Two Constructions of Quaternary Legendre Pairs of Even Length

Jonathan Jedwab and Thomas Pender

Department of Mathematics, Simon Fraser University, Burnaby BC V5A 1S6, Canada
jed@sfu.ca, tsp7@sfu.ca

15 August 2024

Abstract. We give the first general constructions of even length quaternary Legendre pairs: there is a quaternary Legendre pair of length $(q-1)/2$ for every prime power q congruent to 1 modulo 4, and there is a quaternary Legendre pair of length $2p$ for every odd prime p for which $2p-1$ is a prime power.

Keywords. Legendre pairs; quaternary Legendre pairs; Goethals–Seidel sequences; Hadamard matrices.
MSC 05B20, 05B30.

1. Introduction

The study of binary Legendre pairs has attracted renewed interest owing to recent theoretical and computational advances [**10**, **12**, **23**]. These objects were first systematically studied by Szekeres [**21**, **22**] and Whiteman [**26**] via the $\{+1, -1\}$ characteristic vectors of certain subsets of a cyclic group. Much of the motivation for studying binary Legendre pairs is because they can be used to construct binary Hadamard matrices and pairs of amicable Hadamard matrices [**18**, **19**]. Several constructions of infinite families of binary Legendre pairs are known [**5**, **7**, **16**, **21**, **22**, **26**].

Quaternary Legendre pairs were recently introduced by Kotsireas and Winterhof [**11**], and further studied by Kotsireas et al. [**13**], as a natural generalization of the binary case. These authors demonstrated that, analogously to the binary setting, quaternary Legendre pairs can be used to construct quaternary Hadamard matrices. Although they were not able to construct an infinite family of quaternary Legendre pairs of even length, they made the following conjecture based on numerical evidence.

CONJECTURE 1 (Kotsireas and Winterhof [**11**]). There exists a quaternary Legendre pair of even length $2N$ for every $N \geqq 1$.

We shall prove the following two results.

THEOREM 2. Let q be an odd prime power.

(i) (Szekeres [**21**]). If $q \equiv 3 \pmod 4$ then there exists a binary Legendre pair of length $(q-1)/2$.

(ii) If $q \equiv 1 \pmod 4$ then there exists a quaternary Legendre pair (a, b) of length $(q-1)/2$ for which a has only one imaginary element and b is binary.

THEOREM 3. Suppose p is an odd prime for which $2p-1$ is a prime power. Then there exists a quaternary Legendre pair (a, b) of length $2p$ for which b is binary.

Theorem 2 (ii) provides the first known construction of quaternary Legendre pairs for infinitely many even lengths. Theorem 3 does not necessarily provide quaternary Legendre pairs for infinitely many even lengths because, to our knowledge, it is an open question as to whether there are infinitely many primes p for which $2p-1$ is a prime power. (The number of such primes p that are at most 10^2, 10^3, 10^4, 10^5,

10^6, 10^7, 10^8 is 12, 42, 205, 1190, 7802, 56267, 423770. The following heuristic argument suggests that one might expect the stronger result that there are infinitely many primes p for which $2p-1$ is prime: by the Prime Number Theorem, the "probability" that an integer n is prime is approximately $1/\log n$; assuming independence, the "probability" that integers n and $2n-1$ are both prime is approximately $1/(\log n)^2$, and $\sum 1/(\log n)^2$ diverges.)

Prior to this paper, the smallest unresolved case of Conjecture 1 was length 36 [**11**, **13**]. In view of Theorems 2 and 3, the unresolved cases of Conjecture 1 of length at most 100 are now

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

The remainder of this paper is organized in the following way. Section 2 presents preliminary definitions and results, and Sections 3 and 4 describe the constructions establishing Theorems 2 and 3. Section 5 updates the unresolved cases of Conjecture 1 of length at most 100.

2. Background

Quadratic Character of GF(q)

Let q be an odd prime power. Our constructions make use of the multiplicative function χ over GF(q) defined by

$$\chi(\alpha)=\begin{cases}0 & \text{for } \alpha=0,\\ 1 & \text{for } \alpha \text{ a nonzero square in GF}(q),\\ -1 & \text{for } \alpha \text{ a non-square in GF}(q).\end{cases} \tag{1}$$

In other words, χ is the extended quadratic character of GF(q).

We shall use the following well-known properties of the function χ.

PROPOSITION 4. Let q be an odd prime power. Then

(i) ([**15**, Rem. 1.4.53].) $\sum_{h\in \mathrm{GF}(q)} \chi(h)=0$

(ii) ([**15**, Lem. 6.4.7]). $\sum_{h\in \mathrm{GF}(q)} \chi(h)\chi(h+d)=-1$ for fixed nonzero $d\in$ GF(q)

(iii) ([**15**, Prop. 1.2.23]). $\chi(-1)=(-1)^{(q-1)/2}$.

Sequences and their Correlations

Write i for the principal root of -1, and let $j=-i$. A *sequence* $a=(a_k)$ of length N is an N-tuple $(a_0, a_1, \ldots, a_{N-1})$ of complex numbers. The sequence a is *quaternary* if each a_k lies in $\{+1,\ i,\ -1,\ j\}$, it is *binary* if each a_k lies in $\{+1,\ -1\}$, and it is *ternary* if each a_k lies in $\{+1,\ 0,\ -1\}$.

Let $a=(a_k)$ and $b=(b_k)$ be sequences of length N. The *periodic cross-correlations* of a by b are defined as

$$R_{a,b}(u)=\sum_{k=0}^{N-1} a_k\overline{b_{k+u}} \qquad \text{for } u=0,\ 1,\ldots,\ N-1,$$

where the index $k+u$ is calculated modulo N. The *periodic autocorrelations* of a single sequence a are defined as $R_a(u)\equiv R_{a,a}(u)$.

A pair (a,b) of sequences is *complementary* if

$$R_a(u)+R_b(u)=0 \qquad \text{for all } u\neq 0.$$

A pair (a,b) of quaternary sequences is a *Legendre pair* if

$$R_a(u)+R_b(u)=-2 \qquad \text{for all } u\neq 0.$$

EXAMPLE 5. The length 10 sequences

$$\begin{aligned} a &= (\, i \; - \; j \;\; i \; + + + \; i \;\; j \, -), \\ b &= (- - + + - + - + + -) \end{aligned}$$

are easily verified to form a quaternary Legendre pair.

