hexagon:2611.01223v1

PRIMITIVE-PRODUCT CIRCULAR PERMUTATIONS OVER FINITE FIELDS: THE SHIFTS MINUS ONE AND PLUS ONE IN SUN'S CONJECTURE

SAI SMARAN S B

Abstract. In 2013, Zhi-Wei Sun conjectured that for every finite field $\mathbb{F}_q$ of order $q > 7$, there exist circular permutations $(a_1, \ldots, a_{q-1})$ and $(b_1, \ldots, b_{q-1})$ of $\mathbb{F}_q^\times$ such that $a_i a_{i+1} - 1$ (respectively, $b_i b_{i+1} + 1$) is a primitive element of $\mathbb{F}_q$ for every $1 \le i \le q-1$ (indices modulo $q-1$). Recently, Luo and She (`arXiv:2610.06289`, 2026) resolved the analogous problem with constant term $a_0 = 0$ for all $q > 4$, while for $a_0 \neq 0$ they established existence only for $q > 18{,}888{,}871$.

We prove the two cases with shifts -1 and $+1$ for all finite fields $\mathbb{F}_q$ with $q > 7$. Our analytic advance combines the sharp vertex-cut formulation of the Chvátal–Erdős theorem, the exact minimum degree $\delta(G) \ge \varphi(q-1) - 1$, a variance-sharpened Jacobi-sum Expander Mixing Lemma, Cohen–Huczynska–Trudgian lower sieves, and e-free upper sieves on both $I \times (\mathbb{F}_q^\times \setminus I)$ and $A \times (A \cup S)$ into a unified four-inequality *double-squeeze* criterion. This collapses the unconditional analytic threshold from $q > 18{,}888{,}871$ down to $q \ge 8{,}100$, and a certified integer-arithmetic range check over $7 < q < 8{,}100$ leaves only 44 exceptional prime powers (largest $q = 4{,}621$, a $4{,}087\times$ reduction). Sign transport ($b_k = \sqrt{-1}\, a_k$ for $q \equiv 1 \pmod 4$, and characteristic 2 for $q = 16$), explicit algebraic constructions for $\mathbb{F}_{16}$ and $\mathbb{F}_{27}$, and explicit Hamiltonian cycles for the remaining 42 prime and quadratic-extension fields complete the proof. Every step of both proofs has been independently machine-checked in Lean 4.33.1 with zero `sorry`, zero `native_decide`, and only the standard axioms {`propext`, `Classical.choice`, `Quot.sound`}.

1. Introduction

In Conjecture 3.9 of the 2013 preprint [9] (see also OEIS sequence `A229232` [8]), Zhi-Wei Sun posed the following twin conjectures on circular permutations of the multiplicative group $\mathbb{F}_q^\times = \mathbb{F}_q \setminus \{0\}$ of a finite field $\mathbb{F}_q$.

Theorem 1.1 (Main Theorem)**.** *Let $\mathbb{F}_q$ be a finite field of cardinality $q > 7$, and let $n = q - 1$.*

1. *There exists a bijection $a : \mathbb{Z}/n\mathbb{Z} \to \mathbb{F}_q^\times$ such that $a(i)\, a(i+1) - 1$ is a primitive element of $\mathbb{F}_q$ for every $i \in \mathbb{Z}/n\mathbb{Z}$.*
2. *There exists a bijection $b : \mathbb{Z}/n\mathbb{Z} \to \mathbb{F}_q^\times$ such that $b(i)\, b(i+1) + 1$ is a primitive element of $\mathbb{F}_q$ for every $i \in \mathbb{Z}/n\mathbb{Z}$.*

The bound $q > 7$ is sharp for both statements: exhaustive verification shows that neither (1) nor (2) holds for any finite field of cardinality $q \in \{2, 3, 4, 5, 7\}$. (For $q = 2$, $1 \cdot 1 \pm 1 = 0$; for $q = 3$, $1 \cdot 2 \pm 1 \in \{0, 1\}$ misses the unique primitive element 2; for $q = 4$, any 3-cycle on $\{1, \omega, \omega^2\}$ contains the adjacent pair $\{\omega, \omega^2\}$ with $\omega \cdot \omega^2 \pm 1 = 1 + 1 = 0$; for $q = 5$ and $q = 7$, direct enumeration confirms that neither primitive-product graph is Hamiltonian.)

The published formulation [10, Conjecture 3.8] allows an arbitrary shift; our theorem concerns only the two shifts -1 and $+1$. Luo and She [7] studied the generalized problem with an arbitrary shift $a_0 \in \mathbb{F}_q$ (requiring $a(i)a(i+1)+a_0$ to be primitive). They completely resolved the homogeneous case $a_0 = 0$ for all $q > 4$, and for $a_0 \neq 0$ they applied the Chvátal–Erdős theorem [1] together with character-sum bounds to prove existence for all

$$q > 18{,}888{,}871.$$

2020 *Mathematics Subject Classification.* Primary 11T30, 05C45; Secondary 11L40, 11N36, 68V20.

Key words and phrases. Finite fields, primitive elements, circular permutations, Hamiltonian cycles, Chvátal–Erdős theorem, Jacobi sums, expander mixing lemma, prime sieve, Lean 4 formal verification.

Their general bound does not cover the range $7 < q \leq 18{,}888{,}871$.

Overview of the proof. For a finite field $\mathbb{F}_q$ ($q > 7$, $n = q - 1$) and a nonzero non-primitive shift $a_0 \in \mathbb{F}_q^\times$, let $G(\mathbb{F}_q, a_0)$ be the simple undirected graph on vertex set $V = \mathbb{F}_q^\times$ in which distinct $x, y \in \mathbb{F}_q^\times$ are adjacent if and only if $xy + a_0$ is primitive in $\mathbb{F}_q$. Theorem 1.1 asserts that $G(\mathbb{F}_q, -1)$ and $G(\mathbb{F}_q, +1)$ are Hamiltonian for every prime power $q > 7$.

Our proof achieves a 4,087× reduction in the largest required explicit field (from 18,888,871 down to 4,621) through four interlocking ingredients:

(1) *Sharp vertex-cut Chvátal–Erdős criterion* (Section 2): Rather than bounding the global connectivity $\kappa(G)$ crudely, we work directly with an arbitrary vertex cut $V = S \sqcup A \sqcup B$ ($1 \leq |A| \leq |B|$, $E(A, B) = \emptyset$) and independent set I with $|S| < |I|$. Together with the exact minimum degree $\delta(G) \geq \varphi(n) - 1$, this enforces $|A| + |S| \geq \varphi(n)$.

(2) *Variance-sharpened Expander Mixing + double-sided sieves* (Section 3): Using twisted Jacobi-sum bounds and Parseval's identity on $\mathbb{F}_q^\times$, we obtain an Expander Mixing Lemma with the variance factor $\sqrt{|X|(1 - |X|/n)|Y|(1 - |Y|/n)}$. Applying Cohen–Huczynska–Trudgian lower sieves [2, 3, 4] on $I \times I$ and $A \times B$, and e-free *upper* sieves on $I \times (V \setminus I)$ and $A \times (A \cup S)$, yields four simultaneous constraints (7)–(10) on $(\alpha, k, a, b) = (|I|, |S|, |A|, |B|)$.

