An affine criterion for a classical four-point family

Alexandre Couret

7 November 2026 — working draft for review

Abstract

For a classical family of four-point subsets of a cyclic group, we give an explicit greatest-common-divisor criterion for equivalence under translations and arbitrary unit multipliers. The supports have identical labelled ordered sum profiles, including diagonal pairs. The argument handles nonunit parameters by lifting units between quotient rings. No bibliographic novelty is claimed.

hexagon:2611.00199v1

Conventions and scope. For $S \subseteq C_N = \mathbb{Z}/N\mathbb{Z}$, put

$$R_S(z) = \#\{(s,t) \in S \times S : s + t = z\}.$$

The pairs are ordered, diagonal pairs are included, and equality of profiles is pointwise, without relabelling. Two supports are affinely equivalent when $T = uS + v$ for some $u \in (\mathbb{Z}/N\mathbb{Z})^\times$ and $v \in C_N$.

Theorem 1. *Let $q > 0$ and $x \in C_{4q} \setminus \{0, q, 2q, 3q\}$. Define*

$$P = \{0, q, x, x + 2q\}, \qquad Q = \{0, q, x + q, x + 3q\}.$$

Let $X \in \{0, \dots, 4q - 1\}$ represent x, and set $d = \gcd(q, X)$, $a = X/d$, $b = q/d$. Then both supports have four points, $R_P = R_Q$, and

$$P \text{ and } Q \text{ are not affinely equivalent} \iff b \equiv 2 \pmod 4.$$

Equality of the profiles. In $\mathbb{Z}[t]/(t^{4q}-1)$, the masks of P and Q are $p = C+E$ and $r = C+t^qE$, where $C = 1 + t^q$ and $E = t^X(1 + t^{2q})$. Direct expansion gives

$$p^2 - r^2 = (1 - t^{4q})\big[2t^X + t^{2X}(1 + t^{2q})\big] = 0.$$

The coefficient of t^z in a squared mask counts $R_S(z)$, proving the claim.

Reduction to four systems. Every unit modulo $4q$ fixes the unique nonzero involution $2q$. Thus an affine map preserves the relation of being antipodal. In each support the two points whose antipodes are absent are exactly $0, q$. An affine map from P to Q must carry this pair to itself. Either $v = 0$ and $uq = q$, or $v = q$ and $uq = -q$. Its image of x gives the four systems on the next page. Conversely, every solution maps the entire support as required, because the antipodal partner follows its image.

Case	Equations in C_{4q}, u a unit	Solvable exactly when
I	$uq = q,\ ux = x + q$	$4 \mid b$
II	$uq = q,\ ux = x + 3q$	$4 \mid b$
III	$uq = -q,\ ux = x$	a even
IV	$uq = -q,\ ux = x + 2q$	a, b both odd

Cancellation and lifting. Write $q = db$ and $X = da$. Cancelling d reduces the modulus from $4q$ to $4b$; $\gcd(a, b) = 1$. Reduction maps units modulo $4q$ onto units modulo $4b$. To see surjectivity, start with a representative coprime to $4b$ and impose, by the Chinese remainder theorem, the congruence 1 modulo every prime dividing $4q$ but not $4b$. The resulting integer remains in the prescribed class modulo $4b$ and is coprime to $4q$. This proves that cancellation preserves solvability in units.

Necessity. For the reduced unit w, the equation $wb = \pm b$ is equivalent to $w \equiv \pm 1 \pmod 4$. Reducing the other equation modulo four gives, respectively,

$$b \equiv 0, \quad 3b \equiv 0, \quad 2a \equiv 0, \quad 2a \equiv 2b \pmod 4.$$

These are the conditions displayed in the table. In IV, coprimality rules out a, b both even. In III, a even forces b odd.

Sufficiency. For I or II, let $k = 1$ or 3 and assume $4 \mid b$. Then a is odd. Set $w = 1 + kba$ modulo $4b$. This integer is odd and coprime to b, hence a unit. We have $wb = b$ and $wa = a + kb$, since $a^2 \equiv 1 \pmod 4$.

