Quaternary Legendre pairs II

Ilias S. Kotsireas[1] Christoph Koutschan[2]
Arne Winterhof [2]

[1]CARGO Lab, Wilfrid Laurier University, Waterloo, ON N2L 3C5, Canada
[2]RICAM, Austrian Academy of Sciences, Altenberger Straße 69, 4040 Linz, Austria
e-mail: ikotsire@wlu.ca, christoph.koutschan@ricam.oeaw.ac.at, arne.winterhof@oeaw.ac.at

March 27, 2025

Abstract

Quaternary Legendre pairs are pertinent to the construction of quaternary Hadamard matrices and have many applications, for example in coding theory and communications.

In contrast to binary Legendre pairs, quaternary ones can exist for even length ℓ as well. It is conjectured that there is a quaternary Legendre pair for any even ℓ. The smallest open case until now had been $\ell = 28$, and $\ell = 38$ was the only length ℓ with $28 \le \ell \le 60$ resolved before. Here we provide constructions for $\ell = 28, 30, 32$, and 34. In parallel and independently, Jedwab and Pender found a construction of quaternary Legendre pairs of length $\ell = (q-1)/2$ for any prime power $q \equiv 1 \bmod 4$, which in particular covers $\ell = 30$, 36, and 40, so that now $\ell = 42$ is the smallest unresolved case.

The main new idea of this paper is a way to separate the search for the subsequences along even and odd indices which substantially reduces the complexity of the search algorithm.

In addition, we use Galois theory for cyclotomic fields to derive conditions which improve the PSD test.

Keywords. Legendre pair, Hadamard matrix, discrete Fourier transform, power spectral density, autocorrelation, cyclotomic field, Galois theory

1 Introduction

Two sequences

$$A = [a_0, a_1, \ldots, a_{\ell-1}], \quad B = [b_0, b_1, \ldots, b_{\ell-1}] \in \mathbb{C}^\ell$$

of period ℓ form a *Legendre pair* (A, B) if

$$\mathrm{PAF}(A, s) + \mathrm{PAF}(B, s) = -2, \quad s = 1, 2, \ldots, \left\lfloor \frac{\ell}{2} \right\rfloor, \tag{1}$$

where

$$\mathrm{PAF}(A, s) = \sum_{j=0}^{\ell-1} a_j \overline{a_{j+s}}, \quad s = 0, 1, \ldots, \ell - 1,$$

is the *periodic autocorrelation function* $\mathrm{PAF}(A, s)$ of A at lag s. (Note that (1) holds also true for $s = \left\lfloor \frac{\ell}{2} \right\rfloor + 1, \ldots, \ell - 1$ since $\mathrm{PAF}(A, \ell - s) = \overline{\mathrm{PAF}(A, s)}$ for $s = 1, 2, \ldots, \ell - 1$.)

Binary Legendre pairs (A, B) where $A, B \in \{-1, +1\}^\ell$ can be traced back to [2] and [8], see [5, 6] for the state of the art. In particular, the length of a binary Legendre pair must be odd, there are several known infinite classes and it is conjectured that a binary Legendre pair of length ℓ exists for any odd ℓ. The smallest unsettled case is $\ell = 115$.

Very recently [6], we started studying *quaternary* Legendre pairs (A, B), where

$$A, B \in \{-1, +1, -i, +i\}^\ell.$$

Quaternary Legendre pairs (qLPs) are pertinent to the construction of quaternary Hadamard matrices, see [6, Theorem 2.2]. In contrast to the binary case, quaternary Legendre sequences exist also for even ℓ. Since a binary sequence can be considered quaternary, we may restrict ourselves to even ℓ. In our previous paper [6] we constructed quaternary Legendre sequences for all even $\ell \leq 26$ as well as for $\ell = 38, 62, 74, 82$. Note that the latter three lengths are of the form $\ell = 2p$ with a prime such that $2p - 1$ is a sum of two squares, where a special *compressed* pair can be used as a starting point (for the concept of compression, see [6]). However, this idea cannot be used for any ℓ of a different form including $\ell = 28, 30, 32$ and 34.

In parallel and independently, Jedwab and Pender [4] constructed quaternary Legendre pairs of length $\ell = (q - 1)/2$ for every prime power $q \equiv 1 \bmod 4$ as well as of length $\ell = 2p$ for every prime $p > 2$ for which $2p - 1$ is a prime power. This covers $\ell = 30$ but not $\ell = 28$, 32 and 34.

Binary and quaternary Hadamard matrices and thus binary and quaternary Legendre pairs have many applications, for example in coding theory and communication, see for example [3].

In this paper we continue the search for quaternary Legendre pairs of even length ℓ. A new idea for any even ℓ is to separate the search for $[a_0, a_2, \ldots, a_{\ell-2}]$ and $[a_1, a_3, \ldots, a_{\ell-1}]$ or $[b_0, b_2, \ldots, b_{\ell-2}]$ and $[b_1, b_3, \ldots, b_{\ell-1}]$, respectively, which dramatically reduces the complexity of the search algorithm, see Section 3. In the case that ℓ is divisible by 4 we provide some additional speed-ups.

In addition, we also provide some further tests in Section 4 based on Galois theory of cyclotomic fields and a well-known condition for integers which are the square of the absolute value of an algebraic integer in a cyclotomic field.

We start with some preliminary results in Section 2. Our new constructions for $\ell = 28, 30, 32$ and 34 are given in Section 5. (Note that our construction of length 30 is different from the construction of [4].) Now the smallest open case is $\ell = 42$ and there are only 14 unresolved cases ≤ 100:

$$\ell = 42, 46, 52, 58, 64, 66, 70, 72, 76, 80, 88, 92, 94, 100.$$

2 Preliminaries

2.1 Quaternary Legendre pairs

Let $A = [a_0, a_1, \ldots, a_{\ell-1}]$, $B = [b_0, b_1, \ldots, b_{\ell-1}]$ be a quaternary Legendre pair of even length ℓ.

