Periodic Golay pairs of length 106

Peiwei Wu Qian Peng*

Abstract

We construct four pairwise inequivalent binary periodic Golay pairs of length 106, the smallest undecided length in the work of Lumsden, Kotsireas and Bright. An affine permutation and alternating signs determine the second sequence of each pair from the first. The multiplier squares to -1 modulo 106, reducing the periodic Golay check to 26 autocorrelation comparisons per pair. The four distinct peak absolute autocorrelations certify inequivalence. Each pair gives cyclic supplementary difference sets with parameters $(106; 51, 46; 44)$. Lean 4 verifies the correlation identities and the inequivalence of the four pairs.

hexagon:2611.01342v1

1 The length-106 existence problem

For a sequence $A\colon \mathbb{Z}/n\mathbb{Z} \to \{1, -1\}$, its periodic autocorrelation is

$$\mathrm{P}_A(d) = \sum_{j \in \mathbb{Z}/n\mathbb{Z}} A(j)A(j+d).$$

A pair (A, B) is a *periodic Golay pair* if $\mathrm{P}_A(d) + \mathrm{P}_B(d) = 0$ for every nonzero shift d. Đoković and Kotsireas [1] listed existence at length 106 as open. After constructing pairs of length 90, Lumsden, Kotsireas and Bright [2] identified 106 as the smallest remaining case. The existence question has also been formulated in Lean [3].

Theorem 1. *There are at least four pairwise inequivalent binary periodic Golay pairs of length 106 under the equivalence operations of [2, §2.1].*

Proof. Set $n = 106$. A mask $m = \sum_{j=0}^{105} m_j 2^j$ specifies $A(j) = 1 - 2m_j$, with the least significant bit corresponding to $j = 0$. For each choice of m, h, ε below define B by

$$B(23j + h) = \varepsilon(-1)^j A(j). \tag{1}$$

The indices are taken modulo 106. The multiplier 23 is a unit and 106 is even, so the affine permutation and the parity factor in (1) are well defined.

Pair	Mask m	h	ε
1	13744997680842415080923329506062	87	1
2	45131587558751544818782230567518	33	1
3	33231421976668766179629462462853	3	-1
4	55103358605353619565033847182206	15	1

Changing the summation index by $j \mapsto 23j + h$ in $\mathrm{P}_B(23d)$ gives $\mathrm{P}_B(23d) = (-1)^d \mathrm{P}_A(d)$. Thus the periodic Golay condition at shift $23d$ becomes

$$\mathrm{P}_A(23d) = -(-1)^d \mathrm{P}_A(d) \qquad (d \neq 0). \tag{2}$$

*Corresponding author.

At $d = 53$ the identity holds because $23d = d$ modulo 106 and d is odd. For every other nonzero shift the orbit $\{d, 23d, -d, -23d\}$ has size four. Indeed, $23^2 \equiv -1 \pmod{106}$ and $2d \not\equiv 0 \pmod{106}$. The parity of d is constant on the orbit, and $\mathrm{P}_A(-d) = \mathrm{P}_A(d)$. Hence it suffices to check (2) at one representative of each of the 26 orbits.

Table 1 gives $\mathrm{P}_A(d)$ for the least positive representative of each orbit. Both $\mathrm{P}_A(d)$ and $\mathrm{P}_A(23d)$ can be computed directly from the bits using

$$\mathrm{P}_A(d) = 106 - 2\sum_{j=0}^{105}(m_j \text{ xor } m_{(j+d) \bmod 106}).$$

For each even d in the table, evaluation at $23d$ gives the negative of the displayed value. For each odd d it gives the same value. For example, the second mask gives $\mathrm{P}_{A_2}(21) = \mathrm{P}_{A_2}(59) = -18$ and $23 \cdot 21 \equiv 59 \pmod{106}$. This verifies (2) for each of the four pairs.

even d	2	4	6	8	10	12	16	20	22	26	30	34	44
$\mathrm{P}_{A_1}(d)$	2	2	2	−2	−2	−10	−2	−2	2	−6	−10	−2	6
$\mathrm{P}_{A_2}(d)$	6	−10	−14	−2	−6	6	−6	6	6	10	−2	6	−10
$\mathrm{P}_{A_3}(d)$	2	2	−2	−2	2	2	6	−2	6	−6	6	−6	−10
$\mathrm{P}_{A_4}(d)$	−6	2	−6	−6	−14	10	2	−2	−6	−10	2	−6	10
odd d	1	3	5	7	11	13	15	17	21	25	29	35	39
$\mathrm{P}_{A_1}(d)$	10	−2	2	−2	−2	−10	6	−14	2	−6	2	−6	−2
$\mathrm{P}_{A_2}(d)$	2	−2	2	−2	−6	6	6	−6	−18	2	−2	−2	−2
$\mathrm{P}_{A_3}(d)$	2	−2	6	−6	−6	10	6	2	10	14	−2	−2	−2
$\mathrm{P}_{A_4}(d)$	−2	6	10	−6	−6	−6	−6	−6	2	2	−2	−2	2

Table 1: Single-row autocorrelations on the nontrivial four-element orbits.