(3) *Unconditional analytic coverage for* $q \geq 8{,}100$ *and certified integer double-squeeze below* 8,100 (Sections 4–5): An algebraic reduction of (7)–(8) eliminates all $q \geq 8{,}100$ unconditionally: $\omega(n) \geq 8$ via a prime-swap inequality against $P_8 = \{2, 3, 5, 7, 11, 13, 17, 19\}$, and $\omega(n) \in \{1, \ldots, 7\}$ via seven explicit rational parameter sets (Table 1). For $7 < q < 8{,}100$, a certified integer-arithmetic checker partitions the admissible cut-side range $a \in [a_{\mathrm{lo}}, \lfloor n/2 \rfloor]$ into a large-a region killed by the lower-sieve cut bound (8) and a small-a region killed point-by-point by the upper-sieve cut bound (10). This eliminates every prime power $7 < q < 8{,}100$ except precisely 44 fields, all with $q \leq 4{,}621$.

(4) *Sign transport and explicit constructions for the* 44 *exceptions* (Section 6): For $q \equiv 1 \pmod 4$, multiplying a cycle for $a_0 = -1$ by $s \in \mathbb{F}_q^\times$ with $s^2 = -1$ produces a cycle for $a_0 = +1$ (Lemma 2.1); for $\operatorname{char} \mathbb{F}_q = 2$, $-1 = +1$. Thus $a_0 = +1$ requires separate cycles only for the 24 exceptional primes with $p \equiv 3 \pmod 4$ and for $q = 27$. We give self-contained algebraic constructions via Zech logarithms for $\mathbb{F}_{16}$ and $\mathbb{F}_{27}$, and explicit Hamiltonian cycles for the 34 prime fields $\mathbb{F}_p$ and 8 quadratic extensions $\mathbb{F}_{p^2} \cong \mathbb{F}_p[x]/(x^2 - d)$ (Table 2).

Remark 1.2 (General non-primitive shifts). The analytic criterion (Theorem 3.5), its unconditional range $q \geq 8{,}100$ (Theorem 4.3), and the certified range check below 8,100 (Proposition 5.1) depend only on $a_0 \in \mathbb{F}_q^\times$ being non-primitive. Hence $G(\mathbb{F}_q, a_0)$ is Hamiltonian for every finite field $\mathbb{F}_q$ ($q > 7$) outside the 44 prime powers in Table 2 and every non-primitive $a_0 \in \mathbb{F}_q^\times$.

Formal verification. To eliminate any risk of subtle edge-case errors in the sieve inequalities, prime-swap arithmetic, range verification, or cycle checking, the entire proof of both parts of Theorem 1.1—including Göring's proof of Menger's theorem [5], the Chvátal–Erdős theorem, all character-sum and sieve lemmas, all analytic cases, the soundness of the integer range checker, and every single one of the 44 exceptional fields—has been formally verified in Lean 4.33.1 against the formal statements `OeisA229232.conjecture_4` and `OeisA229232.conjecture_5` of `formal-conjectures`. The standalone proofs are archived in the repository `saientropy/open-math-agents` (commits `e6e59ccc` and `64c0bd65`; 6,935 and 6,951 lines, zero warnings, zero `sorry`, zero `native_decide`, depending solely on the standard axioms {`propext`, `Classical.choice`, `Quot.sound`}). Section 7 documents the verification architecture in detail.

2. Sign Transport and the Chvátal–Erdős Reduction

Throughout, let $\mathbb{F}_q$ be a finite field of cardinality $q > 7$ and set $n := q - 1 \geq 7$. An element $x \in \mathbb{F}_q$ is *primitive* if $x \neq 0$ and x has multiplicative order n in $\mathbb{F}_q^\times$. Since $\mathbb{F}_q^\times$ is cyclic of order n, there are exactly $\varphi(n)$ primitive elements in $\mathbb{F}_q$.

Lemma 2.1 (Sign Transport)**.** *Let $\mathbb{F}_q$ be a finite field with $q > 7$ and $n = q - 1$. Suppose Theorem 1.1(1) holds for $\mathbb{F}_q$.*

(a) *If $q \equiv 1 \pmod 4$, then Theorem 1.1(2) also holds for $\mathbb{F}_q$.*
(b) *If q is even (i.e., $\operatorname{char} \mathbb{F}_q = 2$), then Theorem 1.1(2) also holds for $\mathbb{F}_q$.*

Proof. For (b), $2 = 0$ in $\mathbb{F}_q$ gives $-1 = 1$, so the two statements are identical.

For (a), write $n = 4k$ with $k \geq 2$ and let g be a generator of $\mathbb{F}_q^\times$. Set $s := g^k$. Then $s^2 = g^{2k}$ satisfies $(s^2)^2 = g^n = 1$ and $s^2 \neq 1$ (since $\operatorname{ord}(g) = 4k > 2k$), so $s^2 = -1$ in $\mathbb{F}_q$. We claim that if $x \in \mathbb{F}_q^\times$ is primitive, then $-x$ is also primitive. Indeed, $(x^{2k})^2 = x^n = 1$ and $x^{2k} \neq 1$, whence $x^{2k} = -1$ and therefore $-x = x^{2k+1}$. Any divisor d of $\gcd(2k+1, 4k)$ divides $2(2k+1) - 4k = 2$; since $2k+1$ is odd, d cannot equal 2, so $\gcd(2k+1, n) = 1$. Thus $-x = x^{2k+1}$ is primitive.

Now let $a : \mathbb{Z}/n\mathbb{Z} \to \mathbb{F}_q^\times$ be a bijection satisfying Theorem 1.1(1), and define $b(i) := s\, a(i)$. Since multiplication by $s \in \mathbb{F}_q^\times$ is a bijection on $\mathbb{F}_q^\times$, b is a bijection, and for every $i \in \mathbb{Z}/n\mathbb{Z}$,

$$b(i)\, b(i+1) + 1 = s^2 a(i)\, a(i+1) + 1 = -\big(a(i)\, a(i+1) - 1\big),$$

which is primitive by the claim above. □

We now record the exact vertex-cut formulation of the Chvátal–Erdős theorem [1] used in our analytic criterion, together with its self-contained proof via Göring's short proof of vertex-Menger's theorem [5].

Lemma 2.2 (Vertex-Menger's Theorem, after Göring [5])**.** *Let $G = (V, E)$ be a finite simple graph and $A, B \subseteq V$. The maximum number of pairwise vertex-disjoint A–B paths equals the minimum cardinality of an A–B vertex separator $S \subseteq V$ (a set meeting every A–B path).*

Proof. We proceed by induction on $|E|$. When $E = \emptyset$, every A–B path is a single vertex in $A \cap B$, so both quantities equal $|A \cap B|$. Suppose $E \neq \emptyset$ and let k be the minimum size of an A–B separator in G. Pick any edge $e = uv \in E$ and set $G' = G - e$. If G' still has no A–B separator of size $< k$, the induction hypothesis gives k pairwise vertex-disjoint A–B paths in $G' \subseteq G$.