Balance

Put

$$\alpha = \sum_{j=0}^{\ell-1} a_j \quad \text{and} \quad \beta = \sum_{j=0}^{\ell-1} b_j.$$

By [6, Lemma 1] we may assume w.l.o.g.

$$\alpha = 0 \quad \text{and} \quad \beta = 1 + i. \tag{2}$$

DFT and the PSD-test

For an integer $n \geq 1$ we denote by ξ_n the primitive nth root of unity

$$\xi_n = e^{2\pi i/n}.$$

Note that we may fix any other primitive nth root of unity instead.

The *discrete Fourier transform* $\mathrm{DFT}(A, s)$ of A at s is

$$\mathrm{DFT}(A, s) = \sum_{j=0}^{\ell-1} a_j \xi_\ell^{js}, \quad s = 0, 1, \ldots, \ell - 1,$$

and the *power spectral density* $\mathrm{PSD}(A, s)$ of A at s is

$$\mathrm{PSD}(A, s) = |\,\mathrm{DFT}(A, s)|^2 = \sum_{j=0}^{\ell-1} \mathrm{PAF}(A, j)\xi_\ell^{js}.$$

A quaternary Legendre pair (A, B) satisfies

$$\mathrm{PSD}(A, s) + \mathrm{PSD}(B, s) = 2\ell + 2, \quad s = 1, 2, \ldots, \ell - 1. \tag{3}$$

For efficiency, we search for possible candidate sequences A and B separately. An important tool for this separation is the following *PSD-test*. The nonnegativity of the PSD and (3) imply that we must have

$$\mathrm{PSD}(A,s), \mathrm{PSD}(B,s) \le 2\ell + 2, \quad s = 1, 2, \ldots, \ell - 1, \tag{4}$$

which is an analog of the PSD-test for binary Legendre pairs introduced in [2]. Criterion (4) allows us to discard many sequences because they cannot be part of a Legendre pair. (Note that we have $\mathrm{PSD}(A, \ell - s) = \mathrm{PSD}(\overline{A}, s)$ which for binary sequences reduces the PSD-test (4) to $s = 1, 2, \ldots, \frac{\ell-1}{2}$. However, for quaternary sequences we need to check all $s = 1, 2, \ldots, \ell - 1$.)

2.2 Norms in cyclotomic fields

Let

$$\mathbb{Q}(\xi_n) = \left\{ a(\xi_n) = a_0 + a_1\xi_n + \cdots + a_{\varphi(n)-1}\xi_n^{\varphi(n)-1} : a_0, a_1, \ldots, a_{\varphi(n)-1} \in \mathbb{Q} \right\}$$

denote the nth *cyclotomic field*, where $\varphi(n)$ is Euler's totient function. For background on Galois theory and cyclotomic fields see for example [7, 10].

A condition for integers of the form $|\alpha|^2$ for some $\alpha \in \mathbb{Q}(\xi_n)$

We recall the following well-known condition, see for example [1, Theorem 3.1] which follows from [9, Lemma 3].

Lemma 1. *Suppose that $\alpha \in \mathbb{Q}(\xi_n)$ satisfies $|\alpha|^2 = m$ for an integer m, and that p is a rational prime dividing the square-free part of m. Denote by f the order of p modulo n if $\gcd(p, n) = 1$. Then either*

- *f is odd or*
- *f is even and $p^{f/2} \not\equiv -1 \bmod n$.*

For $n = 4$ we get the sum of two squares theorem.

Lemma 2. *Let $m = |\alpha|^2 \in \mathbb{Z}$ for some $\alpha \in \mathbb{Z}[i]$, then every rational prime divisor p of the square-free part of m is either $p = 2$ or $p \equiv 1 \bmod 4$.*

For $n = q > 2$ a prime, Lemma 1 simplifies to the following condition.

Lemma 3. *Let $q > 2$ be a prime. If $m = |\alpha|^2$ is an integer for some $\alpha \in \mathbb{Q}(\xi_q)$, then for every rational prime divisor p of the square-free part of m we have either $p = q$ or the order of p mod q is odd.*

For example, if $q \equiv 3 \bmod 4$, then the eligible p with $p \neq q$ are equivalent to a quadratic residue modulo q, and if $q = 2^s + 1$ is a Fermat prime, then either $p = q$ or $p \equiv 1 \bmod q$.

Norms and automorphisms in cyclotomic fields

The *automorphisms* ψ_j of $\mathbb{Q}(\xi_n)$ are

$$\psi_j(a(\xi_n)) = a(\xi_n^j), \quad \gcd(j,n) = 1,$$

and the group G_n of automorphisms is isomorphic to the multiplicative group $\mathbb{Z}_n^*$ of the residue class ring $\mathbb{Z}_n$ modulo n.

The *absolute norm* of $a(\xi_n)$ is

$$N(a(\xi_n)) = \prod_{\psi \in G_n} \psi(a(\xi_n)) = \prod_{\substack{j=1 \\ \gcd(j,n)=1}}^{n-1} a(\xi_n^j) \ \in \mathbb{Q}$$

and if $a(\xi_n) \in \mathbb{Z}[\xi_n]$ we get $N(a(\xi_n)) \in \mathbb{Z}$.

By the *Fundamental Theorem of Galois Theory* there is a bijection between the subgroups U of G_n and the subfields $\mathbb{F}$ of $\mathbb{Q}(\xi_n)$:

$$U \mapsto \mathbb{F} = \mathrm{Fix}(U) = \{\xi \in \mathbb{Q}(\xi_n) : \psi(\xi) = \xi \text{ for all } \psi \in U\}$$

and

$$\mathbb{F} \mapsto U = \mathrm{Aut}(\mathbb{F}) = \{\psi \in G_n : \psi(\xi) = \xi \text{ for all } \xi \in \mathbb{F}\},$$

respectively. The *relative norm* of $a(\xi_n) \in \mathbb{Q}(\xi_n)$ in $\mathrm{Fix}(U)$ is

$$N_U(a(\xi_n)) = \prod_{\psi \in U} \psi(a(\xi_n)) \ \in \mathrm{Fix}(U).$$

In particular, if $n \equiv 0 \bmod 4$, then $\mathbb{Q}(i)$ is a subfield of $\mathbb{Q}(\xi_n)$ and for

$$U_4 = \{\psi_{4j+1} : \gcd(4j+1, n) = 1\}$$

we get

$$N_{U_4}(a(\xi_n)) = \prod_{\substack{j=0 \\ \gcd(4j+1,n)=1}}^{n/4-1} a(\xi_n^{4j+1}) \ \in \mathbb{Q}(i), \tag{5}$$

since $i^{4j+1} = i$. Moreover, if some prime $p > 2$ divides n, then $\mathbb{Q}(\xi_p)$ is a subfield of $\mathbb{Q}(\xi_n)$ and for

$$U_p = \{\psi_{jp+1} : \gcd(jp+1, n) = 1\}$$

we get

$$N_{U_p}(a(\xi_n)) = \prod_{\substack{j=0 \\ \gcd(jp+1,n)=1}}^{n/p-1} a(\xi_n^{jp+1}) \ \in \mathbb{Q}(\xi_p),$$

since $\xi_p^{jp+1} = \xi_p$.

