THE CYCLIC INTERVAL LEMMA FOR EVERY ODD MODULUS

KOREA SUPERINTELLIGENCE LABS

Abstract. Let $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ and call $W(a, L) = \{a, a+1, \dots, a+L-1\}$, $0 \le L \le m$, an *arc*. An arc W *beats* a set $x \subseteq \mathbb{Z}_m$ when $|W \triangle x| < \min(|W|, m - |W|)$. Fokam Souop and Bitjoka, studying the least dimension $k_{\min}(C_m)$ of a binary Cayley graph into which the cycle C_m embeds isometrically, isolated the assertion that for odd m every $x \notin \{\emptyset, \mathbb{Z}_m\}$ is beaten by some arc. They proved it in one regime, verified it by computer for all odd $m \le 17$, and left it as a conjecture; it is the first of the three problems their paper leaves open. We prove it for every odd m. The argument instantiates the hypothesis "no arc beats x" at exactly two arc lengths, d and $d+1$ where $m = 2d+1$, which squeezes every length-d window of x to the same cardinality, and a single double count then forces $|x| \in \{0, m\}$. We also settle the case the source does not discuss: for $m = 2h$ the sets that no arc beats are *exactly* the sets invariant under the antipodal rotation $i \mapsto i + h$, and there are exactly 2^h of them, $2^h - 2$ of them proper and nonempty. So the parity hypothesis is not an artefact of the proof. An independent exhaustive search over all $2^m - 2$ proper nonempty subsets of $\mathbb{Z}_m$ confirms the odd statement for every odd $m \le 31$ and the count $2^h - 2$ for every even $m \le 24$. Every result below is machine-checked in Lean 4.

1. Introduction

The objects. Fix an integer $m \ge 1$ and write $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$. An *arc* (a cyclic interval) is a set

$$W(a, L) \;=\; \{\, a,\, a+1,\, \dots,\, a+L-1 \,\} \;\subseteq\; \mathbb{Z}_m, \qquad a \in \mathbb{Z}_m, \quad 0 \le L \le m,$$

so that $|W(a, L)| = L$; the two degenerate arcs are $W(a, 0) = \emptyset$ and $W(a, m) = \mathbb{Z}_m$. For $x \subseteq \mathbb{Z}_m$ let $W \triangle x = (W \setminus x) \cup (x \setminus W)$ be the symmetric difference.

Definition 1.1. An arc $W \subseteq \mathbb{Z}_m$ *beats* $x \subseteq \mathbb{Z}_m$ if

$$|W \triangle x| \;<\; \min\big(|W|,\, m - |W|\big).$$

We say x *escapes* if no arc of $\mathbb{Z}_m$ beats it.

The right-hand side is the distance in the cycle C_m between the two ends of the arc: index the vertices of C_m by $\mathbb{Z}_m$ and its edges by $e_i = \{v_i, v_{i+1}\}$, so that a set of edges $W(a, L)$ is a path from v_a to v_{a+L}, and $d_{C_m}(v_a, v_{a+L}) = \min(L, m - L)$. Reading x as a set of edges too, "W beats x" says that the edge set $W \triangle x$ is strictly shorter than the distance between the two vertices it is supposed to join.

The source and its open question. The definition is due to Fokam Souop and Bitjoka [4], who reach it from a question about isometric embeddings. For a finite connected graph G they write

$$k_{\min}(G) \;=\; \min\{\, k :\; G \hookrightarrow \mathrm{Cay}(\mathbb{Z}_2^k, S) \text{ isometrically for some } S \,\},$$

and their companion construction gives $k_{\min}(G) \le n - 1$ for a graph on n vertices. Odd cycles are their extremal example: they prove $k_{\min}(C_m) = m - 1$ for every odd $m \le 17$, and for every odd m for which the following assertion holds, so that the universal upper bound cannot be improved.

Conjecture 1.2 (Fokam Souop–Bitjoka [4, Lemma 3 and Conjecture 1])**.** Let m be odd and $x \subseteq \mathbb{Z}_m$ with $x \notin \{\emptyset, \mathbb{Z}_m\}$. Then there is an arc W with $|W \triangle x| < \min(|W|, m - |W|)$.

