Quaternary Legendre pairs of even length

Jonathan Jedwab and Thomas Pender

Department of Mathematics, Simon Fraser University

Outline

- Hadamard matrix
- Quaternary sequence
- Periodic autocorrelation
- Legendre sequence pair
- Connection to Hadamard matrices
- Central question
- Classical construction of binary Legendre sequence pairs
- Modified construction for quaternary Legendre sequence pairs

Jonathan Jedwab
2 June 2025

Hadamard Matrix

- A Hadamard matrix is an order N matrix over $\{+1, -1\}$ satisfying (row j) . (row k) $= 0$ for all distinct j, k
  - ⋆ columns are necessarily pairwise orthogonal
  - ⋆ necessary condition when $N > 2$ is $N = 4n$

Jacques Hadamard 1865–1963

Hadamard Matrix

+	+	+	+
+	–	+	–
+	+	–	–
+	–	–	+

Hadamard matrix of order 4

Jonathan Jedwab
2 June 2025

Hadamard Matrix

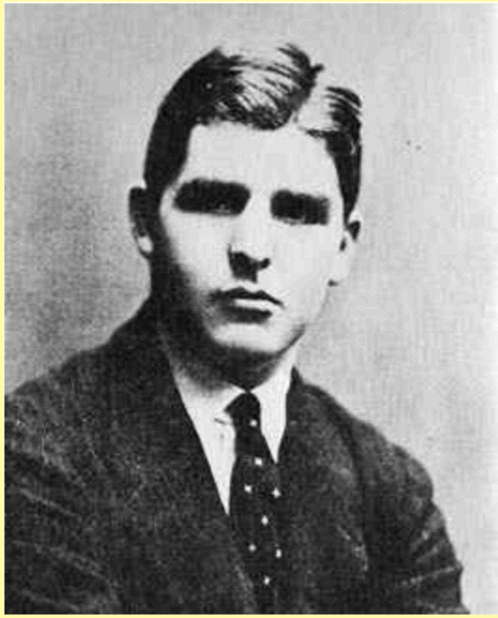
+	+	+	+	+	+	+	+	+	+	+	+
+	−	+	−	+	+	+	−	−	−	+	−
+	−	−	+	−	+	+	+	−	−	−	+
+	+	−	−	+	−	+	+	+	−	−	−
+	−	+	−	−	+	−	+	+	+	−	−
+	−	−	+	−	−	+	−	+	+	+	−
+	−	−	−	+	−	−	+	−	+	+	+
+	+	−	−	−	+	−	−	+	−	+	+
+	+	+	−	−	−	+	−	−	+	−	+
+	+	+	+	−	−	−	+	−	−	+	−
+	−	+	+	+	−	−	−	+	−	−	+
+	+	−	+	+	+	−	−	−	+	−	−

Hadamard matrix of order 12

Jonathan Jedwab
2 June 2025

Hadamard Matrix

- Conjecture (Paley 1933). There is a Hadamard matrix of every order $N = 4n$
    - ⋆ smallest open case is currently $N = 668$



Raymond Paley 1907–1933

Jonathan Jedwab
2 June 2025

Hadamard Matrix

- Theoretical importance: Hadamard matrices solve the maximum determinant problem for complex-valued matrices whose entries have magnitude at most 1

- Practical importance: applications include
  - ⋆ designs: analyse experimental data to determine which quantities depend on others
  - ⋆ coding of digital signals: make messages easy to recover
  - ⋆ cryptography: make messages difficult to recover

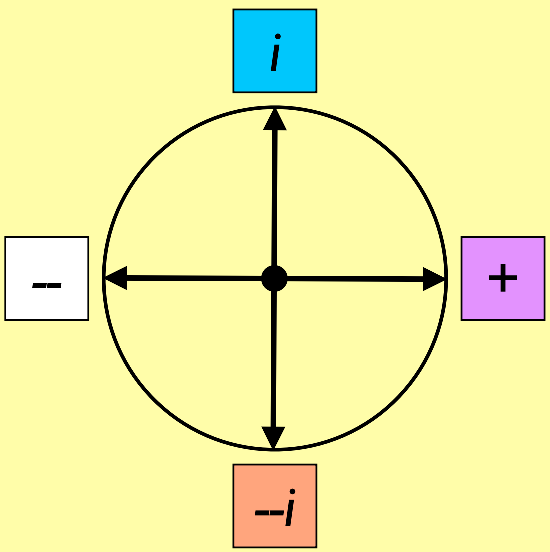
Quaternary Sequence

+	+	*i*	–*i*	–	*i*	–	–*i*	*i*	+

Quaternary sequence

+	–	+	+	+	–	–	+	–	+

Binary sequence



4th roots of unity

Jonathan Jedwab
2 June 2025

Quaternary Hadamard Matrix

- A quaternary Hadamard matrix is an order N quaternary matrix satisfying $(\text{row } j) \,.\, \overline{(\text{row } k)} = 0$ for all distinct j, k
  - ⋆ necessary condition when $N > 1$ is N even