For III or IV, b is odd. The integer $w = 1 + 2b$ is a unit modulo $4b$, and $wb = -b$. If a is even, $wa = a$; if a is odd, $wa = a + 2b$. Lift each witness to a unit modulo $4q$. This establishes the table.

Since a, b are coprime, the union of the four solvability conditions is precisely "b odd or $4 \mid b$". Its complement is $b \equiv 2 \pmod 4$, completing the proof. □

Examples and a lifting caution. For $(q, X) = (2, 1)$ the supports in C_8 are $\{0, 1, 2, 5\}$ and $\{0, 2, 3, 7\}$; they are non-affine. For $(q, X) = (4, 1)$, $b = 4$ and $Q = 5P$ in C_{16}. For $(4, 2)$ the parameter is a nonunit and the pair is non-affine. For $(20, 5)$, the reduced witness 5 modulo 16 is not a unit modulo 80; 21 modulo 80 is a valid lift.

A valuation reformulation. For $X > 0$, $v_2(b) = \max(v_2(q) - v_2(X), 0)$. Thus the obstruction is equivalently $v_2(q) = v_2(X) + 1$. This is an arithmetic consequence, not a claim about the exact API of the Lean development.

Classical background and the novelty question. The four-point homometric families are classical; see Rosenblatt [1], the restatement by Jedrzejewski and Johnson [2], and the discussion in Erickson and Jones [3]. In the notation of the restatement, for $1 \le a < q$,

$$A_0 = \{0, a, a+q, 2q\}, \quad B_0 = \{0, a, q, a+2q\},$$

our $P = B_0$ and $Q = (a+q) - A_0$. The family and its familiar small examples are not claimed as new. The present note isolates the precise criterion for equivalence under all unit affine maps, rather than only translations and reflections. Whether this criterion is already stated or follows immediately from an existing reference remains a question for bibliographic review. Rosenblatt's original proof has not been checked in full for this draft.

Classical homometry uses the ordered difference profile $D_S(z) = \#\{(s,t) : s - t = z\}$. Equality of R implies equality of D: Fourier transformation gives $\widehat{R_S} = \widehat{\mathbf{1}_S}^{\,2}$ and $\widehat{D_S} = |\widehat{\mathbf{1}_S}|^2$. These observables and their equivalence groups must nevertheless be distinguished.

AI assistance, formalization and review status. The mathematical development, calculations, formalization and writing used substantial AI assistance. This draft was prepared with OpenAI ChatGPT/Codex assistance from an existing review note and the project's arithmetic argument. The proof is given here independently of access to code.

A private development contains the declarations `affine_iff_gcd` and `nonaffine_iff_gcd` in `QuarterArithmeticClassification.lean`. Its recorded environment is Lean 4.29.0 and mathlib revision `8a178386ffc0f5fef0b77738bb5449d50efeea95`. The recorded CI reports successful compilation and axiom audits. No new Lean compilation or independent human mathematical review was performed in preparing this draft. A publicly accessible, version-pinned formalization reference remains to be provided before submission if the formalization is to be independently inspected. No complete human understanding declaration is inferred on the contributor's behalf.

References

[1] J. Rosenblatt, *Phase retrieval*, Communications in Mathematical Physics **95** (1984), 317–343. `https://doi.org/10.1007/BF01212402`. Consulted through later restatements for this draft.

[2] F. Jedrzejewski and T. Johnson, *The Structure of Z-Related Sets*, Mathematics and Computation in Music, LNCS 7937 (2013), 128–137. `https://arxiv.org/abs/1304.6608`.

[3] W. Q. Erickson and N. B. Jones, *Homometric subsets of $\mathbb{Z}_n$ with cardinality 5: classification and enumeration*, arXiv:2412.08997v4 (27 August 2026). `https://arxiv.org/abs/2412.08997v4`.