All numbered references to [4] in this paper are to v1, which is the only version on the arXiv and carries no journal reference; the numbers were resolved by compiling the e-print's own LaTeX source,

whose labels are `lem:interval` (Lemma 3), `thm:odd` (Theorem 5), `conj:interval` (Conjecture 1) and `sec:oddcycles` (§4).

The mechanism by which Conjecture 1.2 controls $k_{\min}(C_m)$ is short [4, §4]: an isometric embedding of C_m into $\mathrm{Cay}(\mathbb{Z}_2^k, S)$ assigns a generator s_i to each edge e_i, the *dependency code* $D = \{x \in \mathbb{F}_2^m : \sum_{i\in x} s_i = 0\}$ records the relations among them, and isometry forces $\min_{x\in D} |W \triangle x| = \min(|W|, m - |W|)$ for every arc W. If the generators had rank at most $m-2$ then $\dim D \geq 2$, so D would contain some $x \notin \{\emptyset, \mathbb{Z}_m\}$, and an arc beating that x contradicts isometry. The authors of [4] prove Conjecture 1.2 in what they call the covering-arc regime — when, after complementing so that $|x| \leq d = (m-1)/2$, the set x fits inside an arc of length at most d — and report of the rest that it "was checked exhaustively for all odd $m \leq 17$ ($2^{17} - 2$ subsets at $m = 17$), with no counterexample". Their conclusion lists three open problems, the first of which is this one: it "would give $k_{\min}(C_m) = m - 1$ for all odd m unconditionally". The other two — the exact value of $\nu(\text{Petersen}) \in [11, 16]$, where $\nu(G)$ is the least order of an abelian group hosting G isometrically, and the growth of their "abelian dividend" — are not touched here.

What is settled. Conjecture 1.2 is true, for every odd modulus.

Theorem 1.3 (Theorem 3.1)**.** *Let m be odd and let $x \subseteq \mathbb{Z}_m$ with $x \neq \emptyset$ and $x \neq \mathbb{Z}_m$. Then some arc beats x.*

The proof occupies about fifteen lines and uses no computer search. It instantiates the negated conclusion at only two of the $m+1$ available arc lengths. Writing $m = 2d+1$ and $c(a) = |W(a,d) \cap x|$, the m arcs of length d give $2c(a) \leq |x|$, while the m arcs of length $d+1$ — whose complements are again arcs of length d — give $|x| \leq 2c(a) + 1$. So $2c(a) \in \{|x| - 1, |x|\}$; since $2c(a)$ is even, the parity of $|x|$ pins $c(a)$ to a single value, the *same* value for every a. The double count $\sum_{a\in\mathbb{Z}_m} c(a) = d\,|x|$ then forces $|x| = 0$ when $|x|$ is even and $|x| = m$ when $|x|$ is odd, both excluded.

The second result says why the hypothesis in Conjecture 1.2 is on m and not on x. The source states its lemma for odd m and offers no reason; the even case is not sporadic but exactly describable.

Theorem 1.4 (Theorem 4.1)**.** *Let $m = 2h$ with $h \geq 1$ and let $x \subseteq \mathbb{Z}_m$. Then x escapes if and only if $x + h = x$, that is, if and only if $i \in x \iff i + h \in x$ for every $i \in \mathbb{Z}_m$.*

Theorem 1.5 (Proposition 4.2)**.** *For $m = 2h$ with $h \geq 1$ there are exactly 2^h sets $x \subseteq \mathbb{Z}_m$ invariant under $i \mapsto i + h$, hence exactly 2^h escaping sets, of which exactly $2^h - 2$ are proper and nonempty.*

Together, Theorems 1.3 and 1.4 answer the question for every modulus (Corollary 5.1): a proper nonempty $x \subseteq \mathbb{Z}_m$ is beaten by some arc unless m is even and x is antipodally invariant.

Remark 1.6. Combining Theorem 1.3 with [4, Theorem 5] removes the hypothesis from that theorem: $k_{\min}(C_m) = m - 1$ for every odd cycle, unconditionally. The implication is entirely the source's, and $k_{\min}$ is not among the objects formalized here (§8); we state the consequence and claim only Theorem 1.3.