We have $\psi_{n-1} \notin U_4$ and $\psi_{n-1} \notin U_p$ for any prime divisor $p > 2$ of n since $n - 1 \equiv -1 \bmod 4p$. Note that

$$\psi_{n-1}(a(\xi_n)) = \overline{a(\xi_n)}, \quad \text{and} \quad a(\xi_n)\psi_{n-1}(a(\xi_n)) = |a(\xi_n)|^2,$$

and by the transitivity of the norm we get

$$N(a(\xi_n)) = \left|N_{U_4}(a(\xi_n))\right|^2.$$

In addition, write

$$b(\xi_p) = N_{U_p}(a(\xi_n)) \in \mathbb{Q}(\xi_p)$$

to obtain

$$N(a(\xi_n)) = \left| \prod_{j=1}^{(p-1)/2} b(\xi_p^j) \right|^2,$$

that is, the absolute norm of $b(\xi_p) \in \mathbb{Q}(\xi_p)$ equals the absolute norm of $a(\xi_n) \in \mathbb{Q}(\xi_n)$, again by the transitivity of the norm. Hence, for any $a(\xi_n) \in \mathbb{Z}[\xi_n]$ and for any prime divisor $p > 2$ of n, we have

$$N(a(\xi_n)) = |\alpha_4|^2 = |\alpha_p|^2 \in \mathbb{Z} \tag{6}$$

for some $\alpha_4 \in \mathbb{Q}(i)$ and some $\alpha_p \in \mathbb{Q}(\xi_p)$.

3 General ideas for even ℓ

Let ℓ be even. Conditions on PSD $\left(A, \frac{\ell}{2}\right)$ and PSD $\left(B, \frac{\ell}{2}\right)$ can be used to separate the search for $[a_0, a_2, \ldots, a_{\ell-2}]$ and $[a_1, a_3, \ldots, a_{\ell-1}]$, or $[b_0, b_2, \ldots, b_{\ell-2}]$ and $[b_1, b_3, \ldots, b_{\ell-1}]$, respectively. More precisely, put $k = \frac{\ell}{2}$, and let

$$\alpha_0 = \sum_{j=0}^{k-1} a_{2j}, \qquad \alpha_1 = \sum_{j=0}^{k-1} a_{2j+1}, \tag{7}$$

$$\beta_0 = \sum_{j=0}^{k-1} b_{2j}, \qquad \beta_1 = \sum_{j=0}^{k-1} b_{2j+1}. \tag{8}$$

Obviously, by (2) we have

$$\alpha = \alpha_0 + \alpha_1 = 0, \qquad \beta = \beta_0 + \beta_1 = 1 + i.$$

We get

$$\mathrm{PSD}(A, k) = \left| \sum_{j=0}^{\ell-1} a_j (-1)^j \right|^2 = |\alpha_0 - \alpha_1|^2 = 4|\alpha_0|^2 = 4|\alpha_1|^2$$

and

$$\mathrm{PSD}(B, k) = |\beta_0 - \beta_1|^2 = |2\beta_0 - 1 - i|^2 = |2\beta_1 - 1 - i|^2.$$

In particular,

$$\mathrm{PSD}(A, k) \quad \text{and} \quad \mathrm{PSD}(B, k) \quad \text{are sums of two integer squares.} \tag{9}$$

Let N_b be the number of elements $b \in \{-1, +1, -i, +i\}$ in the subsequence $[a_0, a_2, \ldots, a_{\ell-2}]$. Then

$$|\alpha_0|^2 = (N_1 - N_{-1})^2 + (N_i - N_{-i})^2 \equiv N_1 + N_{-1} + N_i + N_{-i} \equiv k \bmod 2 \quad (10)$$

and thus

$$\mathrm{PSD}(A, k) \equiv 4k \equiv 2\ell \bmod 8. \quad (11)$$

The conditions (3), (9), and (11) can now be used to construct a list of eligible pairs $\big(\mathrm{PSD}(A,k), \mathrm{PSD}(B,k)\big)$. This allows us to separate the search for $[a_0, a_2, \ldots, a_{\ell-2}]$ and $[a_1, a_3, \ldots, a_{\ell-1}]$ as well as for $[b_0, b_2, \ldots, b_{\ell-2}]$ and $[b_1, b_3, \ldots, b_{\ell-1}]$.

Example 4. For $\ell = 6$ there are two pairs

$$\big(\mathrm{PSD}(A,3), \mathrm{PSD}(B,3)\big) = \big(\mathrm{PSD}(A,3), 14 - \mathrm{PSD}(A,3)\big)$$

with $\mathrm{PSD}(A,3) \equiv 4 \bmod 8$, namely $(4, 10)$ and $(12, 2)$. However, since 12 is not the sum of two integer squares we must have

$$\big(\mathrm{PSD}(A,3), \mathrm{PSD}(B,3)\big) = (4, 10).$$

From now on, we assume that k is even, i.e., that ℓ is divisible by 4. In this case

$$\mathrm{DFT}\Big(A, \frac{\ell}{4}\Big),\ \mathrm{DFT}\Big(A, \frac{3\ell}{4}\Big),\ \mathrm{DFT}\Big(B, \frac{\ell}{4}\Big),\ \mathrm{DFT}\Big(B, \frac{3\ell}{4}\Big) \in \mathbb{Z}[i],$$

which means that

$$\mathrm{PSD}\Big(A, \frac{\ell}{4}\Big),\ \mathrm{PSD}\Big(A, \frac{3\ell}{4}\Big),\ \mathrm{PSD}\Big(B, \frac{\ell}{4}\Big),\ \mathrm{PSD}\Big(B, \frac{3\ell}{4}\Big) \quad (12)$$

are all sums of two integer squares.