+	+	+	+	+	+
+	–	i	$-i$	$-i$	i
+	i	–	i	$-i$	$-i$
+	$-i$	i	–	i	$-i$
+	$-i$	$-i$	i	–	i
+	i	$-i$	$-i$	i	–

Quaternary Hadamard matrix of order 6

Quaternary Hadamard Matrix

- Conjecture (Turyn 1970). There is a quaternary Hadamard matrix of every even order N
    - ⋆ smallest open case is currently $N = 94$

Richard Turyn 1930–2022

Jonathan Jedwab
2 June 2025

Quaternary Hadamard Matrix

- Conjecture (Turyn 1970). There is a quaternary Hadamard matrix of every even order N
  - ⋆ smallest open case is currently $N = 94$

- Theorem (Cohn 1965). If there is a quaternary Hadamard matrix of order $2n$ then there is a (binary) Hadamard matrix of order $4n$

Quaternary to Binary Hadamard

+	+	+	+	+	+
+	–	i	$-i$	$-i$	i
+	i	–	i	$-i$	$-i$
+	$-i$	i	–	i	$-i$
+	$-i$	$-i$	i	–	i
+	i	$-i$	$-i$	i	–

$$X + iY$$

$X+Y$	$X-Y$
$-X+Y$	$X+Y$

+	+	+	+	+	+	+	+	+	+	+	+
+	–	+	–	–	+	+	–	–	+	+	–
+	+	–	+	–	–	+	–	–	–	+	+
+	–	+	–	+	–	+	+	–	–	–	+
+	–	–	+	–	+	+	+	+	–	–	–
+	+	–	–	+	–	+	–	+	+	–	–
–	–	–	–	–	–	+	+	+	+	+	+
–	+	+	–	–	+	+	–	+	–	–	+
–	+	+	+	–	–	+	+	–	+	–	–
–	–	+	+	+	–	+	–	+	–	+	–
–	–	–	+	+	+	+	–	–	+	–	+
–	+	–	–	+	+	+	+	–	–	+	–

Hadamard matrix of order 12

Jonathan Jedwab
2 June 2025

Periodic Autocorrelation

a	+	i	i	–	+	$-i$	+	$-i$	i	+

R_a	10	0	$2-4i$	-2	$-2i$	0	$2i$	-2	$2+4i$	0

Periodic autocorrelation function of a is $R_a(u) = \sum_j a_j \overline{a_{j \oplus u}}$

Jonathan Jedwab
2 June 2025

Quaternary Legendre Sequence Pair

a	+	+	i	$-i$	–	i	–	$-i$	i	+
R_a	10	0	0	0	0	–8	0	0	0	0
b	+	+	–	–	+	–	+	–	–	+
R_b	10	–2	–2	–2	–2	6	–2	–2	–2	–2
$R_a + R_b$	20	–2	–2	–2	–2	–2	–2	–2	–2	–2

Legendre sequence pair: $R_a(u) + R_b(u) = -2$ for all $u \neq 0$

Jonathan Jedwab
2 June 2025

Binary Legendre Sequence Pair

a	+	+	+	–	–
R_a	5	1	–3	–3	1
b	+	–	+	–	+
R_b	5	–3	1	1	–3
$R_a + R_b$	10	–2	–2	–2	–2

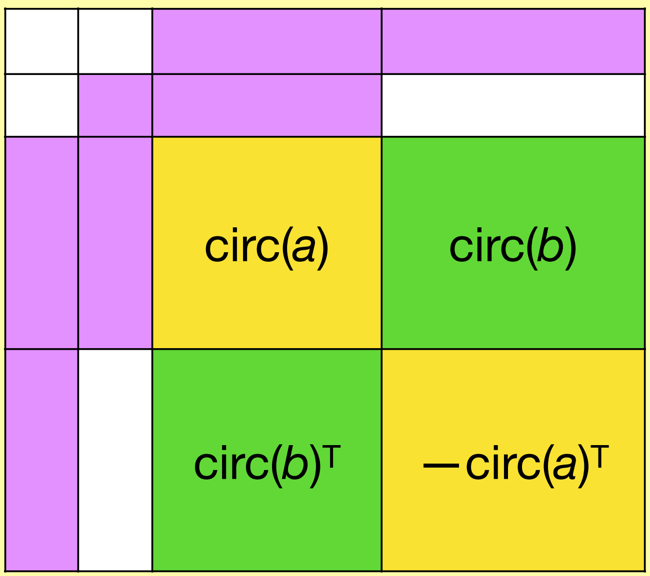
Legendre sequence pair: $R_a(u) + R_b(u) = -2$ for all $u \neq 0$