Otherwise, G' admits an A–B separator S' of size $k - 1$. Since S' is not an A–B separator in G, some A–B path in G avoids S' and must therefore traverse $e = uv$, forcing $u, v \notin S'$. Thus both $S_u := S' \cup \{u\}$ and $S_v := S' \cup \{v\}$ are A–B separators of size k in G (any A–B path avoiding S' traverses $e = uv$, hence visits both u and v). In G', every A–S_u separator is also an A–B separator of G (since every A–B path in G meets S_u before or upon first using e), so the minimum size of an A–S_u separator in G' is at least k, hence equals k. Similarly, the minimum size of an S_v–B separator in G' equals k. By the induction hypothesis on G', there exist k pairwise vertex-disjoint A–S_u paths $P_1, \ldots, P_k$ and k pairwise vertex-disjoint S_v–B paths $Q_1, \ldots, Q_k$ in G'.

Truncating each P_i at its first vertex in S_u and each Q_j at its last vertex in S_v, we may assume that each P_i meets S_u only at its endpoint and each Q_j meets S_v only at its starting vertex. Moreover, no P_i contains a vertex of any Q_j outside S': if some P_i met some Q_j at a vertex $w \notin S'$, then following P_i from A to w and Q_j from w to B would yield an A–B path in G' avoiding S', a contradiction. Thus concatenating the $k - 1$ pairs ending/starting at each vertex of S' together with the path $P_{i_0} \cdot e \cdot Q_{j_0}$ joining the unique P_{i_0} ending at u to the unique Q_{j_0} starting at v produces k pairwise vertex-disjoint A–B paths in G. □

Theorem 2.3 (Chvátal–Erdős Vertex-Cut Criterion)**.** *Let $G = (V, E)$ be a finite simple graph with $|V| \geq 3$. Suppose that for every partition $V = S \sqcup A \sqcup B$ with $A \neq \emptyset$, $B \neq \emptyset$, and $E(A, B) = \emptyset$, and every independent set $I \subseteq V$, we have $|I| \leq |S|$. Then G contains a Hamiltonian cycle.*

Proof. We first verify that G contains a cycle of length at least 3. If G is complete, any cyclic ordering of V is a Hamiltonian cycle. Otherwise, choose non-adjacent $x, y \in V$; applying the hypothesis to $I = \{x, y\}$ shows that G has no vertex cut of size ≤ 1, so G is 2-connected. Since $|V| \geq 3$, every vertex has degree at least 2, and taking a maximal path shows that G contains a cycle of length at least 3.

Let $C = (c_0, c_1, \ldots, c_{L-1})$ be a longest cycle in G ($L \geq 3$), and suppose for contradiction that $L < |V|$. Pick $v \in V \setminus V(C)$, and apply Lemma 2.2 in the induced subgraph $G - v$ to the neighborhood $A_0 := N_G(v)$ and $B_0 := V(C)$. Let $S \subseteq V \setminus \{v\}$ be a minimum-size A_0–B_0 vertex separator in $G - v$, and set $m := |S|$. By Lemma 2.2, $G - v$ contains m pairwise vertex-disjoint A_0–B_0 paths. Truncating each path at its first intersection with $V(C)$ and prepending the vertex v produces m paths $P_1, \ldots, P_m$ from v to distinct vertices $x_1, \ldots, x_m \in V(C)$ that are pairwise vertex-disjoint except at v and meet $V(C)$ only at their endpoints $x_1, \ldots, x_m$.

For each $1 \leq i \leq m$, let x_i^+ denote the successor of x_i along C. We claim that

$$I := \{v, x_1^+, \ldots, x_m^+\}$$

is an independent set of size $m + 1$ in G:

- First, $v \notin V(C)$ and $x_1, \ldots, x_m$ are distinct, so $|I| = m + 1$.
- No x_i^+ is adjacent to v: otherwise replacing the edge $x_i x_i^+$ of C by the path P_i (from x_i to v) followed by the edge $v x_i^+$ yields a cycle strictly longer than C.
- No two distinct x_i^+, x_j^+ are adjacent: otherwise, traversing C forward from x_i^+ to x_j, then along P_j reversed to v, then along P_i to x_i, then backward along C from x_i to x_j^+, and closing via the edge $x_j^+ x_i^+$ yields a cycle strictly longer than C (as it contains all vertices of C plus v).

Thus G has an independent set I of size $m + 1$. In particular, $m < L$ (for if $m = L$, then $\{x_1^+, \ldots, x_L^+\} = V(C)$ would be independent, contradicting $L \geq 3$ and $c_0 c_1 \in E$). Therefore $V(C) \not\subseteq S$, so letting A be the set of vertices reachable from v in $G - S$ and $B := V \setminus (S \cup A)$, we have $v \in A$, $V(C) \setminus S \subseteq B$ (so $A, B \neq \emptyset$), $E(A, B) = \emptyset$, and $|I| = m + 1 > m = |S|$, contradicting the hypothesis. Hence $L = |V|$, and C is a Hamiltonian cycle. □

3. Character Sums, Expander Mixing, and Double-Sided Prime Sieves

Throughout this section, let $\mathbb{F}_q$ be a finite field ($q > 7$, $n = q - 1$), let $a_0 \in \mathbb{F}_q^\times$ be non-primitive, and let $\mathcal{P}(n)$ denote the set of distinct prime divisors of n. We adopt the standard convention that multiplicative characters $\chi : \mathbb{F}_q \to \mathbb{C}$ satisfy $\chi(0) = 0$ (including the trivial character χ_0, which takes the value 1 on $\mathbb{F}_q^\times$ and 0 at 0). Recall that the Jacobi sum of two multiplicative characters ψ, χ is $J(\psi, \chi) := \sum_{t \in \mathbb{F}_q} \psi(t)\, \chi(1 - t)$.