Two pairs of binary sequences $(w,\, x)$ and $(y,\, z)$ (all four sequences having the same length) form an *amicable set* if

$$R_{w,x}(u) + R_{y,z}(u) = R_{x,w}(u) + R_{z,y}(u) \qquad \text{for all } u \neq 0. \tag{2}$$

A length N binary sequence $(a_0,\, a_1, \ldots,\, a_{N-1})$ is *symmetric* if

$$a_k = a_{N-k} \quad \text{for all } k \neq 0.$$

OBSERVATION 6. Suppose w and x are length N symmetric binary sequences. Then

$$R_{w,x}(u) = R_{x,w}(u) \quad \text{for all } u = 0,\, 1, \ldots,\, N-1.$$

In Section 4, we will apply the Gray map to relate quaternary sequences to binary sequences. Recall the usual Gray map $\{+1,\, i,\, -1,\, j\} \to \{+1,\, -1\} \times \{+1,\, -1\}$ is defined by

$$\begin{aligned} +1 &\mapsto (+1,\, +1), \\ i &\mapsto (+1,\, -1), \\ -1 &\mapsto (-1,\, -1), \\ j &\mapsto (-1,\, +1). \end{aligned}$$

Given binary sequences w and x of length N, define $\mathscr{G}(w,\, x)$ to be the length N quaternary sequence

$$\frac{1}{2}(1+i)w + \frac{1}{2}(1+j)x, \tag{3}$$

whose elementwise image under the Gray map is (w, x). Krone and Sarwate [**14**] observed that a simple calculation yields

$$R_{\mathscr{G}(w,x)}(u) = \frac{1}{2}\Big(R_w(u) + R_x(u)\Big) + \frac{i}{2}\Big(R_{w,x}(u) - R_{x,w}(u)\Big) \qquad \text{for all } u \neq 0. \tag{4}$$

REMARK. (i) Fletcher et al. [**5**] showed that a binary Legendre pair $((a_k),\, (b_k))$ must have odd length and that it can be assumed that $\sum a_k = \sum b_k = 1$. It is (implicitly) conjectured in many papers that a binary Legendre pair exists for every odd length. The smallest open case is currently length 115 [**12**].

(ii) Kotsireas and Winterhof [**11**] showed that, in contrast to the binary case, a quaternary Legendre pair of even length can exist. It is therefore particularly interesting to construct even length quaternary Legendre pairs; for such pairs, we may assume that $\sum a_k = 1 + i$ and $\sum b_k = 0$ [**11**, Lemma 2.1]. Prior to this paper, the smallest open case of Conjecture 1 was length 36 [**11**, **13**].

Hadamard Matrices

A *quaternary Hadamard matrix* H of order N is an $N \times N$ matrix with entries in $\{+1,\, i,\, -1,\, j\}$ such that $HH^* = NI$. If the entries of H are further restricted to $\{+1,\, -1\}$, then the Hadamard matrix H is *binary* (often referred to simply as *real*). It is well-known [**8**, sec. 14.1] that the order of a binary Hadamard matrix is 1, 2, or a multiple of 4. Paley [**17**] conjectured in 1933 that there is a binary Hadamard matrix of every order divisible by 4. Since 2005, the smallest unresolved order is 668 [**9**].

There are many constructions of Hadamard matrices; one of the most productive uses complementary sequences.

Turyn [**24**] showed that if there is a quaternary Hadamard matrix of order M, then there is a binary Hadamard matrix of order $2M$ and so $M = 1$ or M is even. Furthermore, Turyn conjectured that there is a quaternary Hadamard matrix of every even order. Since 1993, it appears that the smallest unresolved order is 94 [**4**] (as quoted in [**11**]).

Suppose that Conjecture 1 is true. We briefly review how this would imply that both Turyn's conjecture on quaternary Hadamard matrices and Paley's conjecture on binary Hadamard matrices are true. Kotsireas and Winterhof [**11**] showed that if there is a quaternary Legendre pair of length M, then there is a quaternary Hadamard matrix of order $2M + 2$. It would follow that there is a quaternary Hadamard matrix of order $2(2N) + 2 = 2(2N + 1)$ for every $N \geqq 0$ (where the case $N = 0$ holds trivially). Now Turyn [**24**] also showed that if H is a quaternary Hadamard matrix of order M, then $\left(\begin{smallmatrix} + & + \\ + & - \end{smallmatrix}\right) \otimes H$ is a quaternary Hadamard matrix of order $2M$. We would therefore obtain a quaternary Hadamard matrix of order $2^r(2N + 1)$ for every $r \geqq 1$ and every $N \geqq 0$, proving Turyn's conjecture. This in turn would imply (by Turyn's first construction above) that there is a binary Hadamard matrix of order $2^{r+1}(2N + 1)$ for every $r \geqq 1$ and every $N \geqq 0$, proving Paley's conjecture.

3. The First Construction

Proof of Theorem 2

Let q be an odd prime power. Theorem $2(i)$ asserts the existence of a binary Legendre pair of odd length $(q - 1)/2$. This result is due to Szekeres [**21**], who constructed such pairs using cyclotomy. However, an earlier result due to Goethals and Seidel [**6**, Sect. 2] constructs a pair of ternary sequences of length $(q - 1)/2$, containing only a single zero element, whose nontrivial periodic autocorrelations sum to -2. We shall show that when $q \equiv 3 \pmod 4$ is odd, replacing the single zero element by 1 gives a binary Legendre pair of odd length $(q - 1)/2$ and so recovers Theorem $2(i)$; but when $q \equiv 1 \pmod 4$, replacing the single zero element by i gives a quaternary Legendre pair of even length $(q - 1)/2$ and proves Theorem $2(ii)$. Whereas the construction given in [**6**] relies on results due to Paley [**17**] and the geometry of finite projective planes, we now give a simple, direct, and self-contained proof of both parts of Theorem 2 that does not require geometric arguments.

Let g be a primitive element of GF(q), and define length $(q-1)/2$ sequences $a = (a_k)$ and $b = (b_k)$ by

$$a_k = \begin{cases} 1 & \text{for } k = 0 \text{ and } q \equiv 3 \pmod 4, \\ i & \text{for } k = 0 \text{ and } q \equiv 1 \pmod 4, \\ \chi(g^{2k} - 1) & \text{for } 0 < k < (q-1)/2, \end{cases}$$
$$b_k = \chi(g^{2k+1} - 1) \quad \text{for } 0 \leqq k < (q-1)/2$$

where the function χ is given in (1). Then b is a binary sequence; and a is a binary sequence if $q \equiv 3 \pmod 4$, and has only the imaginary element $a_0 = i$ if $q \equiv 1 \pmod 4$. It remains to show that (a, b) is a Legendre pair.