Now put

$$\alpha'_j = \sum_{s=0}^{\ell/4-1} a_{4s+j}, \quad j = 0, 1, 2, 3.$$

Note that

$$\alpha'_0 + \alpha'_1 + \alpha'_2 + \alpha'_3 = \alpha = 0,$$

and

$$\begin{aligned} \alpha'_0 + \alpha'_2 &= \alpha_0, \\ \alpha'_1 + \alpha'_3 &= \alpha_1 = -\alpha_0. \end{aligned}$$

We get

$$\begin{aligned} \mathrm{PSD}\Big(A, \frac{\ell}{4}\Big) &= \big|\alpha'_0 - \alpha'_2 + (\alpha'_1 - \alpha'_3)i\big|^2 = \big|2\alpha'_0 - \alpha_0 + (2\alpha'_1 + \alpha_0)i\big|^2 \\ &\equiv 2|\alpha_0|^2 \equiv 0 \bmod 4 \end{aligned}$$

by employing (10), and by using the identity

$$|x+2y|^2 = |x|^2 + 4|y|^2 + 4\Re(x\overline{y}) \quad \text{with} \quad x = (i-1)\alpha_0.$$

Since we have

$$\mathrm{PSD}\Big(B, \frac{\ell}{4}\Big) = 2\ell + 2 - \mathrm{PSD}\Big(A, \frac{\ell}{4}\Big) \equiv 2 - \mathrm{PSD}\Big(A, \frac{\ell}{4}\Big) \bmod 8,$$

which in particular implies that $\mathrm{PSD}\big(B, \frac{\ell}{4}\big)$ is even, and since $\frac{1}{2}\,\mathrm{PSD}\big(B, \frac{\ell}{4}\big)$ is a sum of two squares, which by Lemma 2 is impossible if $\mathrm{PSD}\big(B, \frac{\ell}{4}\big) \equiv 6 \bmod 8$, we get

$$\mathrm{PSD}\Big(A, \frac{\ell}{4}\Big) \equiv 0 \bmod 8. \tag{13}$$

Write $\alpha_0 = u + iv$ with integers u and v. We will show that $u \equiv v \equiv 1 \bmod 2$ is not possible. Assume to the contrary that u and v are both odd. Write

$$\alpha_0' = x_0 + iy_0, \quad \alpha_1' = x_1 + iy_1, \quad x_0, y_0, x_1, y_1 \in \mathbb{Z},$$

and observe

$$x_0 + y_0 + x_1 + y_1 \equiv \frac{\ell}{2} \equiv 0 \bmod 2.$$

Hence,

$$\begin{aligned}\mathrm{PSD}\Big(A, \frac{\ell}{4}\Big) &= (2x_0 - u - 2y_1 - v)^2 + (2y_0 - v + 2x_1 + u)^2 \\ &= 4\big((x_0 - y_1)^2 + (y_0 + x_1)^2\big) - 4\big((x_0 - y_1)(u+v) - (x_1 + y_0)(u - v)\big) \\ &\quad + (u+v)^2 + (u-v)^2.\end{aligned}$$

Since $(x_0 - y_1)^2 + (y_0 + x_1)^2 \equiv x_0 + y_1 + y_0 + x_1 \equiv 0 \bmod 2$, and $u \pm v$ is even, we get

$$\mathrm{PSD}\Big(A, \frac{\ell}{4}\Big) \equiv (u+v)^2 + (u-v)^2 \equiv 2(u^2 + v^2) \bmod 8.$$

But our assumption that u and v are odd, that is $u^2 \equiv v^2 \equiv 1 \bmod 8$, implies that $\mathrm{PSD}\big(A, \frac{\ell}{4}\big) \equiv 4 \bmod 8$ which contradicts (13). Therefore, and because $u + v \equiv \frac{\ell}{2} \equiv 0 \bmod 2$, we obtain $u \equiv v \equiv 0 \bmod 2$, and consequently

$$\mathrm{PSD}\Big(A, \frac{\ell}{2}\Big) = 4|\alpha_0|^2 = 4(u^2 + v^2) \equiv 0 \bmod 16. \tag{14}$$

(Note that (13) is equivalent to [6, Theorem 3.2]. However, the proof in [6] was incomplete which is fixed now.)

Example 5. For $\ell = 32$ the pairs $\big(\mathrm{PSD}\big(A, \frac{\ell}{2}\big), \mathrm{PSD}\big(B, \frac{\ell}{2}\big)\big)$ with (14) are $(0, 66), (16, 50), (32, 34), (48, 18), (64, 2)$. However, since 48 and 66 are not sums of two squares, $(0, 66)$ and $(48, 18)$ are not eligible.
The eligible pairs $\big(\mathrm{PSD}\big(A, 8\big), \mathrm{PSD}\big(B, 8\big)\big)$ and $\big(\mathrm{PSD}\big(A, 24\big), \mathrm{PSD}\big(B, 24\big)\big)$ are given in Section 5.

We state the results of this section as a proposition.

Proposition 1. *Let ℓ be even and let (A, B) be a quaternary Legendre pair of length ℓ. Then the following three assertions hold:*

1. *We have the following condition on $\big(\mathrm{PSD}\big(A, \frac{\ell}{2}\big), \mathrm{PSD}\big(B, \frac{\ell}{2}\big)\big)$:*

$$\mathrm{PSD}\big(A, \tfrac{\ell}{2}\big) \equiv 2\ell \bmod 8, \quad \mathrm{PSD}\big(B, \tfrac{\ell}{2}\big) = 2\ell + 2 - \mathrm{PSD}\big(A, \tfrac{\ell}{2}\big),$$

   and both square-free parts of $\mathrm{PSD}\big(A, \frac{\ell}{2}\big)$ and $\mathrm{PSD}\big(B, \frac{\ell}{2}\big)$ are not divisible by a rational prime $p \equiv 3 \bmod 4$.