Lemma 3.1 (Twisted Jacobi-Sum Bound)**.** *For every $a_0 \in \mathbb{F}_q^\times$ and multiplicative characters ψ, χ of $\mathbb{F}_q$ with $\chi \neq \chi_0$,*

$$\left| \sum_{u \in \mathbb{F}_q^\times} \psi(a_0 + u)\, \chi(u) \right| = |J(\psi, \chi)| \leq \begin{cases} 1 & \text{if } \psi = \chi_0, \\ \sqrt{q} & \text{if } \psi \neq \chi_0. \end{cases} \tag{1}$$

Proof. Since $\chi(0) = 0$, the sum over $u \in \mathbb{F}_q^\times$ equals the sum over all $u \in \mathbb{F}_q$. Substituting $t = 1 + a_0^{-1} u$ (a bijection on $\mathbb{F}_q$, with $a_0 + u = a_0 t$ and $u = (-a_0)(1 - t)$) yields

$$\sum_{u \in \mathbb{F}_q^\times} \psi(a_0 + u)\, \chi(u) = \psi(a_0)\, \chi(-a_0) \sum_{t \in \mathbb{F}_q} \psi(t)\, \chi(1 - t) = \psi(a_0)\, \chi(-a_0)\, J(\psi, \chi).$$

Since $|\psi(a_0)| = |\chi(-a_0)| = 1$, the modulus equals $|J(\psi,\chi)|$. By standard properties of Jacobi sums [6, Theorem 5.22], for $\chi \neq \chi_0$: if $\psi = \chi_0$, then $J(\chi_0,\chi) = \sum_{t\neq 0}\chi(1-t) = -\chi(1) = -1$ has norm 1; if $\psi = \chi^{-1}$, then $|J(\chi^{-1},\chi)| = 1 \le \sqrt{q}$; and if $\psi \neq \chi_0$ and $\psi\chi \neq \chi_0$, then $|J(\psi,\chi)| = \sqrt{q}$. □

Lemma 3.2 (Variance-Sharpened Expander Mixing Lemma)**.** *Let $f : \mathbb{F}_q^\times \to \mathbb{R}$ have mean $\mu := \frac{1}{n}\sum_{u\in\mathbb{F}_q^\times} f(u)$ and nontrivial Fourier bound*

$$\left|\sum_{u\in\mathbb{F}_q^\times} f(u)\,\chi(u)\right| \le \Lambda \qquad \text{for all multiplicative characters } \chi \neq \chi_0.$$

Then for any subsets $X, Y \subseteq \mathbb{F}_q^\times$,

$$\left|\sum_{x\in X}\sum_{y\in Y} f(xy) - \mu\,|X|\,|Y|\right| \le \Lambda\sqrt{|X|\left(1-\frac{|X|}{n}\right)|Y|\left(1-\frac{|Y|}{n}\right)}. \tag{2}$$

Proof. Let $\widehat{\mathbb{F}_q^\times}$ denote the group of n multiplicative characters on $\mathbb{F}_q^\times$. By character orthogonality, $f(u) = \frac{1}{n}\sum_{\chi\in\widehat{\mathbb{F}_q^\times}} \widehat{f}(\chi)\,\overline{\chi}(u)$ where $\widehat{f}(\chi) := \sum_{v\in\mathbb{F}_q^\times} f(v)\,\chi(v)$. Substituting $u = xy$ and separating the trivial character $\chi = \chi_0$ (which contributes $\frac{1}{n}\widehat{f}(\chi_0)\,|X|\,|Y| = \mu\,|X|\,|Y|$) gives

$$\sum_{x\in X}\sum_{y\in Y} f(xy) - \mu\,|X|\,|Y| = \frac{1}{n}\sum_{\chi\neq\chi_0}\widehat{f}(\chi)\left(\sum_{x\in X}\overline{\chi}(x)\right)\left(\sum_{y\in Y}\overline{\chi}(y)\right).$$

Applying the triangle inequality, $|\widehat{f}(\chi)| \le \Lambda$, and Cauchy–Schwarz yields

$$\left|\sum_{x\in X}\sum_{y\in Y} f(xy) - \mu\,|X|\,|Y|\right| \le \frac{\Lambda}{n}\sqrt{\sum_{\chi\neq\chi_0}\left|\sum_{x\in X}\overline{\chi}(x)\right|^2}\sqrt{\sum_{\chi\neq\chi_0}\left|\sum_{y\in Y}\overline{\chi}(y)\right|^2}.$$

By Parseval's identity on $\mathbb{F}_q^\times$,

$$\sum_{\chi\neq\chi_0}\left|\sum_{x\in X}\overline{\chi}(x)\right|^2 = \left(\sum_{\chi\in\widehat{\mathbb{F}_q^\times}}\left|\sum_{x\in X}\overline{\chi}(x)\right|^2\right) - |X|^2 = n|X| - |X|^2 = n|X|\left(1-\frac{|X|}{n}\right),$$

and identically for Y. Dividing by n gives (2). □

We now construct the E-free upper sieve and the Cohen–Huczynska–Trudgian lower sieve [2, 3]. For any prime $p \mid n$, define the p-free indicator $\mathbf{1}_p : \mathbb{F}_q \to \{0,1\}$ by $\mathbf{1}_p(x) = 1$ if $x \in \mathbb{F}_q^\times$ is not a p-th power in $\mathbb{F}_q^\times$, and $\mathbf{1}_p(x) = 0$ otherwise. Fixing a generator χ_1 of $\widehat{\mathbb{F}_q^\times}$, the subgroup of characters of order dividing p is $\{\chi_1^{jn/p} : 0 \le j < p\}$, so by character orthogonality,

$$\mathbf{1}_p(x) = \left(1-\frac{1}{p}\right)\chi_0(x) - \frac{1}{p}\sum_{j=1}^{p-1}\chi_1^{jn/p}(x) \qquad (x \in \mathbb{F}_q). \tag{3}$$

For any subset $E \subseteq \mathcal{P}(n)$, set

$$\theta(E) := \prod_{p\in E}\left(1-\frac{1}{p}\right), \qquad \mathbf{1}_E(x) := \chi_0(x)\prod_{p\in E}\mathbf{1}_p(x).$$

Here the trivial character is extended by zero, so $\mathbf{1}_E(0) = 0$ even when E is empty. Notice that $\mathbf{1}_{\mathcal{P}(n)}(x) = 1$ if and only if x is primitive in $\mathbb{F}_q$, and $\mathbf{1}_{\mathcal{P}(n)}(x) \le \mathbf{1}_E(x)$ for every $E \subseteq \mathcal{P}(n)$ and every $x \in \mathbb{F}_q$.

Lemma 3.3 (Fourier Bounds for $\mathbf{1}_E$ and the Cohen–Huczynska–Trudgian Sieve)**.** *Let $a_0 \in \mathbb{F}_q^\times$ be non-primitive.*

(a) (E-free character-sum bound.) *For any $E \subseteq \mathcal{P}(n)$, any multiplicative character η whose order is coprime to $\prod_{p\in E} p$, and any $\chi \neq \chi_0$,*

$$\left|\sum_{u\in\mathbb{F}_q^\times} \eta(a_0+u)\,\mathbf{1}_E(a_0+u)\,\chi(u)\right| \le \begin{cases} \theta(E)\big((2^{|E|}-1)\sqrt{q}+1\big) & \text{if } \eta=\chi_0,\\ \theta(E)\,2^{|E|}\sqrt{q} & \text{if } \eta\neq\chi_0. \end{cases} \tag{4}$$

In particular, setting $L_E := (2^{|E|}-1)\sqrt{q}+1$, we have $\sum_{u\in\mathbb{F}_q^\times} \mathbf{1}_E(a_0+u) \le \theta(E)\,n$ and $\max_{\chi\neq\chi_0} |\sum_{u\in\mathbb{F}_q^\times} \mathbf{1}_E(a_0+u)\chi(u)| \le \theta(E)\,L_E$.