On the size of the contribution. We make no claim of depth. Theorem 1.3 has a fifteen-line elementary proof, and Theorem 1.4 reuses the same window count with the double count forcing equality instead of a contradiction; a reader who classifies such arguments as folklore will not be argued with. What the paper offers is that a specific conjecture, stated as open in a July 2026 preprint by an author writing a series of papers on the invariant it governs, is true, that its parity hypothesis is now explained rather than assumed, and that all of it is machine-checked.

Relation to the literature. We have not found the statement of Definition 1.1, for any modulus, outside [4] and the same authors' dissertation manuscript [5], which states the same lemma, proves the same covering-arc case, and lists the conjecture first among its open problems. The search covered a full-text corpus of 879,091 arXiv sources (mathematics, computer science and economics, 2007–2026, so including the months around [4]), in which the phrase "cyclic interval lemma" occurs in exactly those two documents and the literal patterns $m - |W|$ and $\triangle x|$ occur nowhere else; a full-text

query of OpenAlex returned the same two; the literature citing [4], as recorded by Semantic Scholar, consists of three self-citations by the same authors; and the counts $2, 6, 14, 30, \ldots$ of Theorem 1.5 retrieve only the generic sequence $2^n - 2$ from the OEIS. The arXiv metadata search agrees: the phrase "cyclic interval lemma" returns [4] and nothing else, "binary Cayley graph" returns [4] and [1] and nothing else, and the fifteen hits for "cyclic interval" are otherwise about cyclic interval edge colourings, positroids and unrelated subjects. The searches were run on 2026-08-28.

Two adjacent lines of work should be named, neither of which contains Theorem 1.3. First, the numerology $m-1$ for binary Cayley graphs also arises from odd *girth*: Beaudou, Naserasr and Tardif prove that a binary Cayley graph of odd girth $2k+1$ contains the projective cube PC_{2k}, on 2^{2k} vertices, as a subgraph [1, Theorem 1.5 of arXiv:1502.00776v1]. That containment is theirs and not Payan's: Payan's earlier theorem [8] is weaker, and [1] cite it for the corollary that no binary Cayley graph has chromatic number 3. The odd-girth hypothesis is not the one here — an isometric copy of C_m inside a host does not by itself prevent the host from carrying a shorter odd cycle elsewhere — and [4] cites neither. Second, Definition 1.1 has the shape of a discrepancy condition for arcs, but the circular discrepancy literature, of which Chung and Graham [2] is the nearest item we found, measures a different quantity. Finally, odd cycles are not partial cubes, so the Djoković–Winkler theory of isometric subgraphs of hypercubes [3, 9] does not speak to $k_{\min}(C_m)$.

Organisation. Section 2 fixes the two counting identities the proofs use. Section 3 proves Theorem 1.3, Section 4 Theorems 1.4 and 1.5, and Section 5 combines them. Section 6 records what fails when a hypothesis is dropped. Section 7 describes the exhaustive searches, which are independent confirmation and are not used in any proof. Section 8 describes the formal verification.

2. Preliminaries

Throughout, $m \geq 1$, $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$, and arcs are as in §1. All sets are subsets of $\mathbb{Z}_m$ and $|\cdot|$ is cardinality. We record three facts; all three are immediate, and all three are used repeatedly.

Lemma 2.1. *For all $A, B \subseteq \mathbb{Z}_m$, $|A \triangle B| + 2|A \cap B| = |A| + |B|$.*

Proof. $A \triangle B$ is the disjoint union of $A \setminus B$ and $B \setminus A$, and $|A \setminus B| + |A \cap B| = |A|$, $|B \setminus A| + |A \cap B| = |B|$. □

Lemma 2.2. *Let $0 \leq L \leq m$. The arcs $W(a, L)$ and $W(a + L,\, m - L)$ are disjoint with union $\mathbb{Z}_m$; consequently, for every $x \subseteq \mathbb{Z}_m$,*

$$|W(a, L) \cap x| + |W(a + L,\, m - L) \cap x| = |x|.$$

Proof. Every $i \in \mathbb{Z}_m$ is $a + j$ for a unique $0 \leq j < m$, and i lies in the first arc when $j < L$ and in the second when $j \geq L$. Intersecting the partition with x gives the count. □

We refer to $W(a + L, m - L)$ as the arc *complementary* to $W(a, L)$. Note that $\min(L, m - L)$ is unchanged by $L \mapsto m - L$, and that $|W \triangle x| = |W^c \triangle x^c|$, so an arc W beats x if and only if the complementary arc beats x^c.