2. *The pairs (α_0, α_1) and (β_0, β_1), defined by (7) and (8), satisfy*

$$\mathrm{PSD}\big(A, \tfrac{\ell}{2}\big) = 4|\alpha_0|^2 = 4|\alpha_1|^2$$

   and

$$\mathrm{PSD}\big(B, \tfrac{\ell}{2}\big) = |2\beta_0 - 1 - i|^2 = |2\beta_1 - 1 - i|^2.$$

3. *If $\ell \equiv 0 \bmod 4$, then, in addition, we have*

$$\mathrm{PSD}\big(A, \tfrac{\ell}{2}\big) \equiv 0 \bmod 16,$$
$$\mathrm{PSD}\big(A, \tfrac{\ell}{4}\big) \equiv 0 \bmod 8,$$
$$\mathrm{PSD}\big(B, \tfrac{\ell}{4}\big) = 2\ell + 2 - \mathrm{PSD}\big(A, \tfrac{\ell}{4}\big)$$

   and both square-free parts of $\mathrm{PSD}\big(A, \frac{\ell}{4}\big)$ and $\mathrm{PSD}\big(B, \frac{\ell}{4}\big)$ are not divisible by a rational prime $p \equiv 3 \bmod 4$.

4 Condition for certain products of PSDs

Let $d > 1$ be a divisor of ℓ and let $n = \mathrm{lcm}(4, d)$. Then

$$\mathrm{DFT}\left(A, \frac{\ell}{d}\right) \in \mathbb{Z}[\xi_n].$$

By (5), (6) and

$$\mathrm{PSD}\left(A, \frac{\ell}{d}\right) = \left|\mathrm{DFT}\left(A, \frac{\ell}{d}\right)\right|^2$$

we have the absolute norm from $\mathbb{Q}(\xi_n)$ of the DFTs

$$N\left(\mathrm{DFT}\left(A, s\frac{\ell}{d}\right)\right) = \prod_{\substack{j=0 \\ \gcd(4j+s,n)=1}}^{n/4-1} \mathrm{PSD}\left(A, (4j + s \bmod d)\frac{\ell}{d}\right), \quad s \in \{1, 3\}.$$

Note that for $d \not\equiv 0 \bmod 4$ we get

$$N\left(\mathrm{DFT}\left(A, \frac{\ell}{d}\right)\right) = N\left(\mathrm{DFT}\left(A, 3\frac{\ell}{d}\right)\right)$$

since $4j+1 \equiv 3 \bmod d$ for some j. For $d \equiv 0 \bmod 4$ there is no solution j of $4j+1 \equiv 3 \bmod d$ and the factors of these products use different arguments of the DFTs.

By (6), Lemma 2 and Lemma 3 are applicable and we get the following result for products of PSDs, that is, absolute norms of DFTs.

Theorem 6. *Let $d > 1$ be any divisor of ℓ and let $n = \operatorname{lcm}(4, d)$. Then any prime divisor p of the square-free part of*

$$\begin{aligned}\prod_{\psi \in G_n} \psi\left(\mathrm{DFT}\left(A, \frac{\ell}{d}\right)\right) &= \prod_{\psi \in U_4} \psi\left(\mathrm{PSD}\left(A, \frac{\ell}{d}\right)\right) \\ &= \prod_{\substack{j=0 \\ \gcd(4j+1,n)=1}}^{n/4-1} \mathrm{PSD}\left(A, (4j+1 \bmod d)\frac{\ell}{d}\right) \in \mathbb{Z}\end{aligned}$$

is

$$p = 2 \quad \textit{or} \quad p \equiv 1 \bmod 4$$

and for any prime divisor $q > 2$ of n we have

$$p = q \quad \textit{or} \quad \textit{the order of } p \textit{ modulo } q \textit{ is odd.}$$

If $d \equiv 0 \bmod 4$, the same conditions are true for

$$\begin{aligned}\prod_{\psi \in G_n} \psi\left(\mathrm{DFT}\left(A, 3\frac{\ell}{d}\right)\right) &= \prod_{\psi \in U_4} \psi\left(\mathrm{PSD}\left(A, 3\frac{\ell}{d}\right)\right) \\ &= \prod_{\substack{j=0 \\ \gcd(4j+3,n)=1}}^{n/4-1} \mathrm{PSD}\left(A, (4j+3 \bmod d)\frac{\ell}{d}\right) \in \mathbb{Z}.\end{aligned}$$

Using the Chinese remainder theorem the different conditions modulo 4 and modulo p can be combined to one condition modulo

$$4\prod_{q|n} q,$$

where the product is taken over all odd prime divisors q of n.

For any sequence A the result is true but there may be no complementary B satisfying the condition for

$$\prod_{\substack{j=0 \\ \gcd(4j+s,n)}}^{n/4-1} \left(2\ell + 2 - \mathrm{PSD}\left(A, (4j+s \bmod d)\frac{\ell}{d}\right)\right).$$

Note that for $d = 2$ and $d = 4$ we get the tests of the previous section.

Example 7. For $\ell = 6$ and $d = 3$ or $d = 6$ we get $n = 12$ and any prime divisor p of the square-free parts of

$$\mathrm{PSD}(A, 2)\,\mathrm{PSD}(A, 4) \quad \text{and} \quad \mathrm{PSD}(A, 1)\,\mathrm{PSD}(A, 5)$$

must satisfy both conditions

$$\text{either} \quad p = 2 \quad \text{or} \quad p \equiv 1 \bmod 4$$

and

$$\text{either} \quad p = 3 \quad \text{or} \quad p \equiv 1 \bmod 3.$$

Since $2 \not\equiv 1 \bmod 3$ and $3 \not\equiv 1 \bmod 4$ and by the Chinese remainder theorem this is equivalent to $p \equiv 1 \bmod 12$.