Jonathan Jedwab
2 June 2025

Connection to Hadamard Matrices

a	+	+	+	–	–
b	+	–	+	–	+

Binary Legendre sequence pair length *L*

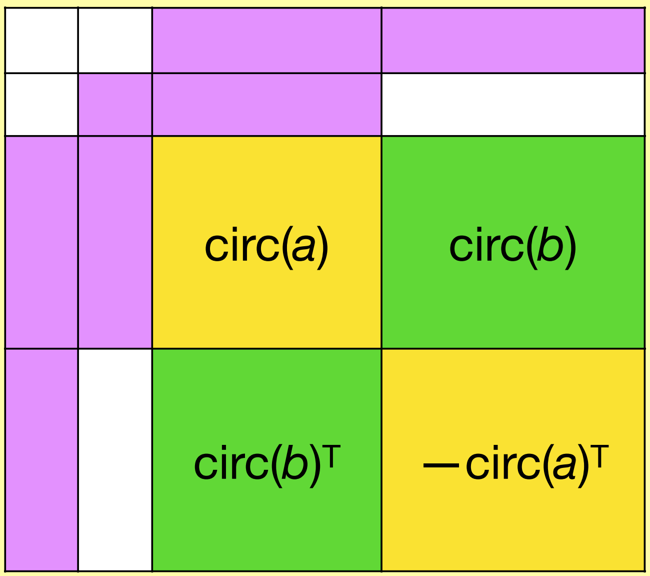


Order 2*L*+2 Hadamard matrix
(Fletcher Gysin Seberry 2001)

so *L* necessarily odd

Connection to Hadamard Matrices

a	+	+	+	–	–
b	+	–	+	–	+



–	–	+	+	+	+	+	+	+	+	+	+
–	+	+	+	+	+	+	–	–	–	–	–
+	+	+	+	+	–	–	+	–	+	–	+
+	+	–	+	+	+	–	+	+	–	+	–
+	+	–	–	+	+	+	–	+	+	–	+
+	+	+	–	–	+	+	+	–	+	+	–
+	+	+	+	–	–	+	–	+	–	+	+
+	–	+	+	–	+	–	–	+	+	–	–
+	–	–	+	+	–	+	–	–	+	+	–
+	–	+	–	+	+	–	–	–	–	+	+
+	–	–	+	–	+	+	+	–	–	–	+
+	–	+	–	+	–	+	+	+	–	–	–

Hadamard matrix of order 12

Jonathan Jedwab
2 June 2025

Legendre Sequence Pair

- Binary Legendre sequence pair must have odd length
  - ⋆ (Kotsireas et al. 2023). Smallest open length is 115

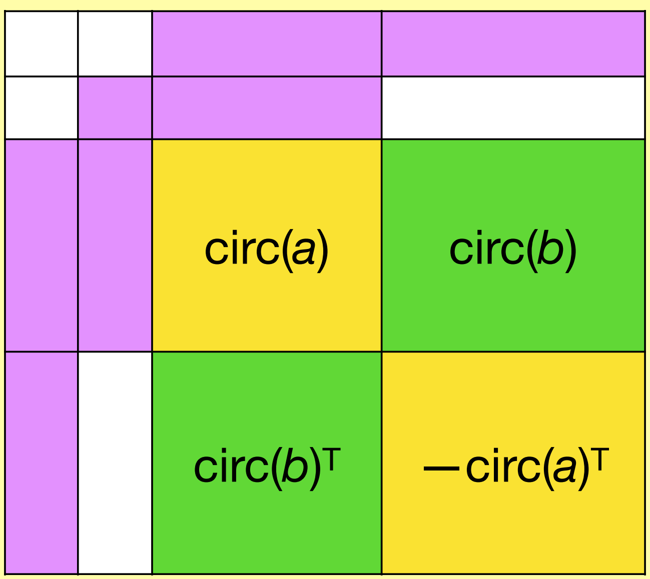
- Quaternary Legendre sequence pair can have even length