Lemma 2.3 (double count)**.** *Let $0 \leq L \leq m$ and $x \subseteq \mathbb{Z}_m$. Then*

$$\sum_{a \in \mathbb{Z}_m} \big|W(a, L) \cap x\big| \;=\; L\,|x|.$$

Proof. Exchange the order of summation: the left side counts the pairs (a, i) with $i \in x$ and $i \in W(a, L)$. For fixed i, the condition $i \in W(a, L)$ says $a \in \{i, i - 1, \ldots, i - L + 1\}$, a set of exactly L starting points since $L \leq m$. □

3. Odd moduli

Theorem 3.1. *Let m be odd and let $x \subseteq \mathbb{Z}_m$ satisfy $x \neq \emptyset$ and $x \neq \mathbb{Z}_m$. Then there exist $a \in \mathbb{Z}_m$ and $0 \leq L \leq m$ with*

$$\big|W(a,L) \triangle x\big| \;<\; \min\big(L,\; m-L\big).$$

Proof. Write $m = 2d+1$ and $w = |x|$, so $0 < w < m$ by hypothesis. Suppose, for contradiction, that no arc beats x; that is,

$$\big|W(a,L) \triangle x\big| \;\geq\; \min(L, m-L) \qquad \text{for all } a \in \mathbb{Z}_m,\ 0 \leq L \leq m. \tag{1}$$

Put $c(a) = |W(a,d) \cap x|$. We use (1) at two lengths only.

Length d. Here $\min(d, m-d) = \min(d, d+1) = d$, and Lemma 2.1 with $A = W(a,d)$ gives $|W(a,d) \triangle x| = d + w - 2c(a)$. So (1) reads $d + w - 2c(a) \geq d$:

$$2c(a) \;\leq\; w \qquad \text{for every } a \in \mathbb{Z}_m. \tag{2}$$

Length $d+1$. Fix $b \in \mathbb{Z}_m$ and apply (1) to the arc $W(b-(d+1),\, d+1)$, whose complementary arc is $W(b,\, m-(d+1)) = W(b,d)$. Here $\min(d+1, m-(d+1)) = \min(d+1, d) = d$. By Lemma 2.2, $|W(b-(d+1), d+1) \cap x| = w - c(b)$, so Lemma 2.1 gives

$$\big|W(b-(d+1), d+1) \triangle x\big| \;=\; (d+1) + w - 2\big(w - c(b)\big) \;=\; d + 1 - w + 2c(b),$$

and (1) reads $d + 1 - w + 2c(b) \geq d$:

$$w \;\leq\; 2c(b) + 1 \qquad \text{for every } b \in \mathbb{Z}_m. \tag{3}$$

The squeeze. By (2) and (3), $2c(a) \in \{w-1, w\}$ for every a. The left side is even, so exactly one of the two values is attainable, and which one is determined by the parity of w alone. Hence c is constant on $\mathbb{Z}_m$: either $2c(a) = w$ for every a (if w is even) or $2c(a) = w - 1$ for every a (if w is odd).

The double count. Lemma 2.3 at $L = d$ gives $\sum_{a \in \mathbb{Z}_m} c(a) = d\,w$, and the sum has $m = 2d+1$ terms. If w is even, summing $2c(a) = w$ gives $2dw = \sum_a 2c(a) = (2d+1)w$, so $w = 0$; if w is odd, summing $2c(a) = w - 1$ gives $2dw = (2d+1)(w-1)$, so $w = 2d+1 = m$. Both contradict $0 < w < m$. □

Nothing in the proof is a search: the hypothesis is used at $2m$ of the $m(m+1)$ arcs, and the two instantiations already determine $|x|$. The theorem is Conjecture 1.2, i.e. [4, Conjecture 1], and with it [4, Lemma 3] becomes a theorem for every odd m.

4. Even moduli

For $m = 2h$ call $x \subseteq \mathbb{Z}_m$ *antipodally invariant* if $i \in x \iff i + h \in x$ for every $i \in \mathbb{Z}_m$, equivalently if $x + h = x$. The two exempted sets $\emptyset$ and $\mathbb{Z}_m$ are antipodally invariant, and so is $\{0, 2\} \subseteq \mathbb{Z}_4$; the next theorem says that these are the only obstructions, at every even modulus.

