A ternary Legendre pair of length 35

Qianghao Wu

November 25, 2026

Abstract

Kotsireas, Liu and Winterhof conjectured that ternary Legendre pairs exist for every length $\ell \equiv -1 \pmod 3$. They found ternary Legendre pairs for every such length $\ell \leq 32$ and named $\ell = 35$ and $\ell = 38$ as the smallest open cases. We give a ternary Legendre pair of length 35. This settles the case $\ell = 35$. Both sequences of the pair are invariant under the multiplier $j \mapsto 6j \pmod{35}$. We found the pair with an exact meet-in-the-middle search over the 42 042 000 sequences that have this symmetry and the required symbol composition. The search gives 2400 ordered pairs. Lean 4 with Mathlib checks the existence theorem, stated from the source's definition, with kernel evaluation and only the standard axioms. Two exact checkers in Python also accept the pair. The case $\ell = 38$ remains open: our searches in some structured families of length 38 found no pair. This work has not yet been reviewed by experts. The computations, the proofs and the text were produced by AI models (from Anthropic and OpenAI), working under the author's direction.

1 Introduction

Let $A = [a_0, \ldots, a_{\ell-1}] \in \mathbb{C}^\ell$ with $\ell \geq 2$, continued periodically with period ℓ. Its periodic autocorrelation function at lag s is

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

Two sequences A, B of length ℓ form a *Legendre pair* if

$$\mathrm{PAF}(A, s) + \mathrm{PAF}(B, s) = -2, \qquad s = 1, 2, \ldots, \lfloor \ell/2 \rfloor. \tag{1}$$

Since $\mathrm{PAF}(A, \ell - s) = \overline{\mathrm{PAF}(A, s)}$, condition (1) then holds for all $s = 1, \ldots, \ell - 1$. Let $\xi_3 = e^{2\pi\sqrt{-1}/3}$. The pair is *ternary* if $A, B \in \{1, \xi_3, \xi_3^2\}^\ell$. These definitions are those of Kotsireas, Liu and Winterhof [4], Section 1. We write a ternary sequence as an *exponent word* $r_0 r_1 \cdots r_{\ell-1}$ with $r_j \in \{0, 1, 2\}$, which means $a_j = \xi_3^{r_j}$.

History. Binary Legendre pairs ($A, B \in \{\pm 1\}^\ell$) give Hadamard matrices of order $2\ell+2$. Kotsireas, Liu and Winterhof [4, Section 1] summarize the known infinite families and state that $\ell = 115$ is the smallest undecided binary length. Composite binary lengths are searched with compression and with fixed row and column sums; this method gave the first Legendre pair of length 77 [9]. Recent work on binary pairs studies multipliers: Ramos, Hulak and de Queiroz [8] study pairs of length 333 in which both sequences are fixed by a common subgroup H of $(\mathbb{Z}/333\mathbb{Z})^\times$, and Bulutoglu, Baczkowski and Yauney [1] determine the group of operations that send Legendre pairs to equivalent pairs.

Kotsireas and Winterhof [5] introduced quaternary Legendre pairs ($A, B \in \{1, i, -1, -i\}^\ell$), which give quaternary Hadamard matrices of order $2\ell + 2$. Jedwab and Pender [2] gave two infinite constructions of even length. According to [4, Section 1], Kotsireas, Koutschan and Winterhof [5, 3] found the remaining quaternary pairs of even length $\ell \le 40$. Lebedev [6] found pairs of lengths 42, 46, 52, 58, 66, 72 and 80, and Verma [10] found a pair of length 64.