a	+	+	i	$-i$	–	i	–	$-i$	i	+
b	+	+	–	–	+	–	+	–	–	+

Connection to Hadamard Matrices

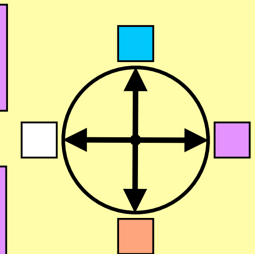
a	+	+	+	–	–
b	+	–	+	–	+

Odd length binary L pair

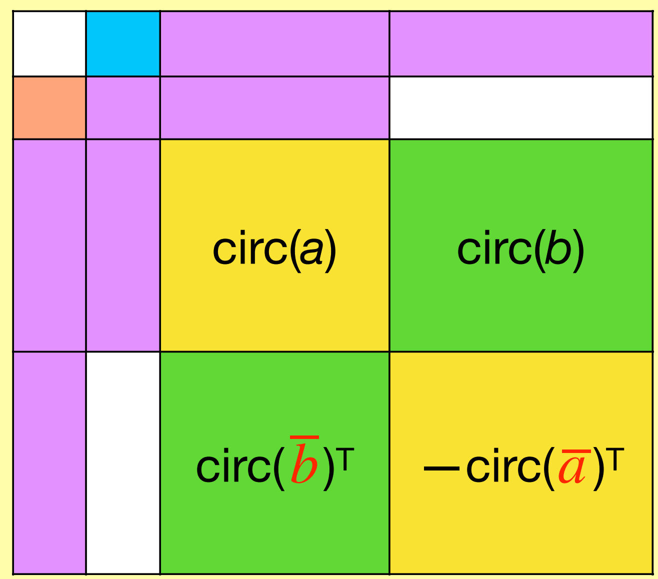


Fletcher Gysin Seberry 2001

a	i	+	–	–	–	+
b	–	+	–	–	+	+



Even length quaternary L pair

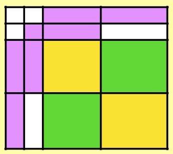


Kotsireas & Winterhof 2024

Jonathan Jedwab
2 June 2025

Connection to Hadamard Matrices

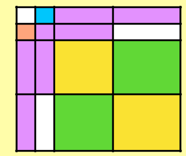
Binary Legendre pair of length $2n - 1$



Fletcher Gysin Seberry 2001

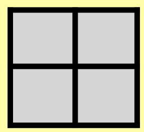
Quaternary Legendre pair of length $n - 1$

Kotsireas & Winterhof 2024



Hadamard matrix of order $4n$

Cohn 1965

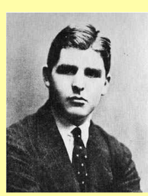


Quaternary Hadamard matrix of order $2n$

? Binary Legendre pair of every odd length

? Quaternary Legendre pair of every even length

Turyn 1970



Hadamard matrix of every order $4n$

Jonathan Jedwab
2 June 2025

Central Question

- Kotsireas & Winterhof 2024 asked:

Is there an infinite family of even length quaternary Legendre sequence pairs ?

Ilias Kotsireas

Arne Winterhof

Jonathan Jedwab
2 June 2025

Extended Quadratic Character χ

- Take q prime power and $\alpha \in \mathrm{GF}(q)$
- Extended quadratic character of $\mathrm{GF}(q)$ is the function

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

  - ⋆ χ takes values in $\{0, +1, -1\}$

Goethals-Seidel Construction 1967

Jean-Marie Goethals, M.S.E.E., 1961, and Ph.D., 1969, Louvain Catholic University, Belgium; MBLE Research Laboratory, Brussels, Belgium, 1963—. Mr. Goethals has been working on algebraic coding theory and applied combinatorial mathematics. He spent the Spring semester (1970) at the University of North Carolina, Chapel Hill, N. C., as a visiting lecturer. He is presently part-time lecturer at the Louvain

947

948 THE BELL SYSTEM TECHNICAL JOURNAL, APRIL 1972

Catholic University, where he delivers courses on information theory and coding, and discrete mathematics. Member, A.M.S., IEEE, Société Mathématique de Belgique.