To distinguish the pairs, take the largest absolute autocorrelation of either sequence over all nonzero shifts. A shift, reversal, or global sign change of a sequence preserves this maximum. Common decimation by a unit permutes the shifts, simultaneous alternating negation changes only the signs of the correlations, and exchanging the sequences leaves the maximum unchanged. Thus the maximum is invariant under the equivalence operations of [2, §2.1]. For a periodic Golay pair, the absolute autocorrelations of A and B agree at each nonzero shift. At shift 53 the four first-sequence correlations are $-2, -2, -30, -34$. These values, together with Table 1, give the four distinct maxima $14, 18, 30, 34$. □

2 Difference families

Pairs 1, 2 and 4 have ordinary row sums $(-4, 14)$ and alternating row sums $(14, 4)$. For pair 3 these sums are $(14, -4)$ and $(4, 14)$, respectively. Exchange the two rows of pair 3 to put their ordinary sums in the same order. Let D be the positive positions of the row of sum -4 and E the negative positions of the row of sum 14. Their sizes are 51 and 46. With $I_D(d) = |D \cap (D + d)|$, the correlation identity reads

$$0 = 212 - 4(51 + 46) + 4\big(I_D(d) + I_E(d)\big) \qquad (d \neq 0).$$

Thus each nonzero residue occurs 44 times among the ordered differences internal to D and E.

3 Search and verification

Write an index as $(e, j) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/53\mathbb{Z}$ using the Chinese remainder theorem. For each sequence, take the half-sum and half-difference of its two parity layers. This gives two ternary sequences with disjoint supports that cover $\mathbb{Z}/53\mathbb{Z}$. Denote these sequences by (X, U) for A and (Y, V) for B. Adding and subtracting the correlation equations on the two parity layers gives

$$\mathrm{P}_X + \mathrm{P}_Y = 53\delta_0, \qquad \mathrm{P}_U + \mathrm{P}_V = 53\delta_0.$$

We searched for $S = \operatorname{supp} X$ and $T = \operatorname{supp} V$ with $T = 23S + t$ in $\mathbb{Z}/53\mathbb{Z}$. Since $\operatorname{supp} Y$ is the complement of T, reduction modulo two requires $I_S(d) + I_T(d)$ to be odd at every nonzero d. For each candidate support, we constrained the signs modulo four and then modulo eight before testing the exact integer correlations. The four pairs have support sizes $|S| = |T|$ of $26, 26, 19, 18$. The archived search code can recover the signs from the corresponding support masks.

Verification and data. The Lean formalization represents a sequence as an integer-valued function on $\mathrm{Fin}\,106$. Checks by kernel reduction cover the correlation sum at every shift for each pair, the affine identities (1), and the peak absolute autocorrelations. The inequivalence proof transports an autocorrelation bound under signed affine reindexing. The ancillary files contain all four signed pairs. The command `python3 anc/verify.py` checks their periodic autocorrelations, difference counts, and equivalence invariants with exact arithmetic.

The versioned GitHub source includes the Lean 4.19.0 project and the search code. The first Zenodo release contains pairs 1 and 2. The second release adds pairs 3 and 4 and the proof of all six inequivalences.

Author contributions and use of AI. Peiwei Wu and Qian Peng directed the study and take responsibility for the manuscript. OpenAI Codex assisted with the literature search, the design and execution of the search for the four pairs, the inequivalence argument, the Lean formalization, and the drafting and revision of the paper.

References

[1] D. Ž. Đoković and I. S. Kotsireas, Periodic Golay pairs of length 72, in *Algebraic Design Theory and Hadamard Matrices*, Springer, 2015, 83–92. doi:10.1007/978-3-319-17729-8_7.

[2] T. Lumsden, I. Kotsireas and C. Bright, New results on periodic Golay pairs, *Math. Comp.* **95** (2026), 1517–1539. doi:10.1090/mcom/4096.

[3] `derekste`, The length-106 periodic Golay question, pull request 7205 in *Formal Conjectures*, 12 October 2026 (see also issue 7189). `https://github.com/google-deepmind/formal-conjectures/pull/7205`.