Ternary pairs. The source of the question is [4]. Its results for k-ary pairs ($A, B \in \{1, \xi_k, \ldots, \xi_k^{k-1}\}^\ell$) include:

- For prime k, a k-ary Legendre pair of length ℓ exists only if $\ell \equiv -1 \pmod k$ [4, Theorem 1]. For $k = 3$ these lengths are called *admissible*.
- For an odd prime p, after each component is multiplied by a suitable p-th root of unity, the components have a fixed symbol composition [4, Theorem 4]. For $k = 3$ and $\ell = 3h - 1$, each normalized component contains 1, ξ_3, ξ_3^2 exactly $h - 1$, h, h times [4, Section 4].
- Every p-ary Legendre pair of length ℓ gives a Butson Hadamard matrix $H(2p, 2\ell + 2)$ [4, Corollary 6].
- Generalized m-sequences give ternary pairs of every length $3^r - 1$ [4, Section 2.3].
- Searches with fixed-content necklaces, integral-PAF symmetries, half-frequency restrictions, compression and PSD tests give ternary pairs of lengths 5, 11, 14, 17, 20, 23, 29 and 32 [4, Section 4, Appendix A]. Together with the m-sequence lengths 2, 8 and 26, this covers every admissible $\ell \le 32$.
- For $\ell = 38$, the power spectral density $\mathrm{PSD}(C, s) = |\sum_j c_j \xi_{38}^{js}|^2$ at the half frequency leaves three cases, $(\mathrm{PSD}(A, 19), \mathrm{PSD}(B, 19)) \in \{(3, 75), (21, 57), (39, 39)\}$, up to the exchange of A and B [4, Section 4.4].

The source then states [4, Section 1]: "In this way we obtain ternary Legendre pairs for every admissible length $\ell \le 32$. The smallest open cases are then $\ell = 35$ and $\ell = 38$." Section 4.4 of [4] states:

> Conjecture 10. Ternary Legendre pairs exist for every admissible length $\ell \equiv -1 \pmod 3$.

and "The next open cases are 35 and 38."

Result. We give a ternary Legendre pair of length 35 (Theorem 1). So $\ell = 35$ is no longer an open case of Conjecture 10, and the smallest open case is $\ell = 38$. The result does not prove the conjecture.

Prior art. On November 24 and 25, 2026, we searched arXiv (API queries for "ternary Legendre", "k-ary Legendre" and "Legendre pairs", and the new listings of math.CO and cs.IT), Zenodo, GitHub code and repositories, OEIS, MathOverflow, OpenAlex and the web. We found no other ternary Legendre pair of length 35 or 38. The source appeared on arXiv on November 23, 2026. We cannot exclude unpublished pairs by its authors or by others.

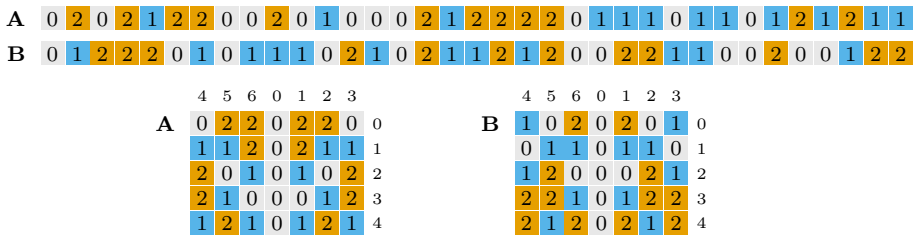


Figure 1: The pair of Theorem 1. Top: the exponent words, $j = 0, \ldots, 34$ from left to right. Bottom: entry j placed in row $j \bmod 5$ and in the column of $j \bmod 7$, with the columns in the order $4, 5, 6, 0, 1, 2, 3$. Since $6j \equiv j \pmod 5$ and $6j \equiv -j \pmod 7$, invariance under $j \mapsto 6j$ makes each row read the same in both directions. The figure is drawn from the certificate by `checks/draw_pair.py`.

2 The pair

Theorem 1. *The sequences with exponent words*

$$A = 02021220020100021222201110110121211,$$
$$B = 01222010111021021121200221100200122$$

form a ternary Legendre pair of length 35.