(b) (Lower sieve.) *For any disjoint partition $\mathcal{P}(n) = E \sqcup S$ with $\Delta := 1 - \sum_{p\in S} \frac{1}{p} > 0$, define*

$$w_{E,S}(x) := \begin{cases} \mathbf{1}_E(x) & \text{if } S=\emptyset,\\ \sum_{p\in S} \mathbf{1}_{E\cup\{p\}}(x) - (|S|-1)\,\mathbf{1}_E(x) & \text{if } S\neq\emptyset, \end{cases}$$

and set $\delta := \theta(E)\,\Delta$,

$$K := \begin{cases} 2^{|E|}-1 & \text{if } S=\emptyset,\\ 2^{|E|}\left(\dfrac{|S|-1}{\Delta}+2\right)-1 & \text{if } S\neq\emptyset, \end{cases} \qquad L := K\sqrt{q}+1.$$

Then $w_{E,S}(x) \le \mathbf{1}_{\mathcal{P}(n)}(x)$ for every $x \in \mathbb{F}_q$, and

$$\sum_{u\in\mathbb{F}_q^\times} w_{E,S}(a_0+u) \ge \delta n, \qquad \max_{\chi\neq\chi_0} \left|\sum_{u\in\mathbb{F}_q^\times} w_{E,S}(a_0+u)\,\chi(u)\right| \le \delta L. \tag{5}$$

Proof. (a) Expanding $\mathbf{1}_E(x) = \prod_{p\in E}\big((1-\frac{1}{p})\chi_0(x) - \frac{1}{p}\sum_{j=1}^{p-1}\chi_1^{jn/p}(x)\big)$ produces a linear combination of products $\psi_T = \prod_{p\in T}\chi_1^{j_p n/p}$ over subsets $T \subseteq E$ and tuples $1 \le j_p < p$, with total weight of the T-terms equal to

$$\prod_{p\in E\setminus T}\left(1-\frac{1}{p}\right)\prod_{p\in T}\frac{p-1}{p} = \theta(E).$$

Because the primes in E are distinct and coprime to $\mathrm{ord}(\eta)$, the product $\eta\psi_T$ is trivial if and only if $\eta = \chi_0$ and $T = \emptyset$. Applying Lemma 3.1 to each term $\sum_{u\in\mathbb{F}_q^\times}(\eta\psi_T)(a_0+u)\chi(u)$ gives norm ≤ 1 when $\eta = \chi_0$ and $T = \emptyset$, and $\le \sqrt{q}$ for all other pairs (η, T). Summing the $2^{|E|}$ subset weights $\theta(E)$ yields (4). Moreover, $\sum_{x\in\mathbb{F}_q}\mathbf{1}_E(x) = \theta(E)\,n$ (since all nontrivial characters sum to 0 over $\mathbb{F}_q$), so $\sum_{u\in\mathbb{F}_q^\times}\mathbf{1}_E(a_0+u) = \theta(E)\,n - \mathbf{1}_E(a_0) \le \theta(E)\,n$.

(b) Pointwise inequality: if $S = \emptyset$, then $E = \mathcal{P}(n)$ and $w_{E,\emptyset} = \mathbf{1}_{\mathcal{P}(n)}$. If $S \neq \emptyset$, then for any $x \in \mathbb{F}_q$: if $\mathbf{1}_E(x) = 0$, every term vanishes so $w_{E,S}(x) = 0 \le \mathbf{1}_{\mathcal{P}(n)}(x)$; if $\mathbf{1}_E(x) = 1$ and $\mathbf{1}_p(x) = 1$ for all $p \in S$, then x is primitive and $w_{E,S}(x) = |S| - (|S|-1) = 1 = \mathbf{1}_{\mathcal{P}(n)}(x)$; if $\mathbf{1}_E(x) = 1$ and $\mathbf{1}_p(x) = 0$ for at least one $p \in S$, then $\sum_{p\in S}\mathbf{1}_{E\cup\{p\}}(x) \le |S|-1$, so $w_{E,S}(x) \le 0 = \mathbf{1}_{\mathcal{P}(n)}(x)$.

In particular, since a_0 is non-primitive, $w_{E,S}(a_0) \le \mathbf{1}_{\mathcal{P}(n)}(a_0) = 0$. Hence

$$\sum_{u\in\mathbb{F}_q^\times} w_{E,S}(a_0+u) = \left(\sum_{x\in\mathbb{F}_q} w_{E,S}(x)\right) - w_{E,S}(a_0) \ge \sum_{x\in\mathbb{F}_q} w_{E,S}(x).$$

For $S = \emptyset$ this equals $\theta(E)n = \delta n$, and for $S \neq \emptyset$ it equals

$$\sum_{p\in S} \theta(E \cup \{p\})n - (|S| - 1)\theta(E)n = \theta(E)n \left(\sum_{p\in S} \left(1 - \frac{1}{p}\right) - (|S| - 1) \right) = \theta(E)\,\Delta\, n = \delta n.$$

For the Fourier bound with $\chi \neq \chi_0$, the case $S = \emptyset$ is immediate from (a). For $S \neq \emptyset$, substituting (3) into $\mathbf{1}_{E\cup\{p\}}(x) = \mathbf{1}_p(x)\,\mathbf{1}_E(x)$ rearranges $w_{E,S}(x)$ cleanly as

$$w_{E,S}(x) = \Delta\,\mathbf{1}_E(x) - \sum_{p\in S} \frac{1}{p} \sum_{j=1}^{p-1} \chi_1^{jn/p}(x)\,\mathbf{1}_E(x).$$

Each character $\eta_{p,j} = \chi_1^{jn/p}$ ($p \in S$, $1 \le j < p$) has exact order p, which is coprime to $\prod_{r\in E} r$ because $E \cap S = \emptyset$. Applying (a) to the $\Delta\,\mathbf{1}_E$ term and to each $\eta_{p,j}\mathbf{1}_E$ term gives

$$\begin{aligned}
\left| \sum_{u\in\mathbb{F}_q^\times} w_{E,S}(a_0 + u)\,\chi(u) \right| &\le \Delta\,\theta(E)\big((2^{|E|} - 1)\sqrt{q} + 1\big) + \sum_{p\in S} \frac{p-1}{p}\,\theta(E)\,2^{|E|}\sqrt{q} \\
&= \Delta\,\theta(E)\big((2^{|E|} - 1)\sqrt{q} + 1\big) + \big((|S| - 1) + \Delta\big)\,\theta(E)\,2^{|E|}\sqrt{q} \\
&= \theta(E)\,\Delta \left[\left(2^{|E|} \left(\frac{|S| - 1}{\Delta} + 2 \right) - 1 \right) \sqrt{q} + 1 \right] = \delta L. \qquad \square
\end{aligned}$$

Lemma 3.4 (Exact Minimum Degree)**.** *If $a_0 \in \mathbb{F}_q^\times$ is non-primitive, then every vertex $x \in \mathbb{F}_q^\times$ has degree at least $\varphi(n) - 1$ in $G(\mathbb{F}_q, a_0)$.*

Proof. Fix $x \in \mathbb{F}_q^\times$. The affine map $y \mapsto xy + a_0$ is a bijection from $\mathbb{F}_q^\times$ onto $\mathbb{F}_q \setminus \{a_0\}$. Because a_0 is non-primitive, all $\varphi(n)$ primitive elements of $\mathbb{F}_q$ lie in $\mathbb{F}_q \setminus \{a_0\}$, so there are exactly $\varphi(n)$ elements $y \in \mathbb{F}_q^\times$ such that $xy + a_0$ is primitive. Excluding at most the single element $y = x$ leaves at least $\varphi(n) - 1$ neighbors of x in $G(\mathbb{F}_q, a_0)$. $\square$

Combining Theorem 2.3 with Lemmas 3.2, 3.3, and 3.4 yields our master four-inequality criterion.