Theorem 4.1. *Let $m = 2h$ with $h \geq 1$ and let $x \subseteq \mathbb{Z}_m$. Then no arc beats x if and only if x is antipodally invariant.*

Proof. ($\Leftarrow$) Invariant sets escape. Let $x + h = x$ and let $W = W(a,L)$ with $L \leq h$. Then W and $W + h = W(a+h, L)$ are disjoint, because $L \leq h$ and the two starting points differ by h in $\mathbb{Z}_{2h}$; and $|W \cap x| = |(W+h) \cap x|$, because translation by h is a bijection of $\mathbb{Z}_m$ carrying W to $W + h$ and x to itself. Therefore

$$2|W \cap x| \;=\; |W \cap x| + |(W+h) \cap x| \;=\; \big|(W \cup (W+h)) \cap x\big| \;\leq\; |x|,$$

and Lemma 2.1 turns this into $|W \triangle x| = L + |x| - 2|W \cap x| \geq L = \min(L, m-L)$. So no arc of length at most h beats x. For $L > h$ the complementary arc W^c has length $m - L < h$ and x^c is again antipodally invariant, so the case already proved gives $|W \triangle x| = |W^c \triangle x^c| \geq m - L = \min(L, m-L)$.

(⇒) Escaping sets are invariant. Suppose no arc beats x, and put $w = |x|$ and $c(a) = |W(a,h) \cap x|$. Since $\min(h, m-h) = h$, the argument of (2) applies verbatim at length h and gives $2c(a) \le w$ for every $a \in \mathbb{Z}_m$. Summing over the $m = 2h$ elements of $\mathbb{Z}_m$ and using Lemma 2.3 at $L = h$,

$$\sum_{a \in \mathbb{Z}_m} 2c(a) \;=\; 2h\,w \;=\; m\,w \;=\; \sum_{a \in \mathbb{Z}_m} w,$$

so the termwise inequality $2c(a) \le w$ is an equality for every a; in particular c is constant. Now compare two ways of peeling the arc of length $h+1$ starting at a:

$$W(a, h+1) = W(a,h) \cup \{a+h\} = \{a\} \cup W(a+1, h),$$

both unions being disjoint. Intersecting with x and counting,

$$c(a) + [\,a + h \in x\,] \;=\; \big|W(a, h+1) \cap x\big| \;=\; c(a+1) + [\,a \in x\,],$$

where $[\,\cdot\,]$ is 1 or 0 according to truth. As $c(a) = c(a+1)$, we get $[\,a+h \in x\,] = [\,a \in x\,]$ for every $a \in \mathbb{Z}_m$, which is antipodal invariance. □

Theorem 4.1 needs no properness hypothesis: $\emptyset$ and $\mathbb{Z}_m$ are invariant and do escape, consistently with both sides. It also explains the shape of Conjecture 1.2: at an even modulus the escaping sets form a structured family of size 2^h, not a sporadic list.

Proposition 4.2. *Let $m = 2h$ with $h \ge 1$. The number of antipodally invariant $x \subseteq \mathbb{Z}_m$ is exactly 2^h, and exactly $2^h - 2$ of them satisfy $x \ne \emptyset$ and $x \ne \mathbb{Z}_m$. By Theorem 4.1 these are the escaping sets, so $\mathbb{Z}_m$ has exactly $2^h - 2$ proper nonempty escaping subsets.*

Proof. The arc $A = W(0,h)$ and its translate $A + h$ partition $\mathbb{Z}_m$ (Lemma 2.2 with $L = h$). Map an invariant x to $x \cap A$. In the other direction send $S \subseteq A$ to $S \cup (S+h)$, which is invariant because $2h = 0$ in $\mathbb{Z}_m$. The two maps are mutually inverse: $(S \cup (S+h)) \cap A = S$ since $S \subseteq A$ and $(S+h) \cap A = \emptyset$; and $x = (x \cap A) \cup ((x \cap A) + h)$ for invariant x, because every $i \in x$ lies in A or in $A + h$, and in the second case $i - h \in x \cap A$. Hence the invariant sets are in bijection with the $2^{|A|} = 2^h$ subsets of A. Both $\emptyset$ and $\mathbb{Z}_m$ are invariant and they are distinct since $h \ge 1$, which gives the second count. □