Proof. Let e be an exponent word and $a_j = \xi_3^{e_j}$. Since $\overline{\xi_3} = \xi_3^2$ and $\xi_3^3 = 1$, we have $a_j \overline{a_{j+s}} = \xi_3^{(e_j - e_{j+s}) \bmod 3}$. For a lag s and $r \in \{0, 1, 2\}$, let $M_r(s)$ be the number of $j \in \mathbb{Z}/35\mathbb{Z}$ with $(e_j - e_{j+s}) \bmod 3 = r$, counted for A and for B together. Then

$$\mathrm{PAF}(A, s) + \mathrm{PAF}(B, s) = M_0(s) + M_1(s)\,\xi_3 + M_2(s)\,\xi_3^2.$$

Direct counting gives $(M_0, M_1, M_2)(s) = (22, 24, 24)$ for every $s = 1, \ldots, 34$. Since $1 + \xi_3 + \xi_3^2 = 0$, the sum is $22 + 24(\xi_3 + \xi_3^2) = 22 - 24 = -2$. □

This count is the integer test of [4, Appendix A]: with $\ell = 3h - 1$, a ternary pair satisfies $(M_0, M_1, M_2)(s) = (2h - 2, 2h, 2h)$, and here $h = 12$. The proof needs the counts only for $s = 1, \ldots, 17$; the counts hold for all 34 nonzero lags.

Further facts about the pair, all checked by `checks/check.py`:

- Each word has 11 zeros, 12 ones and 12 twos, that is, composition $(11, 12, 12)$. This agrees with the normalized composition $(h-1, h, h)$ of [4]. Each component has sum $11+12\xi_3+12\xi_3^2 = -1$.
- Both words are invariant under $j \mapsto 6j \pmod{35}$, that is, $e_{6j} = e_j$ for all j. The group $\{1, 6\}$ has order 2 and does not contain -1. Neither word is invariant under $j \mapsto -j$.
- In both words, the entries at the multiples of 7 (the points fixed by $j \mapsto 6j$) are all 0 (Figure 1, middle column of each grid).

Remark 2. By [4, Corollary 6], the pair gives a Butson Hadamard matrix $H(6, 72)$. We did not construct this matrix. We make no claim that an $H(6, 72)$ is new.

H	$\lvert H\rvert$	H-invariant words with composition $(11,12,12)$	ordered pairs
$\langle 34\rangle = \{\pm 1\}$	2	5 717 712	0
$\langle 6\rangle$	2	42 042 000	2400
$\langle 29\rangle$	2	130 162 032	0
$\langle 11\rangle$	3	87 150	0
$\langle 8\rangle$	4	14 840	0
$\langle 13\rangle$	4	1 400	0
$\langle 3\rangle$	12	2	0

Table 1: Searches at $\ell = 35$: the number of ordered pairs (A, B) in which both A and B are H-invariant and have composition $(11, 12, 12)$. The rerun command is `python3 -I checks/search.py`.

3 How the pair was found

Multiplier orbits. Let H be a subgroup of the unit group $\mathbb{Z}_{35}^{\times}$. A sequence A is *H-invariant* if $a_{tj} = a_j$ for all $t \in H$ and all j. An H-invariant sequence is constant on each orbit of H on $\mathbb{Z}/35\mathbb{Z}$. If A is H-invariant and $t \in H$, the substitution $j \mapsto tj$ gives $\mathrm{PAF}(A, ts) = \mathrm{PAF}(A, s)$. The same idea, for binary pairs of length 333, is the subject of [8].

For $H = \langle 6\rangle = \{1, 6\}$, the orbits are the 5 fixed points $0, 7, 14, 21, 28$ and 15 orbits $\{j, 6j\}$ of size 2. So an H-invariant word is given by 20 symbols. Exactly 42 042 000 of these words have composition $(11, 12, 12)$.

Normalization. Multiplication of A by a constant ξ_3^c does not change $\mathrm{PAF}(A, s)$, and it keeps H-invariance. By [4, Theorem 4], every ternary pair of length 35 becomes, after such multiplications of A and of B, a pair in which both words have composition $(11, 12, 12)$. So a search over the words with this composition finds an H-invariant pair if one exists.