We have $4^6 = 4096$ quaternary sequences of length 6. There are 100 sequences B with

$$b_0 = 1 \quad \text{and} \quad \beta = 1 + i.$$

By Example 4, we must have

$$\mathrm{PSD}(B, 3) = 10$$

and only 36 sequences B remain. 20 sequences B pass the PSD-test (4) and only 4 of them also the last PSD-tests of this example. All these B have the same PAFs, $\mathrm{PAF}(B, 1) = \mathrm{PAF}(B, 2) = 0$, $\mathrm{PAF}(B, 3) = -4$ and there are 12 sequences A with $a_0 = 1$ and the desirable PAFs, $\mathrm{PAF}(A, 1) = \mathrm{PAF}(A, 2) = -2$, $\mathrm{PAF}(A, 3) = 2$.

5 Legendre pairs for $\ell = 28, 30, 32$ and 34

In this section, we report some computational findings, namely quaternary Legendre pairs of the previously open lengths $28, 30$, and 32, that were made possible by the theoretical results presented in the previous sections. Our strategy is as follows: we fix an eligible pair $\big(\mathrm{PSD}\big(A, \frac{\ell}{2}\big), \mathrm{PSD}\big(B, \frac{\ell}{2}\big)\big)$, from which we can deduce the possible choices for $\alpha_0, \alpha_1, \beta_0, \beta_1$ (see Section 3). Fix one such choice and generate the set S_0 (resp. S_1) of all $\{+1, -1, +i, -i\}$-sequences of length $\ell/2$ whose sum equals α_0 (resp. α_1). Then $S_0 \times S_1$ (with suitable interlacing applied to each member) forms a set of candidate A-sequences. The same is done analogously and independently for the B-sequences. Certain optimizations can be implemented, such as modding out cyclic shifts and constant multiples of sequences, and precomputing the DFTs of the subsequences in S_0 and S_1 so that the DFT of a member of $S_0 \times S_1$ is obtained by a single addition.

The main point of our investigations, and the reason why such searches become feasible at all, is the fact that many of these candidate sequences can be filtered out at an early stage, i.e., before it is tried to find a corresponding partner sequence for a Legendre pair. In particular, we have the following tests at our disposal:

(T1) the PSD test (4),

(T2) the $\mathrm{PSD}\big(\cdot, \frac{\ell}{4}\big)$ and $\mathrm{PSD}\big(\cdot, \frac{3\ell}{4}\big)$ tests (13) in the case that ℓ is divisible by 4,

(T3) a set of product tests that arise from the results of Section 4.

We store only those candidate A- and B-sequences that pass all tests, and then try to find matches between them that form Legendre pairs.

5.1 The case $\ell = 28$

By (3), (9) and (14) there are only two eligible pairs $\big(\mathrm{PSD}(A,14), \mathrm{PSD}(B,14)\big)$:

$$(0,58),\ (32,26).$$

By (3), (12), (13) and Lemma 2 the eligible pairs $\big(\mathrm{PSD}(A,7), \mathrm{PSD}(B,7)\big)$, $\big(\mathrm{PSD}(A,21), \mathrm{PSD}(B,21)\big)$ are

$$(0,58),\ (8,50),\ (32,26),\ (40,18).$$

We also need that the prime divisors p of the square-free parts of the integers

$$\prod_{j=1}^{6} \big(58 - \mathrm{PSD}(A,4j)\big), \qquad \prod_{j=1}^{6} \big(58 - \mathrm{PSD}(B,4j)\big),$$

$$\prod_{\substack{j=0\\ j\neq 3}}^{6} \big(58 - \mathrm{PSD}(A,4j+2)\big), \qquad \prod_{\substack{j=0\\ j\neq 3}}^{6} \big(58 - \mathrm{PSD}(B,4j+2)\big),$$

$$\prod_{j\in\{1,5,9,13,17,25\}} \big(58 - \mathrm{PSD}(A,j)\big), \qquad \prod_{j\in\{1,5,9,13,17,25\}} \big(58 - \mathrm{PSD}(B,j)\big),$$

$$\prod_{j\in\{3,11,15,19,23,27\}} \big(58 - \mathrm{PSD}(A,j)\big), \qquad \prod_{j\in\{3,11,15,19,23,27\}} \big(58 - \mathrm{PSD}(B,j)\big)$$

are either $p = 2$ or $p \equiv 1, 9$ or $25 \bmod 28$.

We performed an exhaustive search for Legendre pairs of length 28, which means for $\big(\mathrm{PSD}(A,14), \mathrm{PSD}(B,14)\big) = (0,58)$ to generate 9,909,733,287,168 (resp. 5,164,090,709,778) candidates for the A- (resp. B-) sequences, while for $\big(\mathrm{PSD}(A,14), \mathrm{PSD}(B,14)\big) = (32,26)$ it means to generate 3,372,055,150,464 (resp. 11,618,309,811,108) candidates for the A- (resp. B-) sequences. To demonstrate the effectiveness of our tests, we look at the A-sequences of the latter case: after applying tests (T1) and (T2) only 1,028,107,232 sequences survive ($\sim 0.03\%$). This number can be further reduced by applying test (T3), after which only 289,305,112 sequences remain, that is, a further reduction by a factor 3.5 approximately. In total, we found 529,152 qLPs with $\mathrm{PSD}(A,14) = 0$ and 383,328 qLPs with $\mathrm{PSD}(A,14) = 32$. All of them satisfy the predicted properties from Theorem 6, of course. The total time to perform this search was about 46 CPU days.