Fix $u \in \{1, 2, \ldots, (q-3)/2\}$. Then

$$\begin{aligned} R_a(u) + R_b(u) &= \sum_{k=0}^{(q-3)/2} (a_k \overline{a_{k+u}} + b_k \overline{b_{k+u}}) \\ &= a_0 a_u + a_{(q-1)/2-u} \overline{a_0} + \sum_{\substack{k=1 \\ k \neq (q-1)/2-u}}^{(q-3)/2} a_k a_{k+u} + \sum_{k=0}^{(q-3)/2} b_k b_{k+u}. \end{aligned} \tag{5}$$

We next show that $a_0a_u + a_{(q-1)/2-u}\overline{a_0} = 0$. By Proposition $4(iii)$ we have

$$a_{(q-1)/2-u} = \chi(g^{-2u} - 1) = \chi((-1)(g^{-u})^2(g^{2u} - 1)) = (-1)^{(q-1)/2}\chi(g^{2u} - 1) = (-1)^{(q-1)/2}a_u,$$

and so

$$\begin{aligned} a_0a_u + a_{(q-1)/2-u}\overline{a_0} &= \begin{cases} a_u - a_u & \text{for } q \equiv 3 \text{ (mod 4)}, \\ ia_u + a_u\bar{i} & \text{for } q \equiv 1 \text{ (mod 4)}. \end{cases} \\ &= 0, \end{aligned}$$

as claimed.

Substitute in (5) to give

$$\begin{aligned} R_a(u) + R_b(u) &= \sum_{\substack{k=1 \\ k\neq(q-1)/2-u}}^{(q-3)/2} \chi(g^{2k} - 1)\chi(g^{2k+2u} - 1) + \sum_{k=0}^{(q-3)/2} \chi(g^{2k+1} - 1)\chi(g^{2k+2u+1} - 1) \\ &= \sum_{\substack{m=1 \\ m\neq q-1-2u}}^{q-2} \chi(g^m - 1)\chi(g^{m+2u} - 1) \\ &= \sum_{m=0}^{q-2} \chi(g^m - 1)\chi(g^{m+2u} - 1) \end{aligned}$$

because $\chi(0) = 0$. Replace $g^m - 1$ by h and write $g^{m+2u} - 1$ as $g^{2u}(h + 1 - g^{-2u})$ so that

$$R_a(u) + R_b(u) = \sum_{\substack{h\in\mathrm{GF}(q) \\ h\neq-1}} \chi(h)\chi(h + 1 - g^{-2u}).$$

Then by Proposition $4(ii)$ we obtain

$$R_a(u) + R_b(u) = -1 - \chi(-1)\chi(-g^{-2u}) = -1 - \chi\big((g^{-u})^2\big) = -2,$$

as required. This completes the proof of Theorem 2.

Table 1 lists examples of even length quaternary Legendre pairs of length at most 40 obtained from Theorem $2(ii)$.

TABLE 1 . Quaternary Legendre pairs of even length $N \leq 40$ from Theorem $2(ii)$

N	Sequence Pair
2	$(\,i\,-)$ $(-+)$
4	$(\,i\,-+-)$ $(+--+)$
6	$(\,i\,+---+)$ $(-+--++)$
8	$(\,i\,+--+--+)$ $(-+++-+--)$
12	$(\,i\,-++--+--++-)$ $(+-+----++++-)$

Continuation of Table 1

N	Sequence Pair
14	$(i\ --++-+-+-++--)$ $(-++----+-++++-)$
18	$(i\ +-++-+-----+-++-+)$ $(-++-+++---+++---+-)$
20	$(i\ ---++-+-+++-+-++---)$ $(-++--+-++++----+-++-)$
24	$(i\ +--+-+++---+---+++-+--+)$ $(+-+--+++++-++--+-----++-)$
26	$(i\ -++++-+---+---+---+-++++-)$ $(-++----++-++-+-+--+--++++-)$
30	$(i\ ++--+----+++-+-+-+++----+--++)$ $(-+--+-+-----++--++--+++++-+-++)$
36	$(i\ +-++++-+-----++--+--++-----+-++++-+)$ $(-+---+---+++--+-++-+--+-++---+++-+++)$
40	$(i\ ---++-+--+++--+-+-+++-+-+--+++--+-++---)$ $(+---+------+++-+--+--++-++-+---++++++-++)$

4. The Second Construction

Overview of Proof of Theorem 3

The principal insight in the derivation of Theorem 3 is to apply the Gray map in order to reason about binary sequences. We begin by noting that combination of (4) with the definition (2) gives the following result.

PROPOSITION 7. Let w, x, y, and z be binary sequences of the same length. Then $\big(\mathscr{G}(w,x),\, \mathscr{G}(y,z)\big)$ is a quaternary Legendre pair if and only if $(w,\, x)$ and $(y,\, z)$ are an amicable set and

$$R_w(u) + R_x(u) + R_y(u) + R_z(u) = -4 \qquad \text{for all } u \neq 0. \tag{6}$$

EXAMPLE 8. Let

$$\begin{aligned} w &= (+--+++++--), \\ x &= (--+-+++-+-), \\ y &= (--++-+-++-), \\ z &= (--++-+-++-). \end{aligned}$$

Then $\mathscr{G}(w,\, x)$ and $\mathscr{G}(y,\, z)$ are the quaternary sequences $(a,\, b)$ of Example 5. We may verify Proposition 7 by checking directly that $(w,\, x)$ and $(y,\, z)$ are an amicable set and satisfy (6).

We shall use the following two propositions to construct binary sequences w, x, y, and z with the properties specified in Proposition 7, and thereby prove Theorem 3.