Meet in the middle. For a fixed H, the program `checks/search/mitm.c` does these steps:

1. It lists every H-invariant word with composition $(11, 12, 12)$.
2. For each word X and each lag $s = 1, \ldots, 17$, it computes $\mathrm{PAF}(X, s) = u_s + v_s\xi_3$ exactly, with $u_s = N_0(s) - N_2(s)$ and $v_s = N_1(s) - N_2(s)$, where $N_r(s)$ counts the j with $(x_j - x_{j+s}) \bmod 3 = r$. It stores a 64-bit hash of the vector $(u_s, v_s)_{s=1}^{17}$ with the word, and sorts the records by hash.
3. For each word A, it looks up the hash of the target vector $(-2 - u_s, -v_s)_{s=1}^{17}$. For each word B with that hash, it checks $\mathrm{PAF}(A, s) + \mathrm{PAF}(B, s) = -2$ for $s = 1, \ldots, 17$ exactly, in integers.

A true pair always has equal hashes, so the hash causes no missed pairs. Each reported pair passed the exact check of step 3. The program counts ordered pairs (A, B).

Results. Table 1 gives the runs at $\ell = 35$. Each run used one thread on an Apple M1 Pro. The run for $\langle 6\rangle$ took about 85 s. The pair of Theorem 1 is one of the 2400 pairs that it prints. The 2400 ordered pairs include pairs that are equivalent under shifts, multipliers, conjugation and the exchange of A and B. We did not count the equivalence classes.

The group $\mathbb{Z}_{35}^{\times}$ has 15 subgroups other than $\{1\}$. A direct enumeration (`checks/check.py`) shows that each of them contains one of the four subgroups of prime order, $\langle 34\rangle$, $\langle 6\rangle$, $\langle 29\rangle$ and $\langle 11\rangle$.

If $H \subseteq H'$, every H'-invariant word is H-invariant. With the zero rows of Table 1 for $\langle 34\rangle$, $\langle 29\rangle$ and $\langle 11\rangle$, this gives:

Proposition 3 (computer-assisted)**.** *Let $H \neq \{1\}$ be a subgroup of $\mathbb{Z}_{35}^{\times}$. A ternary Legendre pair of length 35 in which both components are H-invariant exists if and only if $H = \langle 6\rangle$.*

The "only if" part rests on the search program, which is not formally verified. The "if" part is Theorem 1. The element 6 acts as $+1$ on $\mathbb{Z}/5\mathbb{Z}$ and as -1 on $\mathbb{Z}/7\mathbb{Z}$. We do not have an explanation of why this group gives pairs and the other groups do not.

4 Verification

Lean. The file `lean/TernaryLP35.lean` imports only Mathlib. It states the definition of [4] over $\mathbb{C}$ and proves the existence theorem:

```
def ξ3 : ℂ := Complex.exp (2 * Real.pi * Complex.I / 3)

def PAF {ℓ : ℕ} [NeZero ℓ] (a : Fin ℓ → ℂ) (s : Fin ℓ) : ℂ :=
  ∑ j : Fin ℓ, a j * (starRingEnd ℂ) (a (j + s))

def IsTernaryLegendrePair (ℓ : ℕ) [NeZero ℓ] (A B : Fin ℓ → ℂ) : Prop :=
  (∀ j, A j ∈ ({1, ξ3, ξ3 ^ 2} : Set ℂ)) ∧
  (∀ j, B j ∈ ({1, ξ3, ξ3 ^ 2} : Set ℂ)) ∧
  ∀ s : Fin ℓ, 1 ≤ s.val → s.val ≤ ℓ / 2 → PAF A s + PAF B s = -2

theorem exists_ternary_legendre_pair_35 :
    ∃ A B : Fin 35 → ℂ, IsTernaryLegendrePair 35 A B
```

The definitions match the source line by line:

- `ξ3` is $e^{2\pi\sqrt{-1}/3}$. The proof gets from Mathlib that it is a primitive cube root of unity.
- Addition in `Fin` ℓ is addition modulo ℓ, so `a (j + s)` is the periodic continuation $a_{(j+s) \bmod \ell}$. The sum runs over all ℓ indices. `starRingEnd` $\mathbb{C}$ is complex conjugation, and it is on the second factor, as in the source.
- The lags are $1 \le s \le \ell/2$, where ℓ `/ 2` is division in $\mathbb{N}$, that is, $\lfloor \ell/2 \rfloor$. For $\ell = 35$ these are $s = 1, \ldots, 17$.
- Every entry of A and of B is in $\{1, \xi_3, \xi_3^2\}$: this is the ternary case $k = 3$.
- `[NeZero` ℓ`]` only makes the arithmetic of `Fin` ℓ available. It adds no condition for $\ell = 35$.

The proof follows the proof of Theorem 1. The witnesses are $a_j = \xi_3^{e_j}$ for the two exponent words. A lemma rewrites PAF as $M_0 + M_1\xi_3 + M_2\xi_3^2$. The lemma `counts_ok` states that the combined counts are $(22, 24, 24)$ at every nonzero lag, and the kernel proves it with `decide`. A final `linear_combination` with $1 + \xi_3 + \xi_3^2 = 0$ closes the goal. The proof does not use `native_decide`. The command `#print axioms exists_ternary_legendre_pair_35` prints

```
'exists_ternary_legendre_pair_35' depends on axioms: [propext, Classical.choice, Quot.sound]
```

These are the standard axioms of Lean and Mathlib; `Lean.ofReduceBool` does not occur. The file contains no `sorry`, `admit`, `axiom`, `implemented_by` or `unsafe`. With Lean v4.36.0 and Mathlib v4.36.0, the check takes about 1 to 3 minutes on an M1 Pro; three measured runs took 151 s, 60 s and 56 s. In two mutation tests, one entry of the certificate in a copy of the file was changed; each time, `decide` reported that `counts_ok` is false.

Python. Two exact checkers were written separately. `checks/check_pair.py` computes the integer counts $M_r(s)$ for $s = 1, \ldots, 34$. `checks/check_pair_zw.py` multiplies in $\mathbb{Z}[\omega] = \mathbb{Z}[x]/(x^2+x+1)$ and also reports a floating-point cross-check (maximum error $7.3 \cdot 10^{-15}$). Both accept the pair. Both accept the eight pairs printed in [4] (lengths 5, 11, 14, 17, 20, 23, 29, 32). Both reject each of the 140 pairs that differ from ours in one entry. `checks/check.py` runs all of these checks in less than 1 s. It also checks that the words in the Lean file equal the certificate `data/lp35.txt`.

Independent review. A second AI session, separate from the session that found the pair, reran the checks from a clean copy. It wrote its own checker (now `checks/check_pair_zw.py`) before it read the first checker. It compared the Lean statement with the source, reran the Lean proof and the searches of Table 1, and added the $\langle 29 \rangle$ row.

5 The case $\ell = 38$

We applied the same exact meet-in-the-middle method at $\ell = 38$, where the normalized composition is $(12, 13, 13)$ and the combined counts must be $(24, 26, 26)$. A family is the set of words e with composition $(12, 13, 13)$ that satisfy $e_{hx+c} \equiv \sigma e_x + k \pmod 3$ for all x, for one fixed map (h, c, σ, k) with $\sigma = \pm 1$. The sign $\sigma = -1$ means complex conjugation. For example, $(37, 0, 1, 0)$ is the family of symmetric words ($a_{-x} = a_x$), and $(1, 19, -1, 0)$ is the family with $a_{x+19} = \overline{a_x}$. The searched combinations were:

- 10 families with themselves: $(27, 0, 1, 0)$ and $(31, 0, 1, 0)$ (180 words each); $(7, 1, -1, 0)$, $(11, 1, -1, 0)$, $(27, 1, -1, 0)$, $(31, 1, -1, 0)$ (480 each); $(7, 0, 1, 0)$, $(11, 0, 1, 0)$ (69 300 each); $(37, 0, 1, 0)$ (34 306 272); $(37, 0, -1, 0)$ (70 189 056);
- 12 combinations of two different families, with family sizes up to 222 265 344 (for $(37, 1, -1, 0)$ and $(1, 19, -1, 0)$);
- $(1, 19, -1, 0)$ with itself (222 265 344 words, run in 5 parts).