Example 8. We get the Legendre pair

$$\begin{aligned} A = [&-1,-1,-i,-1,-i,-i,-i,1,i,-i,-1,1,i,1,\\ &-i,-1,-1,i,i,i,-i,i,1,1,i,i,-i,1],\\ B = [&-1,i,-i,1,i,-i,i,i,i,-1,-i,1,-i,-1,\\ &i,i,-i,i,-i,1,-i,1,1,-1,-i,-1,i,1], \end{aligned}$$

with the following PSD values at multiples of $\frac{\ell}{4}$:

$$\begin{aligned} (\mathrm{PSD}(A,14),\mathrm{PSD}(B,14)) &= (32,26),\\ (\mathrm{PSD}(A,7),\mathrm{PSD}(B,7)) &= (8,50),\\ (\mathrm{PSD}(A,21),\mathrm{PSD}(B,21)) &= (40,18). \end{aligned}$$

Moreover, we can verify that all PSD products satisfy our conditions:

$$\prod_{j=1}^{6} \mathrm{PSD}(A,4j) = 164204096 = 2^6 \cdot 7^2 \cdot 52361,$$

$$\prod_{j=1}^{6} \mathrm{PSD}(B,4j) = 315341888 = 2^6 \cdot 1933 \cdot 2549,$$

$$\prod_{\substack{j=0\\ j\neq 3}}^{6} \mathrm{PSD}(A,4j+2) = 340963904 = 2^6 \cdot 29 \cdot 183709,$$

$$\prod_{\substack{j=0\\ j\neq 3}}^{6} \mathrm{PSD}(B,4j+2) = 20892992 = 2^6 \cdot 29 \cdot 11257,$$

$$\prod_{j\in\{1,5,9,13,17,25\}} \mathrm{PSD}(A,j) = 120847168 = 2^6 \cdot 13^2 \cdot 11173,$$

$$\prod_{j\in\{1,5,9,13,17,25\}} \mathrm{PSD}(B,j) = 510607168 = 2^6 \cdot 7978237,$$

$$\prod_{j\in\{3,11,15,19,23,27\}} \mathrm{PSD}(A,j) = 288564032 = 2^6 \cdot 113 \cdot 39901,$$

$$\prod_{j\in\{3,11,15,19,23,27\}} \mathrm{PSD}(B,j) = 36675136 = 2^6 \cdot 757^2.$$

Note that all prime numbers p appearing in the square-free parts of the above products satisfy $p \equiv 1 \bmod 28$.

5.2 The case $\ell = 30$

There are only three eligible pairs for $\big(\mathrm{PSD}(A,15),\mathrm{PSD}(B,15)\big)$:

$$(4,58),\ (36,26),\ (52,10).$$

Moreover, we get the following conditions:

1. Any prime divisor p of the square-free parts of

$$\begin{aligned} &\mathrm{PSD}(A,10)\,\mathrm{PSD}(A,20), \quad \mathrm{PSD}(B,10)\,\mathrm{PSD}(B,20),\\ &\mathrm{PSD}(A,5)\,\mathrm{PSD}(A,25), \quad \mathrm{PSD}(B,5)\,\mathrm{PSD}(B,25) \end{aligned}$$

   satisfies $p \equiv 1 \bmod 12$.

2. Any prime divisor p of the square-free parts of

$$\begin{aligned} &\mathrm{PSD}(A,6)\,\mathrm{PSD}(A,12)\,\mathrm{PSD}(A,18)\,\mathrm{PSD}(A,24),\\ &\mathrm{PSD}(B,6)\,\mathrm{PSD}(B,12)\,\mathrm{PSD}(B,18)\,\mathrm{PSD}(B,24),\\ &\mathrm{PSD}(A,3)\,\mathrm{PSD}(A,9)\,\mathrm{PSD}(A,21)\,\mathrm{PSD}(A,27),\\ &\mathrm{PSD}(B,3)\,\mathrm{PSD}(B,9)\,\mathrm{PSD}(B,21)\,\mathrm{PSD}(B,27) \end{aligned}$$

   is $p = 5$ or satisfies $p \equiv 1 \bmod 20$.

3. Any prime divisor p of the square-free parts of

$$\prod_{\substack{j=1\\ \gcd(j,15)=1}}^{14} \mathrm{PSD}(A,2j), \qquad \prod_{\substack{j=1\\ \gcd(j,15)=1}}^{14} \mathrm{PSD}(B,2j),$$

$$\prod_{\substack{j=0\\ \gcd(2j+1,15)=1}}^{14} \mathrm{PSD}(A,2j+1), \qquad \prod_{\substack{j=0\\ \gcd(2j+1,15)=1}}^{14} \mathrm{PSD}(B,2j+1)$$

   satisfies $p \equiv 1 \bmod 60$.

Because of the computational complexity, we did not perform an exhaustive search for $\ell = 30$, but we stopped the computations as soon as some qLPs were found (that is, after about 65 hours in each of the three cases). We obtained 71 qLPs with $\mathrm{PSD}(A,15) = 4$, then 111 qLPs with $\mathrm{PSD}(A,15) = 36$, and finally 93 qLPs with $\mathrm{PSD}(A,15) = 52$. Here are two quaternary Legendre pairs for $\ell = 30$:

$$\begin{aligned} A = [&-1, i, -i, 1, -i, i, -i, -i, -i, i, i, -i, 1, -1, -i,\\ &i, i, 1, -i, -i, -i, -i, i, i, i, -1, i, i, i, -i],\\ B = [&-1, 1, -i, -i, i, -i, -i, i, -i, -1, i, 1, i, 1, i,\\ &i, -1, -i, i, -i, i, 1, i, 1, i, -1, -i, -i, 1, -1], \end{aligned}$$

and

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

A different Legendre pair of length 30 is given by Jedwab's and Pender's general construction [4]:

$$A = \left[\left(\frac{2-1}{61}\right), \left(\frac{2\cdot 4-1}{61}\right), \ldots, \left(\frac{2\cdot 4^{29}-1}{61}\right)\right],$$
$$B = \left[i, \left(\frac{4-1}{61}\right), \left(\frac{4^2-1}{61}\right), \ldots, \left(\frac{4^{29}-1}{61}\right)\right],$$

where $\left(\frac{\cdot}{\cdot}\right)$ is the Legendre symbol.