PROPOSITION 9. Suppose p is an odd prime for which $2p-1$ is a prime power. Then there exist symmetric binary sequences w and x of length $2p$ such that

$$R_w(u) + R_x(u) = \begin{cases} 4-4p & \text{for } u = p, \\ 0 & \text{for } u \notin \{0,\, p\}. \end{cases} \tag{7}$$

PROPOSITION 10. Let p be an odd prime. Then there exists a binary sequence y of length $2p$ such that

$$R_y(u) = \begin{cases} 2p-4 & \text{for } u = p, \\ -2 & \text{for } u \notin \{0, p\}. \end{cases} \tag{8}$$

We can now prove Theorem 3 in the following way. Suppose p is an odd prime for which $2p-1$ is a prime power. Let w and x be the length $2p$ symmetric binary sequences constructed in Proposition 9, and let y be the length $2p$ binary sequence constructed in Proposition 10. Since w and x are symmetric, Observation 6 gives that $(w,\, x)$ and $(y,\, y)$ form an amicable set. Furthermore, (7) and (8) imply that (6) is satisfied. It follows by Proposition 7 that $\big(\mathscr{G}(w,\, x),\, \mathscr{G}(y,\, y)\big)$, which is equal to

$$\big(\mathscr{G}(w,\, x),\, y\big), \tag{9}$$

is the required quaternary Legendre pair of length $2p$.

Our remaining task is to prove Propositions 9 and 10. In order to prove Proposition 9, we require a construction found in Goethals and Seidel [**6**, Sect. 2]. The properties of this construction were stated although not fully derived in [**6**], and the proof given there relies on results due to Paley [**17**]. We shall give a detailed, direct, and self-contained proof of this result.

REMARK. Binary sequences having the properties specified in Propositions 9 and 10 were constructed by Whiteman in [**27**] and [**28**], respectively, although his proof for Proposition 9 was difficult and rather opaque. Here, we prove both propositions by entirely elementary means.

Goethals–Seidel Sequences

Throughout this subsection, let q be a prime power where $q \equiv 1 \pmod 4$. We shall use the following result to prove Proposition 9.

RESULT 11 (Goethals and Seidel [**6**, Sect. 2]). There exists a pair of symmetric complementary ternary sequences $\big((a_k),\, (b_k)\big)$ of length $(1+q)/2$ for which the only zero element of the two sequences is a_0.

First, we describe how to construct the ternary sequences (a_k) and (b_k). Then we show they are symmetric and complementary.

Regard the quadratic extension GF(q^2) as a 2-dimensional vector space over GF(q), and let g be a primitive element of GF(q^2). Then $\{1,\, g\}$ is a basis for the vector space and we may represent its q^2 elements as length 2 column vectors over GF(q) with respect to this basis.

Consider the two commuting, invertible linear maps whose matrix forms with respect to the chosen basis $\{1,\, g\}$ are given by

$$V = \frac{1}{2}\begin{pmatrix} g^{q-1} + g^{1-q} & g^{\frac{1}{2}(1+q)}(g^{q-1} - g^{1-q}) \\ g^{-\frac{1}{2}(1+q)}(g^{q-1} - g^{1-q}) & g^{q-1} + g^{1-q} \end{pmatrix}, \quad W = \begin{pmatrix} 0 & g^{1+q} \\ 1 & 0 \end{pmatrix}.$$

Note that $g^{q-1} + g^{1-q}$ and $g^{\pm\frac{1}{2}(1+q)}(g^{q-1} - g^{1-q})$ and g^{1+q} are each elements of the base field GF(q) because they are roots of the defining polynomial $t^q - t$. Then by induction on $k \geqq 1$ we find that, for all integers k,

$$V^k = \frac{1}{2}\begin{pmatrix} g^{k(q-1)} + g^{k(1-q)} & g^{\frac{1}{2}(1+q)}\big(g^{k(q-1)} - g^{k(1-q)}\big) \\ g^{-\frac{1}{2}(1+q)}\big(g^{k(q-1)} - g^{k(1-q)}\big) & g^{k(q-1)} + g^{k(1-q)} \end{pmatrix} \tag{10}$$

and so

$$V^kW = \frac{1}{2}\begin{pmatrix} g^{\frac{1}{2}(1+q)}\big(g^{k(q-1)} - g^{k(1-q)}\big) & g^{1+q}\big(g^{k(q-1)} + g^{k(1-q)}\big) \\ g^{k(q-1)} + g^{k(1-q)} & g^{\frac{1}{2}(1+q)}\big(g^{k(q-1)} - g^{k(1-q)}\big) \end{pmatrix}. \tag{11}$$

Solving the characteristic equation for V shows that its eigenvalues are g^{q-1} and g^{1-q}. The smallest power of each of these eigenvalues that lies in the base field is $(1+q)/2$. Similar calculation shows that the eigenvalues of W are $\pm g^{\frac{1}{2}(1+q)}$, both of whose squares lie in the base field. Furthermore, the eigenvalues of $V^k W$ for $k = 0, 1, \ldots, (q-1)/2$ are $g^{\frac{1}{2}(1+q)} g^{k(q-1)}$ and $-g^{\frac{1}{2}(1+q)} g^{k(1-q)}$, both of which are not in the base field because $q \equiv 1 \pmod 4$. Set $x = \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$, and consider the set

$$\{x, Vx, \ldots, V^{\frac{q-1}{2}}x, Wx, VWx, \ldots, V^{\frac{q-1}{2}}Wx\} \tag{12}$$

of $1+q$ vectors, each of which is nonzero because V and W are invertible. No two vectors of this set are scalar multiples of each other, otherwise (because V and W commute, and $V^{(1+q)/2} = -I$ from (10)) we would obtain the contradiction that $(V^k - cI)x = 0$ or $(V^k W - cI)x = 0$ for some scalar c and some $k \in \{0, 1, \ldots, (q-1)/2\}$.

Writing the matrix whose columns are c_1 and c_2 as (c_1, c_2), we define the sequences (a_k) and (b_k) of length $(1+q)/2$ by

$$a_k = \chi \det(x, V^k x) \quad \text{and} \quad b_k = \chi \det(x, V^k W x) \quad \text{for } k = 0, 1 \ldots, (q-1)/2, \tag{13}$$

where the function χ is given in (1). Since $V^{\frac{1+q}{2}} = -I$ and $g^{k(q-1)} + g^{k(1-q)} = g^{-k(q-1)} + g^{-k(1-q)}$ and $g^{k(q-1)} - g^{k(1-q)} = -g^{-k(q-1)} + g^{-k(1-q)}$, it follows that

$$\chi \det(x, V^{\frac{1+q}{2}-k} W^l x) = \chi \det(x, -V^{-k} W^l x) = \chi \det(x, V^k W^l x) \quad \text{for } l = 0 \text{ and } 1,$$

so (a_k) and (b_k) are symmetric. Since no two of the elements of the set (12) are scalar multiples of each other, the only zero element of the two sequences is a_0. It remains to show these two sequences are complementary.