Theorem 3.5 (Master Double-Squeeze Criterion)**.** *Let $\mathbb{F}_q$ be a finite field with $q > 7$, $n = q-1$, and let $a_0 \in \mathbb{F}_q^\times$ be non-primitive. If $G(\mathbb{F}_q, a_0)$ is not Hamiltonian, then there exist integers $\alpha, k, a, b \in \mathbb{N}$ satisfying*

$$1 \le a \le b, \qquad a + b + k = n, \qquad k < \alpha \le n, \qquad \varphi(n) \le a + k, \tag{6}$$

such that:

(1) *For every partition $\mathcal{P}(n) = E \sqcup S$ with $\Delta = 1 - \sum_{p\in S} \frac{1}{p} > 0$, letting δ, K, L be as in Lemma 3.3(b),*

$$\alpha(n + L) \le n(L + 1/\delta), \tag{7}$$

$$n^2 ab \le L^2(a + k)(b + k). \tag{8}$$

(2) *For every subset $E \subseteq \mathcal{P}(n)$, letting $L_E = (2^{|E|} - 1)\sqrt{q} + 1$,*

$$(\varphi(n) - 1)\,n \le \theta(E)\,(n - \alpha)(n + L_E), \tag{9}$$

$$a\,(\varphi(n) - 1)\,n \le \theta(E)\,a(a + k)\,n + \theta(E)\,L_E \sqrt{ab(a + k)(b + k)}. \tag{10}$$

Proof. Suppose $G = G(\mathbb{F}_q, a_0)$ is not Hamiltonian. Since $n = q - 1 \ge 7 \ge 3$, Theorem 2.3 gives a vertex cut $V = S_{\text{cut}} \sqcup A \sqcup B$ ($A, B \neq \emptyset$, $E(A, B) = \emptyset$) and an independent set $I \subseteq V$ with $|S_{\text{cut}}| < |I|$. Swapping A and B if necessary, assume $|A| \le |B|$. Set $\alpha := |I|$, $k := |S_{\text{cut}}|$, $a := |A|$, $b := |B|$. Clearly $1 \le a \le b$, $a + b + k = n$, and $k < \alpha \le n$. Picking any $x_0 \in A$, all neighbors of x_0 in G lie in $(A \setminus \{x_0\}) \cup S_{\text{cut}}$, so Lemma 3.4 gives $\varphi(n) - 1 \le (a - 1) + k$, i.e., $\varphi(n) \le a + k$, proving (6).

Proof of (7). Fix a partition $\mathcal{P}(n) = E \sqcup S$ with $\Delta > 0$ and set $f(u) := w_{E,S}(a_0 + u)$. By Lemma 3.3(b), $\mu = \frac{1}{n}\sum_u f(u) \geq \delta$ and $\Lambda = \delta L$ is valid for Lemma 3.2. Applying Lemma 3.2 to $X = Y = I$ gives

$$\delta\alpha^2 - \delta L\,\alpha\Big(1 - \frac{\alpha}{n}\Big) \leq \sum_{x\in I}\sum_{y\in I} f(xy).$$

Since I is independent in G, for $x \neq y \in I$ we have $f(xy) \leq \mathbf{1}_{\mathcal{P}(n)}(xy + a_0) = 0$; on the diagonal $x = y \in I$, $f(x^2) \leq \mathbf{1}_{\mathcal{P}(n)}(x^2 + a_0) \leq 1$. Thus the double sum is at most α. Dividing by $\delta > 0$ and clearing n gives $\alpha^2 n - L\alpha(n-\alpha) \leq n\alpha/\delta$; since $\alpha > k \geq 0$, dividing by α yields $\alpha(n+L) \leq n(L+1/\delta)$.

Proof of (8). Applying Lemma 3.2 to the same f on $X = A$ and $Y = B$, every pair $(x, y) \in A \times B$ has $x \neq y$ and $xy \notin E(G)$, so $f(xy) \leq \mathbf{1}_{\mathcal{P}(n)}(xy + a_0) = 0$. Hence

$$\delta ab \leq \delta L\sqrt{a\Big(1 - \frac{a}{n}\Big)\,b\Big(1 - \frac{b}{n}\Big)} = \delta L\sqrt{a\,\frac{b+k}{n}\,b\,\frac{a+k}{n}}.$$

Dividing by $\delta > 0$, squaring, multiplying by n^2, and canceling $ab > 0$ produces $n^2 ab \leq L^2(a+k)(b+k)$.

Proof of (9). Fix $E \subseteq \mathcal{P}(n)$ and set $g(u) := \mathbf{1}_E(a_0 + u)$. By Lemma 3.3(a), $\mu_g \leq \theta(E)$ and $\Lambda_g = \theta(E)\,L_E$. Since I is independent, every neighbor of every $x \in I$ lies in $V \setminus I$, so Lemma 3.4 gives

$$\alpha(\varphi(n) - 1) \leq \sum_{x\in I}\sum_{y\in V\setminus I} \mathbf{1}_{\mathcal{P}(n)}(xy + a_0) \leq \sum_{x\in I}\sum_{y\in V\setminus I} g(xy).$$

By Lemma 3.2 on $X = I$ and $Y = V \setminus I$ (noting $|V \setminus I| = n - \alpha$ and $\sqrt{\alpha(1-\alpha/n)(n-\alpha)(\alpha/n)} = \alpha(n-\alpha)/n$),

$$\alpha(\varphi(n) - 1) \leq \theta(E)\,\alpha(n-\alpha) + \theta(E)\,L_E\,\frac{\alpha(n-\alpha)}{n}.$$

Multiplying by n and dividing by $\alpha > 0$ yields (9).

Proof of (10). Every neighbor of every $x \in A$ lies in $A \cup S_{\mathrm{cut}}$ (which has cardinality $a + k = n - b$). Hence Lemma 3.4 and Lemma 3.2 on $X = A$ and $Y = A \cup S_{\mathrm{cut}}$ give

$$\begin{aligned} a(\varphi(n) - 1) &\leq \sum_{x\in A}\sum_{y\in A\cup S_{\mathrm{cut}}} g(xy) \\ &\leq \theta(E)\,a(a+k) + \theta(E)\,L_E\sqrt{a\,\frac{b+k}{n}\,(a+k)\,\frac{b}{n}}. \end{aligned}$$

Multiplying through by n gives (10). □

4. Unconditional Analytic Coverage for All $q \geq 8{,}100$

In this section we prove unconditionally that no tuple (α, k, a, b) can satisfy (6)–(8) whenever $q \geq 8{,}100$. (Remarkably, the lower-sieve inequalities (7)–(8) alone suffice for all $q \geq 8{,}100$; the upper sieves (9)–(10) are needed only in the finite range $q < 8{,}100$.)