5.3 The case $\ell = 32$

The eligible values for $\big(\mathrm{PSD}(A,16), \mathrm{PSD}(B,16)\big)$ are

$$(16,50),\ (32,34),\ (64,2),$$

while for $\big(\mathrm{PSD}(A,8), (\mathrm{PSD}(B,8)\big)$ and $\big(\mathrm{PSD}(A,24), \mathrm{PSD}(B,24)\big)$ the eligible values are

$$(8,58),\ (16,50),\ (32,34),\ (40,26),\ (64,2).$$

Moreover, the integers

$$\begin{array}{ll}
\mathrm{PSD}(A,4)\,\mathrm{PSD}(A,20), & \mathrm{PSD}(B,4)\,\mathrm{PSD}(B,20),\\
\mathrm{PSD}(A,12)\,\mathrm{PSD}(A,28), & \mathrm{PSD}(B,12), \mathrm{PSD}(B,28),\\
\prod_{j=0}^{3} \mathrm{PSD}(A,8j+2), & \prod_{j=0}^{3} \mathrm{PSD}(B,8j+2),\\
\prod_{j=0}^{3} \mathrm{PSD}(A,8j+6), & \prod_{j=0}^{3} \mathrm{PSD}(B,8j+6),\\
\prod_{j=0}^{7} \mathrm{PSD}(A,4j+1), & \prod_{j=0}^{7} \mathrm{PSD}(B,4j+1),\\
\prod_{j=0}^{7} \mathrm{PSD}(A,4j+3), & \prod_{j=0}^{7} \mathrm{PSD}(B,4j+3)
\end{array}$$

are all sums of two squares and thus their square-free parts are not divisible by any prime $p \equiv 3 \bmod 4$.

Similar to $\ell = 30$ we did not perform an exhaustive search. In total, we identified 12 qLPs of length 32. Here are two quaternary Legendre pairs of length $\ell = 32$ with $\mathrm{PSD}(A,16) = 32$ and $\mathrm{PSD}(A,16) = 64$, respectively:,

$$\begin{aligned}
A = [&-1,-i,-i,-1,i,i,-1,-1,i,i,i,1,-i,-i,i,i,\\
&-i,i,-i,-i,-i,-i,-i,1,i,1,-i,1,i,i,-i,i],\\
B = [&-1,i,-i,1,i,-i,i,-i,-i,i,-i,-i,i,i,i,-i,\\
&i,-i,-1,1,i,-1,i,-i,i,1,-i,-i,-i,i,1,i],
\end{aligned}$$

and

$$\begin{aligned}A &= [1,-i,i,i,-1,i,i,1,1,-i,-1,i,-1,-i,1,1,\\ &\quad -1,i,-i,1,-1,1,-1,1,i,-i,-1,i,-i,-1,-i,-i],\\ B &= [i,1,1,1,i,1,1,-1,-i,-1,i,-1,-1,1,i,-i,\\ &\quad -i,-1,-1,1,-i,-1,-i,i,-i,1,i,i,-1,-1,1,1].\end{aligned}$$

5.4 The case $\ell = 34$

We have the following PSD-conditions,

$$(\mathrm{PSD}(A,17),\mathrm{PSD}(B,17)) \in \{(20,50),(36,34),(52,18),(68,2)\}$$

and any prime divisor p of the square-free parts of the integers

$$\prod_{j=1}^{16}(70-\mathrm{PSD}(A,2j)),\prod_{j=1}^{16}(70-\mathrm{PSD}(B,2j)),$$

$$\prod_{\substack{j=0\\ j\neq 8}}^{16}(70-\mathrm{PSD}(A,2j+1)),\prod_{\substack{j=0\\ j\neq 8}}^{16}(70-\mathrm{PSD}(B,2j+1)),$$

satisfies $p = 17$ or $p \equiv 1 \bmod 68$. We found 22 quaternary Legendre pairs of length 34, for example,

$$\begin{aligned}A &= [-1,i,-1,-1,-i,1,1,i,1,i,-i,-i,i,-i,-i,-i,-i,\\ &\quad -1,1,1,i,-i,-i,i,-i,i,-i,i,i,i,-1,i,i,-i],\\ B &= [-1,-i,-1,i,1,i,i,-i,-1,-i,i,1,1,-i,-i,i,-1,\\ &\quad i,-i,1,i,i,-i,-1,i,i,-i,i,-i,1,1,-i,-i,i],\end{aligned}$$

with

$$(\alpha_0,\beta_0) = (-3i,-1-2i)$$

and thus

$$(\mathrm{PSD}(A,17),\mathrm{PSD}(B,17)) = (36,34).$$

Acknowledgments

Christoph Koutschan was supported by the Austrian Science Fund (FWF): grant 10.55776/I6130.
Arne Winterhof was funded in part by the Austrian Science Fund (FWF): grant 10.55776/PAT4719224.
The authors would like to thank Jonathan Jedwab and Thomas Pender for pointing to their parallel and independent work [4].
The authors also would like to thank the anonymous referees for many very useful comments.
We dedicate this work to the memory of Douglas Adams.

References

[1] Brock, B.W.: Hermitian congruence and the existence and completion of generalized Hadamard matrices. J. Combin. Theory Ser. A 49 (1988), no.2, 233–261. https://doi.org/10.1016/0097-3165(88)90054-4

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

[3] Horadam, K.J.; Hadamard matrices and their applications. Princeton University Press, Princeton, NJ, 2007.

[4] Jedwab, J., Pender, T.: Two constructions of quaternary Legendre pairs of even length. arXiv:2408.08472

[5] Kotsireas, I.S., Koutschan, C., Bulutoğlu, D.A., Arquette, D.M., Turner, J., Ryan, K.J.: Legendre pairs of lengths $\ell \equiv 0 \pmod 5$. Spec. Matrices 11 (2023), Paper No. 20230105, 15 pp. https://doi.org/10.1515/spma-2023-0105

[6] Kotsireas, I.S., Winterhof, A.: Quaternary Legendre pairs. In: New Advances in Designs, Codes and Cryptography. Fields Inst. Commun. 86, 279–294, Springer, Cham, 2024. https://doi.org/10.1007/978-3-031-48679-1_15

[7] Lorenz, F.: Algebra. Vol. 1 Universitext, Springer, New York, 2006.

[8] Szekeres, G.: Tournaments and Hadamard matrices. Enseign. Math. (2) 15 (1969), 269–278.

[9] Turyn, R.J. Character sums and difference sets. Pacific J. Math. 15 (1965), 319–346.

[10] Washington, L.C.: Introduction to cyclotomic fields. Grad. Texts in Math. 83, Springer-Verlag, New York, 1997. https://doi.org/10.1007/978-1-4612-1934-7