Write $V^k x = \left(\begin{smallmatrix} \alpha_k \\ \beta_k \end{smallmatrix}\right)$ and $V^k W x = \left(\begin{smallmatrix} \alpha_{(1+q)/2+k} \\ \beta_{(1+q)/2+k} \end{smallmatrix}\right)$ for $k = 0, 1, \ldots, (q-1)/2$. Note that for each $k \neq 0$, we have $\beta_k \neq 0$ and so $\alpha_k = \beta_k \gamma_k$ for some γ_k. Since V and W are invertible, each $\left(\begin{smallmatrix} \alpha_k \\ \beta_k \end{smallmatrix}\right)$ is nonzero and so corresponds to some nonzero element of GF(q^2). It follows that γ_k ranges over GF(q) as k ranges over $\{1, 2, \ldots, q\}$. This can be seen by observing that if $\gamma_k = \gamma_l$ for some $k \neq l$, then $\left(\begin{smallmatrix} \alpha_k \\ \beta_k \end{smallmatrix}\right) = \beta_k \left(\begin{smallmatrix} \gamma_k \\ 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} \alpha_l \\ \beta_l \end{smallmatrix}\right) = \beta_l \left(\begin{smallmatrix} \gamma_k \\ 1 \end{smallmatrix}\right)$ are scalar multiples of each other, contrary to what we have shown.

Fix $u \in \{1, 2, \ldots, (q-1)/2\}$, and write $V^{-u}x = \left(\begin{smallmatrix} v_0 \\ v_1 \end{smallmatrix}\right)$. Then, using that $\det(V^u) = 1$ and that χ and det are multiplicative functions, we find that

$$\begin{aligned}
R_a(u) + R_b(u) &= \sum_{k=0}^{(q-1)/2} (a_k a_{k+u} + b_k b_{k+u}) \\
&= \sum_{k=0}^{(q-1)/2} \Big(\chi \det(x, V^k x) \chi \det(x, V^{k+u} x) + \chi \det(x, V^k W x) \chi \det(x, V^{k+u} W x) \Big) \\
&= \sum_{k=0}^{(q-1)/2} \Big(\chi \det(x, V^k x) \chi \det(V^{-u} x, V^k x) + \chi \det(x, V^k W x) \chi \det(V^{-u} x, V^k W x) \Big) \\
&= \chi \det \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \chi \det \begin{pmatrix} v_0 & 1 \\ v_1 & 0 \end{pmatrix} + \sum_{k=1}^{q} \chi \det \begin{pmatrix} 1 & \alpha_k \\ 0 & \beta_k \end{pmatrix} \chi \det \begin{pmatrix} v_0 & \alpha_k \\ v_1 & \beta_k \end{pmatrix} \\
&= \sum_{k=1}^{q} \chi \det \begin{pmatrix} v_0 + v_1 \alpha_k & \alpha_k + \alpha_k \beta_k \\ v_1 \beta_k & \beta_k^2 \end{pmatrix} \\
&= \sum_{k=1}^{q} \chi (v_0 \beta_k^2 - v_1 \alpha_k \beta_k) \\
&= \sum_{k=1}^{q} \chi(\beta_k^2) \chi(v_0 - v_1 \gamma_k)
\end{aligned}$$

$$= \sum_{k=1}^{q} \chi(\upsilon_0 - \upsilon_1\gamma_k)$$

because β_k^2 is a quadratic residue in GF(q). As k ranges over $\{1, 2, \ldots, q\}$, we know that γ_k ranges over GF(q) and so $\upsilon_0 - \upsilon_1\gamma_k$ also ranges over GF(q) because $\upsilon_1 \neq 0$. We conclude from Proposition 4(i) that $R_a(u) + R_b(u) = 0$, as required.

EXAMPLE 12. Let $q = 25$. Realize GF(25^2) as the polynomial quotient ring GF(5)$[t]/(t^4 - t^2 - t + 2)$. Then

$$V = \begin{pmatrix} 2t^3 + 2t^2 + 2t - 2 & 2t^3 + 2t^2 + 2t - 2 \\ -t^3 - t^2 - t & 2t^3 + 2t^2 + 2t - 2 \end{pmatrix}, \quad W = \begin{pmatrix} 0 & t^3 + t^2 + t - 2 \\ 1 & 0 \end{pmatrix}$$

and

$$\begin{aligned}
x &= \begin{pmatrix} 1 \\ 0 \end{pmatrix}, & Wx &= \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \\
Vx &= \begin{pmatrix} 2t^3 + 2t^2 + 2t - 2 \\ -t^3 - t^2 - t \end{pmatrix}, & VWx &= \begin{pmatrix} 2t^3 + 2t^2 + 2t - 2 \\ 2t^3 + 2t^2 + 2t - 2 \end{pmatrix}, \\
V^2x &= \begin{pmatrix} -t^3 - t^2 - t - 2 \\ -t^3 - t^2 - t + 2 \end{pmatrix}, & V^2Wx &= \begin{pmatrix} -t^3 - t^2 - t - 1 \\ -t^3 - t^2 - t - 2 \end{pmatrix}, \\
V^3x &= \begin{pmatrix} -t^3 - t^2 - t + 2 \\ -2t^3 - 2t^2 - 2t - 1 \end{pmatrix}, & V^3Wx &= \begin{pmatrix} -2t^3 - 2t^2 - 2t - 2 \\ -t^3 - t^2 - t + 2 \end{pmatrix}, \\
V^4x &= \begin{pmatrix} -2t^3 - 2t^2 - 2t + 1 \\ 1 \end{pmatrix}, & V^4Wx &= \begin{pmatrix} t^3 + t^2 + t - 2 \\ -2t^3 - 2t^2 - 2t + 1 \end{pmatrix}, \\
V^5x &= \begin{pmatrix} -2t^3 - 2t^2 - 2t - 2 \\ t^3 + t^2 + t + 2 \end{pmatrix}, & V^5Wx &= \begin{pmatrix} -2 \\ -2t^3 - 2t^2 - 2t - 2 \end{pmatrix}, \\
V^6x &= \begin{pmatrix} 2t^3 + 2t^2 + 2t + 1 \\ -t^3 - t^2 - t - 1 \end{pmatrix}, & V^6Wx &= \begin{pmatrix} t^3 + t^2 + t \\ 2t^3 + 2t^2 + 2t + 1 \end{pmatrix}, \\
V^7x &= \begin{pmatrix} -2t^3 - 2t^2 - 2t - 1 \\ -t^3 - t^2 - t - 1 \end{pmatrix}, & V^7Wx &= \begin{pmatrix} t^3 + t^2 + t \\ -2t^3 - 2t^2 - 2t - 1 \end{pmatrix}, \\
V^8x &= \begin{pmatrix} 2t^3 + 2t^2 + 2t + 2 \\ t^3 + t^2 + t + 2 \end{pmatrix}, & V^8Wx &= \begin{pmatrix} -2 \\ 2t^3 + 2t^2 + 2t + 2 \end{pmatrix}, \\
V^9x &= \begin{pmatrix} 2t^3 + 2t^2 + 2t - 1 \\ 1 \end{pmatrix}, & V^9Wx &= \begin{pmatrix} t^3 + t^2 + t - 2 \\ 2t^3 + 2t^2 + 2t - 1 \end{pmatrix}, \\
V^{10}x &= \begin{pmatrix} t^3 + t^2 + t - 2 \\ -2t^3 - 2t^2 - 2t - 1 \end{pmatrix}, & V^{10}Wx &= \begin{pmatrix} -2t^3 - 2t^2 - 2t - 2 \\ t^3 + t^2 + t - 2 \end{pmatrix}, \\
V^{11}x &= \begin{pmatrix} t^3 + t^2 + t + 2 \\ -t^3 - t^2 - t + 2 \end{pmatrix}, & V^{11}Wx &= \begin{pmatrix} -t^3 - t^2 - t - 1 \\ t^3 + t^2 + t + 2 \end{pmatrix}, \\
V^{12}x &= \begin{pmatrix} -2t^3 - 2t^2 - 2t + 2 \\ -t^3 - t^2 - t \end{pmatrix}, & V^{12}Wx &= \begin{pmatrix} 2t^3 + 2t^2 + 2t - 2 \\ -2t^3 - 2t^2 - 2t + 2 \end{pmatrix}.
\end{aligned}$$