Lemma 4.1 (Universal Constant-Bound Contradiction)**.** *Suppose* (α, k, a, b) *satisfies* (6)*, and* (7)–(8) *hold for some* $\delta > 0$*,* $K \geq 0$*, and* $L = K\sqrt{q} + 1$*. Suppose further that there exist positive real constants* $n_{\mathrm{lo}}, \theta_{\mathrm{lo}}, K_{\mathrm{hi}}, \delta_{\mathrm{lo}}, \mathrm{sq}_{\mathrm{hi}}, u_0, c_0, \alpha_0$ *satisfying*

$$\begin{gathered} n \geq n_{\mathrm{lo}}, \quad \theta_{\mathrm{lo}} \leq \tfrac{1}{2}, \quad \varphi(n) \geq \theta_{\mathrm{lo}} n, \quad K \leq K_{\mathrm{hi}}, \quad \delta \geq \delta_{\mathrm{lo}}, \quad n_{\mathrm{lo}} + 1 \leq \mathrm{sq}_{\mathrm{hi}}^2, \\ \frac{K_{\mathrm{hi}}\,\mathrm{sq}_{\mathrm{hi}} + 1}{n_{\mathrm{lo}}} \leq u_0 < 1, \quad \frac{1}{\delta_{\mathrm{lo}} n_{\mathrm{lo}}} \leq c_0 < 1, \quad \frac{u_0 + c_0}{1 + u_0} \leq \alpha_0 < \theta_{\mathrm{lo}}, \end{gathered}$$

and

$$\alpha_0 u_0^2 < (\theta_{\mathrm{lo}} - \alpha_0)(1 - \theta_{\mathrm{lo}})(1 - u_0^2). \tag{11}$$

Then a contradiction ensues.

Proof. Set $u := L/n$ and $c := 1/(\delta n)$. Since $(n_{\mathrm{lo}}+1)n^2 - (n+1)n_{\mathrm{lo}}^2 = (n-n_{\mathrm{lo}})(nn_{\mathrm{lo}}+n+n_{\mathrm{lo}}) \geq 0$, we have

$$\frac{\sqrt{q}}{n} = \frac{\sqrt{n+1}}{n} \leq \frac{\sqrt{n_{\mathrm{lo}}+1}}{n_{\mathrm{lo}}} \leq \frac{\mathrm{sq}_{\mathrm{hi}}}{n_{\mathrm{lo}}},$$

whence $u = K\frac{\sqrt{q}}{n} + \frac{1}{n} \leq \frac{K_{\mathrm{hi}}\,\mathrm{sq}_{\mathrm{hi}}+1}{n_{\mathrm{lo}}} \leq u_0 < 1$, and $c \leq \frac{1}{\delta_{\mathrm{lo}} n_{\mathrm{lo}}} \leq c_0 < 1$. From (7),

$$\frac{\alpha}{n} \leq \frac{u+c}{1+u} \leq \frac{u_0+c_0}{1+u_0} \leq \alpha_0,$$

using $(u_0+c_0)(1+u)-(u+c)(1+u_0) = (u_0-u)(1-c_0)+(c_0-c)(1+u_0) \geq 0$. Hence $k < \alpha \leq \alpha_0 n$ and $L \leq u_0 n$.

Next, from $a \leq b$, $a+b+k = n$, and $\varphi(n) \leq a+k$, we have $2\varphi(n) \leq 2(a+k) \leq a+b+2k = n+k \leq (1+\alpha_0)n$, so $\varphi(n) \leq \frac{1+\alpha_0}{2}n$. We now use two exact algebraic identities. First, substituting $n = a+b+k$,

$$ab - (\varphi(n)-k)(n-\varphi(n)) = (a+k-\varphi(n))(b+k-\varphi(n)) \geq 0.$$

Moreover, since $\theta_{\mathrm{lo}} n \leq \varphi(n) \leq \frac{1+\alpha_0}{2}n$ and $\theta_{\mathrm{lo}} \leq \frac{1}{2}$ imply $(1+\alpha_0)n - \varphi(n) - \theta_{\mathrm{lo}} n \geq (\frac{1+\alpha_0}{2} - \theta_{\mathrm{lo}})n \geq 0$,

$$(\varphi(n)-\alpha_0 n)(n-\varphi(n)) - (\theta_{\mathrm{lo}}-\alpha_0)(1-\theta_{\mathrm{lo}})n^2 = (\varphi(n)-\theta_{\mathrm{lo}}n)\big((1+\alpha_0)n - \varphi(n) - \theta_{\mathrm{lo}}n\big) \geq 0.$$

Therefore

$$ab \geq (\varphi(n)-k)(n-\varphi(n)) \geq (\varphi(n)-\alpha_0 n)(n-\varphi(n)) \geq (\theta_{\mathrm{lo}}-\alpha_0)(1-\theta_{\mathrm{lo}})n^2. \tag{12}$$

Second, $(a+k)(b+k) = ab + k(a+b+k) = ab + kn$, so (8) rearranges to

$$ab(n^2 - L^2) \leq knL^2. \tag{13}$$

Combining (12), $n^2 - L^2 \geq (1-u_0^2)n^2$, $k \leq \alpha_0 n$, and $L^2 \leq u_0^2 n^2$ in (13) gives

$$(\theta_{\mathrm{lo}}-\alpha_0)(1-\theta_{\mathrm{lo}})(1-u_0^2)n^4 \leq ab(n^2-L^2) \leq knL^2 \leq \alpha_0 u_0^2 n^4,$$

contradicting (11). □

Proposition 4.2 (All $\omega(n) \geq 8$)**.** *If $\omega(n) = |\mathcal{P}(n)| \geq 8$, then no tuple (α, k, a, b) can satisfy* (6) *together with* (7)–(8) *for the trivial partition $E = \mathcal{P}(n)$, $S = \emptyset$.*

Proof. Let $P_8 := \{2,3,5,7,11,13,17,19\}$, so $\prod_{p\in P_8} p = 9{,}699{,}690$. Put $A_0 := \mathcal{P}(n) \cap P_8$, $B_0 := \mathcal{P}(n) \setminus P_8$, and $C_0 := P_8 \setminus \mathcal{P}(n)$. Since $|\mathcal{P}(n)| \geq 8 = |P_8|$, we have $|C_0| \leq |B_0|$; furthermore, every $p \in C_0$ satisfies $2 \leq p \leq 19$, while every $p \in B_0$ satisfies $p \geq 23$. We derive three elementary prime-swap inequalities:

(i) $\prod_{p\in C_0} p \leq 19^{|C_0|} \leq 23^{|B_0|} \leq \prod_{p\in B_0} p$, so $n \geq \prod_{p\in\mathcal{P}(n)} p \geq \prod_{p\in P_8} p = 9{,}699{,}690$. In particular, $q = n+1 \leq \frac{9{,}699{,}691}{9{,}699{,}690} n$.