5. Every modulus at once

Corollary 5.1. *Let $m \ge 1$ and let $x \subseteq \mathbb{Z}_m$ with $x \ne \emptyset$ and $x \ne \mathbb{Z}_m$. Then some arc beats x if and only if x is not antipodally invariant for a halving of m; that is, if and only if there is no h with $m = 2h$ and $x + h = x$.*

Proof. If $m = 2h$ and $x + h = x$ then no arc beats x by Theorem 4.1. Conversely, suppose no such h exists. If m is odd, Theorem 3.1 produces a beating arc. If $m = 2h$, then x is not antipodally invariant, and Theorem 4.1 again produces one. □

For odd m the right-hand side is vacuously true, so Corollary 5.1 contains Theorem 3.1; for even m it is Theorem 4.1 restricted to proper nonempty sets.

6. Sharpness

The following are finite verifications, each decided by direct evaluation over the sets and arcs named; none is used in the proofs above. They record that no hypothesis of Theorem 3.1 can be dropped and that its conclusion cannot be strengthened.

Proposition 6.1.
(i) *In $\mathbb{Z}_5$, no arc beats $\emptyset$ and no arc beats $\mathbb{Z}_5$; so both exclusions in Theorem 3.1 are needed.*
(ii) *In $\mathbb{Z}_4$, no arc beats $\{0,2\}$; so the hypothesis that m is odd cannot be removed from Theorem 3.1.*
(iii) *In $\mathbb{Z}_5$, no arc W satisfies $|W \triangle \{0\}| + 1 < \min(|W|, 5 - |W|)$; so the bound in Definition 1.1 cannot be lowered by one.*

(iv) *In $\mathbb{Z}_5$, no arc of length at most 1 beats $\{0,2\}$, while $W(0,3)$ does; so the quantifier over lengths in Theorem 3.1 is not decoration and its conclusion is not vacuous.*
(v) *Every one of the $2^5-2=30$ proper nonempty subsets of $\mathbb{Z}_5$ is beaten by some arc.*

Item (ii) is the smallest antipodally invariant set of Theorem 4.1, and item (v) is Theorem 3.1 at $m=5$ re-derived from the definitions rather than from the theorem.

7. Exhaustive confirmation

The searches in this section are independent of Sections 3–5: they were run in a second encoding, in which a subset of $\mathbb{Z}_m$ is the set of positions of the set bits of an integer below 2^m, symmetric difference is bitwise exclusive-or, and cardinality is a bit-count loop. They share no definitions with the development that proves Theorems 3.1 and 4.1. Their value is agreement between two encodings, not evidence for the theorems, which are proved outright.

For each modulus m the search enumerated all 2^m-2 integers x with $0<x<2^m-1$, that is all proper nonempty subsets of $\mathbb{Z}_m$, ranging for each of them over all $m(m+1)$ pairs (a,L) with $a\in\mathbb{Z}_m$ and $0\le L\le m$ (at $m=31$ that is 992 pairs), and reported the number of x for which no such pair yields a beating arc. The scan stops at the first beating arc it finds, which changes its running time and not the number it reports.

Proposition 7.1. *For every odd m with $3\le m\le 17$, the number of proper nonempty $x\subseteq\mathbb{Z}_m$ that escape is 0.*

This reproduces, in the encoding just described, exactly the computation [4] reports in the proof of its Lemma 3, which "was checked exhaustively for all odd $m\le 17$ ($2^{17}-2$ subsets at $m=17$), with no counterexample". The datum is theirs; the program behind it is not public, so the reproduction is independent of it.

Proposition 7.2. *For every odd m with $19\le m\le 31$, the number of proper nonempty $x\subseteq\mathbb{Z}_m$ that escape is 0.*

These seven moduli lie beyond what [4] verified; the largest, $m=31$, is a scan of $2^{31}-2=2\,147\,483\,646$ subsets. Since Theorem 3.1 proves the statement for every odd m, they are corroboration rather than evidence, and we say so.

Proposition 7.3. *For every even m with $4\le m\le 24$, the number of proper nonempty $x\subseteq\mathbb{Z}_m$ that escape is exactly $2^{m/2}-2$, that is*

$$2,\ 6,\ 14,\ 30,\ 62,\ 126,\ 254,\ 510,\ 1022,\ 2046,\ 4094$$

for $m=4,6,\dots,24$ respectively.