The symmetric length 13 sequences defined by (13) are then calculated to be

$$\begin{aligned}
a &= (0 - - - + - + + - + - - -), \\
b &= (+ + - - - + - - + - - - +).
\end{aligned}$$

Note from (1) that for nonzero $\alpha \in$ GF(25), we have $\chi(\alpha) = 1$ exactly when $\alpha = \beta^2$ for some $\beta \in$ GF(25). We can determine all such α by calculating the squares of those elements $\beta \in$ GF(25^2) for which $\beta^{24} = 1$.

REMARK. (i) It is stated in Theorem 2.3 of Goethals and Seidel [**6**] that the construction leading to Result 11 also holds in the case that $q \equiv -1 \pmod 4$. However, Corneil and Mathon noted in [**20**, p. 260, footnote] that a nonexistence result for a particular parameter family of strongly regular graphs due to Bussemaker et al. [**1**] shows this to be false. We note here, however, that the failure of the construction for $q \equiv -1 \pmod 4$ follows more simply by observing the form (11). Taking $k = (1+q)/4$, one has that $V^{\frac{1}{4}(1+q)}W = g^{\frac{1}{4}(1+q)^2}I$. Therefore, there are two nonzero vectors in the set (12) that are scalar multiples of each other, and the construction fails.

For a corrected construction in the case that $q \equiv -1 \pmod 4$, see de Launey [**2**] which considers the linear maps $\alpha \mapsto g^2\alpha$ and $\alpha \mapsto g\alpha^q$; see the monograph by de Launey and Flannery [**3**, chap. 18] for more discussion. In this case, in order to construct the desired pairs of ternary sequences one must consider the negaperiodic autocorrelations; see Seberry [**18**, chap. 4] for the relevant definitions.

(ii) Turyn [**25**] constructed ternary sequences having the same properties stated in Result 11, but instead considered the maps $\alpha \mapsto g^4\alpha$ and $\alpha \mapsto g^{\frac{1+q}{2}}\alpha$. It appears that the construction due to Goethals and Seidel [**6**] predates that of Turyn's. See Hall [**8**, sec. 14.3] for a full discussion of Turyn's construction.

(iii) A further construction of sequences satisfying Result 11, subsequent to the work of Goethals and Seidel [**6**] and Turyn [**25**], was given by Whiteman [**27**] using the field trace of a quadratic extension.

Proof of Proposition 9

We now are ready to provide the proof of Proposition 9.

Suppose p is an odd prime for which $q = 2p-1$ is a prime power. Since $q \equiv 1 \pmod 4$, by Result 11 there are symmetric complementary ternary sequences $a = (a_k)$ and $b = (b_k)$ of length p for which the only zero element is a_0. Define length $2p$ binary sequences $w = (w_k)$ and $x = (x_k)$ by

$$w_k = \begin{cases} 1 & \text{for } k \in \{0, p\}, \\ (-1)^k a_{k \bmod p} & \text{for } 0 < k < 2p \text{ and } k \neq p, \end{cases} \tag{14}$$

$$x_k = (-1)^k b_{k \bmod p} \quad \text{for } 0 \leqq k < 2p. \tag{15}$$

The symmetry of a and b implies that of w and x, so we need only prove (7).

Consider firstly the sequence x. For $0 < u < 2p$, we have

$$\begin{aligned} R_x(u) &= \sum_{k=0}^{2p-1} x_k x_{(k+u) \bmod 2p} \\ &= \sum_{k=0}^{2p-1} (-1)^k b_{k \bmod p} (-1)^{k+u} b_{(k+u) \bmod p} \\ &= 2(-1)^u \sum_{k=0}^{p-1} b_k b_{(k+u) \bmod p} \\ &= 2(-1)^u R_b(u \bmod p). \end{aligned}$$

Now consider the sequence w. Since $a_0 = 0$, we have

$$\begin{aligned} R_w(p) &= \sum_{k=0}^{2p-1} w_k w_{(k+p) \bmod 2p} \\ &= w_0 w_p + w_p w_0 + \sum_{\substack{k=0 \\ k \notin \{0,p\}}}^{2p-1} w_k w_{(k+p) \bmod 2p} \\ &= 1 + 1 + \sum_{k=0}^{2p-1} (-1)^k a_{k \bmod p} (-1)^{k+p} a_{(k+p) \bmod p} \end{aligned}$$

$$
\begin{aligned}
&= 2 + 2(-1)^p \sum_{k=0}^{p-1} a_k^2 \\
&= 4 - 2p.
\end{aligned}
$$