In total these are 27 runs. All of them found no pair. The full list of runs, with their set sizes, is in `NUMBERS.md`. The independent review reran 19 of these 27 runs with identical output: the 9 self-runs of the families other than $(37, 0, 1, 0)$, and 10 of the 12 combinations of two different families. For this paper we reran $(37, 0, 1, 0)$ with itself and again found 34 306 272 words and 0 pairs. The other 7 runs ($(37, 0, 1, 0)$ with $(37, 1, -1, 0)$, $(37, 0, 1, 0)$ with $(1, 19, -1, 0)$, and the 5 parts of $(1, 19, -1, 0)$ with itself) were not rerun. Each of them holds a set of 222 265 344 records, about 3.6 GB, which is near the 4 GB memory limit of one job on our machine. These are negative results inside the listed families only. They say nothing about whether a ternary Legendre pair of length 38 exists. A natural next step is the compression method of [4], run separately in each of the three half-frequency cases; we did not try it.

6 Limits

- The result settles $\ell = 35$ only. It does not prove Conjecture 10, and $\ell = 38$ remains open.
- Theorem 1 is checked in Lean from the definitions. Proposition 3, the count 2400 and all results at $\ell = 38$ come from a C program that is not formally verified. We make no claim about the number of pairs, or of equivalence classes, of length 35.

- The Lean proof uses kernel `decide` on a statement about 34 lags and two words of length 35. Its run time varies from about 1 to about 3 minutes.

Code and data

The certificate, the Lean file, the checkers, the search program and the figure script are in the result folder. `bash checks/ci.sh` reruns all checks and all searches of Table 1, and fails if a number differs from this paper.

References

[1] D. Bulutoglu, D. Baczkowski, J. Yauney, Determining the group that sends each Legendre pair to an equivalent Legendre pair, arXiv:2604.22423 (2026). https://arxiv.org/abs/2604.22423

[2] J. Jedwab, T. Pender, Two constructions of quaternary Legendre pairs of even length, Comb. Theory 5 (2025), no. 2, Paper No. 15. arXiv:2408.08472. https://arxiv.org/abs/2408.08472

[3] I. S. Kotsireas, C. Koutschan, A. Winterhof, Quaternary Legendre pairs II, Discrete Math. 348 (2025), no. 9, Paper No. 114501. arXiv:2408.16318. https://arxiv.org/abs/2408.16318

[4] I. S. Kotsireas, H. Liu, A. Winterhof, k-ary Legendre pairs, arXiv:2611.31067v1 (November 23, 2026). https://arxiv.org/abs/2611.31067

[5] I. S. Kotsireas, A. Winterhof, Quaternary Legendre pairs, in: New Advances in Designs, Codes and Cryptography, Fields Inst. Commun. 86, Springer, 2024, pp. 289–304. arXiv:2212.10953. https://arxiv.org/abs/2212.10953

[6] N. Lebedev, Quaternary Legendre pairs of lengths 42, 46, 52, 58, 66, 72, and 80, arXiv:2609.04589 (2026). https://arxiv.org/abs/2609.04589

[7] The mathlib Community, Mathlib, tag v4.36.0. https://github.com/leanprover-community/mathlib4

[8] A. F. Ramos, D. B. Hulak, R. J. G. B. de Queiroz, Multiplier obstructions for Legendre pairs of length 333, arXiv:2607.20765 (2026). https://arxiv.org/abs/2607.20765

[9] J. Turner, I. Kotsireas, D. Bulutoglu, A. Geyer, Legendre pair of length 77 using complementary binary matrices with fixed marginals, arXiv:2101.10918 (2021). https://arxiv.org/abs/2101.10918

[10] H. Verma, A quaternary Legendre pair of length 64, arXiv:2609.25573 (2026). https://arxiv.org/abs/2609.25573