This is the finite shadow of Proposition 4.2. A separate scan of the same range, run outside the formal development as a prototype in C, checked the finer statement that at each even $m\le 24$ the escaping sets are *exactly* the proper nonempty antipodally invariant ones — no escaping set outside that family, no invariant set beaten — which is Theorem 4.1 cell by cell. That prototype is a cross-check and nothing more: it was written from Definition 1.1 alone, it lies outside the formal development, it is not verified by Lean in any sense, and no statement of this paper rests on it. What is formally verified at even moduli is Proposition 7.3, the count; the finer cell-by-cell statement is a theorem, proved in §4 with no computation at all.

The searches stop at $m=31$ for odd and $m=24$ for even moduli. The cost grows by a factor of about 4.5 per step of 2 in m: the whole of the range odd $3\le m\le 29$ together with even $4\le m\le 24$ runs in about five and a half minutes, while $m=31$ alone takes about twenty-one minutes, and $m=33$ would take hours. Nothing is lost by stopping, since Theorem 3.1 settles every odd modulus and Theorem 4.1 every even one.

8. Formal verification

All statements of this paper have been formally verified in Lean 4 (toolchain `v4.32.0`) against *Mathlib* [7, 6]; the development is free of `sorry`. Arcs are `Finset (ZMod m)` in the sense of Definition 1.1, and Theorems 3.1 and 4.1, Proposition 4.2, Corollary 5.1 and Proposition 6.1 are checked by the Lean kernel, depending only on the three standard axioms `propext`, `Classical.choice` and `Quot.sound`. The exhaustive searches of Section 7 are stated over a separate, import-free bitmask model and are evaluated by compiled code through Lean's `native_decide`; each such statement therefore carries, in addition to `propext`, the per-declaration axiom that records trust in the compiler and runtime, and none of them is used in the proof of any other statement here. The quantity $k_{\min}$ of Remark 1.6 is not formalized: the passage from Theorem 3.1 to $k_{\min}(C_m) = m - 1$ is [4, Theorem 5] and needs a development of isometric graph embeddings that this work does not contain. The repository is private; repository reference to be added at submission.

References

[1] L. Beaudou, R. Naserasr and C. Tardif, *Homomorphisms of binary Cayley graphs*, Discrete Math. **338** (2015), no. 12, 2539–2544; doi:10.1016/j.disc.2015.06.025; arXiv:1502.00776.

[2] F. R. K. Chung and R. L. Graham, *On the discrepancy of circular sequences of reals*, J. Number Theory **164** (2016) 52–65; doi:10.1016/j.jnt.2015.12.009.

[3] D. Ž. Djoković, *Distance-preserving subgraphs of hypercubes*, J. Combin. Theory Ser. B 14 (1973) 263–267.

[4] R. Fokam Souop and L. Bitjoka, *Dimension and Order Bounds for Isometric Embeddings of Graphs into Abelian Cayley Graphs, and the Abelian Dividend*, arXiv:2607.07939v1 [math.CO], 8 July 2026; submitted to European Journal of Combinatorics.

[5] R. Fokam Souop and L. Bitjoka, *Minimal Isometric Embeddings of Graphs into Abelian Groups: Theory, Algorithms, and Applications to Signal Processing over Networks*, arXiv:2606.29391v1 [math.CO], 28 June 2026; posted with the comment "Draft PhD thesis awaiting defense".

[6] L. de Moura and S. Ullrich, *The Lean 4 theorem prover and programming language*, in: Automated Deduction — CADE 28, Lecture Notes in Computer Science 12699, Springer, 2021, pp. 625–635.

[7] The mathlib Community, *The Lean mathematical library*, in: Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs (CPP 2020), ACM, 2020, pp. 367–381; arXiv:1910.09336.

[8] C. Payan, *On the chromatic number of cube-like graphs*, Discrete Math. **103** (1992), no. 3, 271–277; doi:10.1016/0012-365X(92)90319-B; Zbl 0772.05043.

[9] P. M. Winkler, *Isometric embedding in products of complete graphs*, Discrete Appl. Math. 7 (1984) 221–225.