For $0 < u < 2p$ and $u \neq p$, using $a_0 = 0$ again we have

$$
\begin{aligned}
R_w(u) &= \sum_{k=0}^{2p-1} w_k w_{(k+u) \bmod 2p} \\
&= w_0 w_u + w_{(p-u) \bmod 2p} w_p + w_p w_{(p+u) \bmod 2p} + w_{2p-u} w_0 \\
&\qquad + \sum_{\substack{k=0 \\ k \notin \{0,\, (p-u) \bmod 2p,\, p,\, 2p-u\}}}^{2p-1} w_k w_{(k+u) \bmod 2p} \\
&= (-1)^u a_{u \bmod p} + (-1)^{p-u} a_{(-u) \bmod p} + (-1)^{p+u} a_{u \bmod p} + (-1)^{-u} a_{(-u) \bmod p} \\
&\qquad + \sum_{k=0}^{2p-1} (-1)^k a_{k \bmod p} (-1)^{k+u} a_{(k+u) \bmod p} \\
&= 2(-1)^u R_a(u \bmod p).
\end{aligned}
$$

Combining results, we find that

$$
R_w(p) + R_x(p) = (4 - 2p) + 2(-1)^p p = 4 - 4p
$$

and that, for $0 < u < 2p$ and $u \neq p$,

$$
R_w(u) + R_x(u) = 2(-1)^u \Big(R_a(u \bmod p) + R_b(u \bmod p) \Big) = 0
$$

because a, b are complementary. This establishes (7) and so completes the proof of Proposition 9.

EXAMPLE 13. Let $p = 13$. Apply the construction of Proposition 9 to the sequences a and b of Example 12 to obtain the symmetric binary length 26 sequences

$$
\begin{aligned}
w &= (++-++++----+-+-+----++++-+), \\
x &= (+--+---+++-++-++-+++---+--).
\end{aligned}
$$

Proof of Proposition 10

The proof is similar to that for the sequence w in the proof of Proposition 9 and so is abbreviated. Let p be an odd prime and define the ternary sequence $c = (c_k)$ of length p by

$$
c_k = \chi(k),
$$

where the function χ is given in (1) with $q = p$. Then the only zero element of c is c_0, and by Proposition 4(ii) we have

$$
R_c(u) = \begin{cases} p-1 & \text{for } u = 0, \\ -1 & \text{for } 0 < u < p. \end{cases}
$$

Define the length $2p$ binary sequence $y = (y_k)$ by

$$
y_k = \begin{cases} 1 & \text{for } k = 0, \\ -1 & \text{for } k = p, \\ c_{k \bmod p} & \text{for } 0 < k < 2p \text{ and } k \neq p. \end{cases} \tag{16}
$$

Then

$$\begin{aligned}
R_y(p) &= y_0 y_p + y_p y_0 + \sum_{\substack{k=0\\ k\notin\{0,p\}}}^{2p-1} y_k y_{(k+p) \bmod 2p} \\
&= -1 - 1 + 2\sum_{k=0}^{p-1} c_k^2 \\
&= 2p - 4,
\end{aligned}$$

and for $0 < u < 2p$ and $u \neq p$ we have

$$\begin{aligned}
R_y(u) &= y_u - y_{(p-u) \bmod 2p} - y_{(p+u) \bmod 2p} + y_{2p-u} + \sum_{k=0}^{2p-1} c_{k \bmod p} c_{(k+u) \bmod p} \\
&= c_{u \bmod p} - c_{(-u) \bmod p} - c_{u \bmod p} + c_{(-u) \bmod p} + 2R_c(u \bmod p) \\
&= -2,
\end{aligned}$$

as required. This completes the proof of Proposition 10.

EXAMPLE 14. Let $p = 13$. Apply the construction of Proposition 10 to the ternary sequence

$$c = (0 + - + + - - - - + + - +)$$

to obtain the binary length 26 sequence

$$y = (+ + - + + - - - - + + - + - + - + + - - - - + + - +).$$

(This sequence y is symmetric because $p \equiv 1 \pmod 4$.) Let w, x be the length 26 binary sequences constructed in Example 13. As noted after Proposition 10, the binary sequence y and the quaternary sequence

$$\mathscr{G}(w,\, x) = (+ \ i \ - + \ i \ \ i \ \ i \ \ j \ \ j \ \ j \ - + \ j \ \ i \ \ j \ + - \ j \ \ j \ \ j \ \ i \ \ i \ \ i \ + - i\,)$$

together form a quaternary Legendre pair of length 26.

REMARK. Recall that Theorem 3 is proved using a sequence pair $\big(\mathscr{G}(w,x), y\big)$ (see (9)), where the quaternary sequence $\mathscr{G}(w,x)$ is constructed via Proposition 9 and the binary sequence y is constructed via Proposition 10. Kotsireas and Winterhof [**11**] found examples of quaternary Legendre pairs for lengths 38, 62, 74, and 82 in the following way (each of these lengths being covered by the construction of Theorem 3). Let p be an odd prime. Seek a quaternary length $2p$ sequence $a = (a_k)$ computationally which satisfies

$$a_k + a_{k+p} = \begin{cases} 1+i & \text{for } k = 0, \\ 0 & \text{for } 0 < k < p, \end{cases} \tag{17}$$

and which forms a Legendre pair with the same binary sequence y as specified in (16).

We now show that the sequence $a = (a_k) = \mathscr{G}(w,x)$ constructed via Proposition 9 satisfies condition (17), so we can regard Theorem 3 as realizing the construction procedure proposed in [**11**] for all odd primes p for which $2p-1$ is a prime power and so removing the necessity for computational search. By the definition (3) of the map $\mathscr{G}$ we have

$$a_k + a_{k+p} = \frac{1}{2}(1+i)(w_k + w_{k+p}) + \frac{1}{2}(1+j)(x_k + x_{k+p}) \quad \text{for } 0 \leqq k < p.$$

Using the definition of w and x given in (14) and (15), we calculate

$$a_0 + a_p = \frac{1}{2}(1+i)(1+1) + \frac{1}{2}(1+j)(1-1) = 1 + i,$$

and

$$a_k + a_{k+p} = \frac{1}{2}(1+i)(w_k - w_k) + \frac{1}{2}(1+j)(x_k - x_k) = 0 \quad \text{for } 0 < k < p,$$

so condition (17) is satisfied.

Table 2 lists examples of even length quaternary Legendre pairs of length at most 40 obtained from Theorem 3.