Jean-Marie Goethals

Jaap Seidel 1919–2001

Goethals-Seidel Construction 1967

- Take q odd prime power and $g \in \mathrm{GF}(q)$ primitive
- Define length $\frac{q-1}{2}$ sequences $a = (a_k)$ and $b = (b_k)$ by

$$a_k = \begin{cases} 0 & \text{if } k = 0 \\ \chi(g^{2k} - 1) & \text{otherwise} \end{cases}$$

$$b_k = \chi(g^{2k+1} - 1)$$

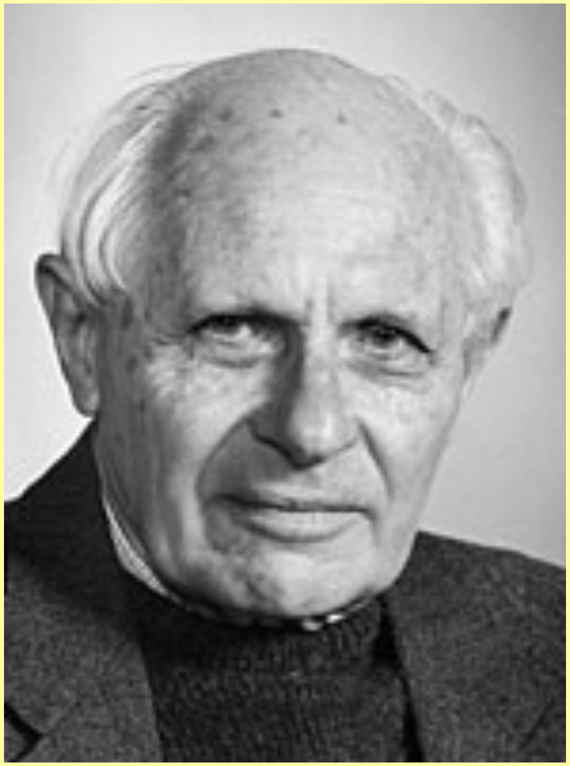
a, b binary except initial element of a is 0

- By standard character arguments, for each $u \neq 0$

$$R_a(u) + R_b(u) = -2$$

Jonathan Jedwab
2 June 2025

Szekeres Construction 1969



George Szekeres 1911–2005

Jonathan Jedwab
2 June 2025

Szekeres Construction 1969

- Take $q \equiv 3 \pmod 4$ prime power and $g \in \mathrm{GF}(q)$ primitive
- Define length $\frac{q-1}{2}$ sequences $a = (a_k)$ and $b = (b_k)$ by

$$a_k = \begin{cases} 1 & \text{if } k = 0 \\ \chi(g^{2k} - 1) & \text{otherwise} \end{cases}$$

$$b_k = \chi(g^{2k+1} - 1)$$

a, b binary

- By standard character arguments, for each $u \neq 0$

$$R_a(u) + R_b(u) = -2 + a_0 a_u + a_{(q-1)/2-u} a_0$$
$$= -2 + 1 \cdot a_u + (-a_u) \cdot 1 = -2$$

- So a, b are a binary Legendre sequence pair

Modified Construction

- Take $q \equiv 1 \pmod 4$ prime power and $g \in \mathrm{GF}(q)$ primitive
- Define length $\frac{q-1}{2}$ sequences $a = (a_k)$ and $b = (b_k)$ by

$$a_k = \begin{cases} i & \text{if } k = 0 \\ \chi(g^{2k} - 1) & \text{otherwise} \end{cases}$$

a, b quaternary

$$b_k = \chi(g^{2k+1} - 1)$$

- By standard character arguments, for each $u \neq 0$

$$R_a(u) + R_b(u) = -2 + a_0\, a_u + a_{(q-1)/2-u}\, \overline{a_0}$$
$$= -2 + i \cdot a_u + a_u \cdot (-i) = -2$$

- So a, b are a quaternary Legendre sequence pair

Jonathan Jedwab
2 June 2025

Constructions for Legendre pairs

- (Szekeres 1969). For $q \equiv 3 \pmod 4$ prime power

Binary Legendre pair
of odd length $(q-1)/2$

- (Jedwab & Pender 2025+). For $q \equiv 1 \pmod 4$ prime power

Quaternary Legendre pair
of even length $(q-1)/2$

- (Jedwab & Pender 2025+). For p odd prime and $2p-1$ prime power

Quaternary Legendre pair
of even length $2p$

Central Question

- Kotsireas & Winterhof 2024 asked:

> Is there an infinite family of even length quaternary Legendre sequence pairs ?

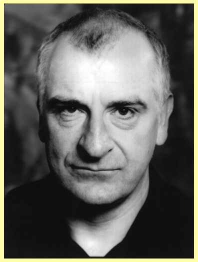
- Yes for lengths $\frac{q-1}{2}$ where $q \equiv 1 \pmod{4}$ is prime power
- Possibly for lengths $2p$ where p is odd prime and $2p-1$ is prime power

Future Research

- Are there further infinite families of even length quaternary Legendre pairs?

- Is there a quaternary Legendre sequence pair for every even length?

  - ⋆ (Kotsireas & Winterhof 2024, Kotsireas Koutschan Winterhof 2025). Examples found by computation show that smallest open length is now 42



Jonathan Jedwab
2 June 2025