aligned}$$

4 Conclusion

We provide an update to the comprehensive list of open lengths for Legendre pairs, listed in [**?**]. The list in [**?**] is carefully constructed and corrects certain misprints and oversights by previous authors. In particular, we furnish the first ever examples of Legendre pairs of the three open lengths $117, 129, 133$. In the case of the two open lengths $117, 129$, we make extensive use of the determination of the complete spectrum of the (resp. 39-th, 43-rd) value of the Discrete Fourier Transform for Legendre pairs. In fact, we describe an algorithm that yields the complete spectrum of the $\frac{\ell}{3}$-rd value of the Discrete Fourier Transform for Legendre pairs of lengths $\ell \equiv 0 \pmod 3$. A Legendre pair of length $\ell = 77$ was reported in 2020 in [**?**]. Therefore, the state-of-the-art list of thirteen integers in the range < 200 for which the question of existence of Legendre pairs is still unresolved is:

$$85, 87, 115, 145, 147, 159, 161, 169, 175, 177, 185, 187, 195.$$

Twenty years after the fundamental paper [**?**] for Legendre pairs appeared, there are still interesting questions and open problems to ponder in this area.

References

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

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

[3] Jonathan Turner et al. personal communication. Dec 7, 2020.

[4] Roderick J. Fletcher, Marc Gysin, and Jennifer 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] Ilias S. Kotsireas, Christos Koukouvinos, and Jennifer Seberry. Weighing matrices and string sorting. *Ann. Comb.*, 13(3):305–313, 2009.

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

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

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