TABLE 2 . Quaternary Legendre pairs of even length $N \leq 40$ from Theorem 3

N	Sequence Pair
6	$(+ + - \ i \ - +)$ $(+ + - - + -)$
10	$(+ + \ i \ j \ - \ i \ - \ j \ i \ +)$ $(+ + - - + - + - - +)$
14	$(+ - - \ i \ j \ + + \ i \ + + \ j \ i \ - -)$ $(+ + + - + - - - + + - + - -)$
26	$(+ \ i \ - + \ i \ i \ i \ j \ j \ j \ - + \ j \ i \ j \ + - \ j \ j \ j \ i \ i \ i \ + - \ i)$ $(+ + - + + - - - - + + - + - + - + + - - - - + + - +)$
38	$(+ \ i \ i \ - \ i \ - \ j \ j \ i \ + - \ j \ i \ i \ + \ j \ + \ j \ j \ i \ j \ j \ + \ j \ + \ i \ i \ j \ - + \ i \ j \ j \ - \ i \ - \ i \ i)$ $(+ + - - + + + + - + - + - - - - + + - - + - - + + + + - + - + - - - - + + -)$

5. Open Cases

Theorem 2 provides a quaternary Legendre pair for each of these even lengths at most 100:

$$2, 4, 6, 8, 12, 14, 18, 20, 24, 26, 30, 36, 40, 44, 48, 50, 54, 56, 60, 62, 68, 74, 78, 84, 86, 90, 96, 98.$$

Theorem 3 provides a quaternary Legendre pair for each of these even lengths at most 100:

$$4, \ 6, \ 10, \ 14, \ 26, \ 38, \ 62, \ 74, \ 82.$$

Examples for lengths 16, 22, 28, 32, 34 were given in [**11**, **13**]. The unresolved cases of Conjecture 1 of length at most 100 are therefore now

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

Acknowledgements

We are grateful to Ilias Kotsireas, Christoph Koutschan, and Arne Winterhof for helpful comments on the manuscript and for kindly providing a copy of [**13**] in which quaternary Legendre pairs of lengths 28, 30, 32, and 34 are constructed computationally.

References

1. F. C. Bussemaker, W. H. Haemers, R. Mathon, and H. A. Wilbrink. A $(49, 16, 3, 6)$ strongly regular graph does not exist. *European J. Combin.*, 10(5):413–418, 1989.

2. W. de Launey. On a family of cocyclic Hadamard matrices. In *Codes and Designs (Columbus, OH, 2000)*, volume 10 of *Ohio State Univ. Math. Res. Inst. Publ.*, pages 187–205. de Gruyter, Berlin, 2002.

3. W. de Launey and D. Flannery. *Algebraic Design Theory*, volume 175 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2011.

4. D. Ž. Đoković. Good matrices of orders 33, 35 and 127 exist. *J. Comb. Math. Comb. Comput.*, 14: 145–152, 1993.

5. 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.

6. J.-M. Goethals and J. J. Seidel. Orthogonal matrices with zero diagonal. *Canadian J. Math.*, 19: 1001–1010, 1967.

7. S. W. Golomb and G. Gong. *Signal Design for Good Correlation*. Cambridge University Press, Cambridge, 2005. For wireless communication, cryptography, and radar.

8. M. Hall, Jr. *Combinatorial Theory*. Wiley-Interscience Series in Discrete Mathematics. John Wiley & Sons, Inc., New York, second edition, 1986. A Wiley-Interscience Publication.

9. H. Kharaghani and B. Tayfeh-Rezaie. A Hadamard matrix of order 428. *J. Combin. Des.*, 13(6): 435–440, 2005.

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

11. I. S. Kotsireas and A. Winterhof. Quaternary Legendre pairs. In C. J. Colbourn and J. H. Dinitz, editors, *New Advances in Designs, Codes and Cryptography, Fields Institute Communications 86*, pages 289–304. Springer Nature, Switzerland, 2024.

12. I. S. Kotsireas, C. Koutschan, D. A. Bulutoglu, D. M. Arquette, J. S. Turner, and K. J. Ryan. Legendre pairs of lengths $\ell \equiv 0 \pmod 5$. *Spec. Matrices*, 11:Paper No. 20230105, 15, 2023.

13. I. S. Kotsireas, C. Koutschan, and A. Winterhof. Quaternary Legendre pairs II. Preprint, August 2024.

14. S. M. Krone and D. V. Sarwate. Quadriphase sequences for spread-spectrum multiple-access communication. *IEEE Trans. Inform. Theory*, 30(3):520–529, 1984.

15. H. Niederreiter and A. Winterhof. *Applied number theory*. Springer, Cham, 2015.

16. P. Ó Catháin and R. M. Stafford. On twin prime power Hadamard matrices. *Cryptogr. Commun.*, 2 (2):261–269, 2010.

17. R. E. Paley. On orthogonal matrices. *Journal of Mathematics and Physics*, 12(1-4):311–320, 1933.

18. J. Seberry. *Orthogonal Designs*. Springer, Cham, updated edition, 2017. Hadamard matrices, quadratic forms and algebras.

19. J. Seberry and M. Yamada. *Hadamard Matrices — Constructions using Number Theory and Algebra*. John Wiley & Sons, Inc., Hoboken, NJ, 2020.

20. J. J. Seidel. *Geometry and combinatorics*. Academic Press, Inc., Boston, MA, 1991. Selected works of J. J. Seidel, Edited and with a preface by D. G. Corneil and R. Mathon.

21. G. Szekeres. Tournaments and Hadamard matrices. *Enseign. Math. (2)*, 15:269–278, 1969.

22. G. Szekeres. A note on skew type orthogonal ± 1 matrices. In *Combinatorics (Eger, 1987)*, volume 52 of *Colloq. Math. Soc. János Bolyai*, pages 489–498. North-Holland, Amsterdam, 1988.

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

24. R. J. Turyn. Complex Hadamard matrices. In *Combinatorial Structures and their Applications (Proc. Calgary Internat. Conf., Calgary, Alta., 1969)*, pages 435–437. Gordon and Breach, New York-London-Paris, 1970.

25. R. J. Turyn. An infinite class of Williamson matrices. *J. Combinatorial Theory Ser. A*, 12:319–321, 1972.

26. A. L. Whiteman. An infinite family of skew Hadamard matrices. *Pacific J. Math.*, 38:817–822, 1971.

27. A. L. Whiteman. An infinite family of Hadamard matrices of Williamson type. *J. Combinatorial Theory Ser. A*, 14:334–340, 1973.

28. A. L. Whiteman. Hadamard matrices of order $4(2p+1)$. *Journal of Number Theory*, 8(1):1–11, 1976.