(ii) Writing $|B_0| = |C_0| + d$ ($d \geq 0$), since $19 < 23$ and $4 < 23$,

$$4^{|B_0|} \prod_{p\in C_0} p \leq 4^{|C_0|+d} 19^{|C_0|} \leq 4^{|C_0|} 23^{|C_0|+d} \leq 4^{|C_0|} \prod_{p\in B_0} p,$$

and multiplying by $4^{|A_0|}\prod_{p\in A_0} p$ gives $4^{\omega(n)} \cdot 9{,}699{,}690 \leq 4^8 \prod_{p\in\mathcal{P}(n)} p \leq 65{,}536\, n$.

(iii) Observe that $\frac{(p-1)^2}{4p} \leq \frac{9}{2}$ for all $2 \leq p \leq 19$ (since $(p-1)^2 \leq 18p \iff p^2 - 20p + 1 \leq 0$), whereas $\frac{(p-1)^2}{4p} \geq \frac{9}{2}$ for all $p \geq 23$ (since $p^2 - 20p + 1 > 0$). Hence

$$\prod_{p\in C_0} \frac{(p-1)^2}{4p} \leq \left(\frac{9}{2}\right)^{|C_0|} \leq \left(\frac{9}{2}\right)^{|B_0|} \leq \prod_{p\in B_0} \frac{(p-1)^2}{4p},$$

and therefore

$$\frac{\theta(\mathcal{P}(n))^2\, n}{4^{\omega(n)}} \geq \prod_{p\in\mathcal{P}(n)} \frac{(p-1)^2}{4p} \geq \prod_{p\in P_8} \frac{(p-1)^2}{4p} = \frac{1{,}399{,}680}{323{,}323} > \frac{43}{10}.$$

Let $L = (2^{\omega(n)}-1)\sqrt{q}+1 \leq 2^{\omega(n)}\sqrt{q}$ (as $\sqrt{q}\geq 1$). From (i) and (iii),

$$L^2 \leq 4^{\omega(n)} q \leq \frac{10}{43}\theta(\mathcal{P}(n))^2 n \cdot \frac{9{,}699{,}691}{9{,}699{,}690} n < \left(\frac{49}{100}\theta(\mathcal{P}(n))n\right)^2,$$

so $L \leq \frac{49}{100}\varphi(n)$. Similarly, from (i) and (ii),

$$L^2 \leq 4^{\omega(n)} q \leq \frac{65{,}536}{9{,}699{,}690} n \cdot \frac{9{,}699{,}691}{9{,}699{,}690} n < \left(\frac{1}{10}n\right)^2,$$

so $L \leq \frac{1}{10}n$. Moreover, since $2^{\omega(n)} \geq 256$, (iii) gives $\theta(\mathcal{P}(n))^2 n > \frac{43}{10}\cdot 256^2 > 100$, hence $1/\theta(\mathcal{P}(n)) \leq \frac{1}{100}\theta(\mathcal{P}(n))n = \frac{1}{100}\varphi(n)$.

From (7) with $\delta = \theta(\mathcal{P}(n))$, we deduce $\alpha \leq L + 1/\theta(\mathcal{P}(n)) \leq \frac{49}{100}\varphi(n) + \frac{1}{100}\varphi(n) = \frac{1}{2}\varphi(n)$, so $k < \frac{1}{2}\varphi(n)$. Since $2\varphi(n) \leq n + k \leq n + \frac{1}{2}\varphi(n) \leq \frac{3}{2}n$, we get $n - \varphi(n) \geq \frac{1}{4}n$, and (12) yields

$$ab \geq (\varphi(n) - k)(n - \varphi(n)) \geq \frac{1}{2}\varphi(n) \cdot \frac{1}{4}n = \frac{1}{8}\varphi(n)\, n.$$

Finally, $L \leq \frac{1}{10}n$ implies $n^2 - L^2 \geq \frac{99}{100}n^2$, so (13) forces

$$\frac{99}{800}\varphi(n)n^3 \leq ab(n^2 - L^2) \leq knL^2 \leq \frac{1}{2}\varphi(n) \cdot n \cdot \frac{1}{100}n^2 = \frac{1}{200}\varphi(n)n^3,$$

contradicting $\frac{99}{800} > \frac{4}{800} = \frac{1}{200}$. □

Theorem 4.3 (Unconditional Analytic Coverage for $q \geq 8{,}100$)**.** *For every finite field $\mathbb{F}_q$ with $q \geq 8{,}100$ and every non-primitive $a_0 \in \mathbb{F}_q^\times$, the graph $G(\mathbb{F}_q, a_0)$ is Hamiltonian.*

Proof. Let $n = q - 1 \geq 8{,}099$ and $r := \omega(n)$. If $r \geq 8$, Theorem 3.5 and Proposition 4.2 give the result immediately. Otherwise $r \in \{1, 2, 3, 4, 5, 6, 7\}$; list the primes of $\mathcal{P}(n)$ in increasing order as $p_0 < p_1 < \cdots < p_{r-1}$. Then $p_0 \geq 2, p_1 \geq 3, p_2 \geq 5, p_3 \geq 7, p_4 \geq 11, p_5 \geq 13, p_6 \geq 17$, and consequently:

- $n \geq \prod_{i=0}^{r-1} p_i$, which strengthens $n \geq 8{,}099$ to $n \geq 30{,}030$ for $r = 6$ and $n \geq 510{,}510$ for $r = 7$;
- $\theta(\mathcal{P}(n)) = \prod_{i=0}^{r-1}(1 - 1/p_i) \geq \prod_{i=0}^{r-1}(1 - 1/q_i)$ where $q_0, q_1, \ldots$ are the consecutive primes $2, 3, 5, 7, 11, 13, 17$.

For $r \in \{1, 2, 3, 7\}$ we apply the unsieved partition $E = \mathcal{P}(n)$, $S = \emptyset$ ($s = 0$), where $\delta = \theta(\mathcal{P}(n))$ and $K = 2^r - 1$. For $r \in \{4, 5, 6\}$ we apply the Cohen–Huczynska–Trudgian sieve with $E = \{p_0, p_1\}$ and $S = \{p_2, \ldots, p_{r-1}\}$ ($s = r - 2$), noting that $\theta(E) \geq (1 - \frac{1}{2})(1 - \frac{1}{3}) = \frac{1}{3}$ and $\Delta = 1 - \sum_{i=2}^{r-1} \frac{1}{p_i} \geq 1 - \sum_{i=2}^{r-1} \frac{1}{q_i} =: \Delta_{\mathrm{lo}}$, whence $\delta \geq \frac{1}{3}\Delta_{\mathrm{lo}}$ and $K \leq 4\big(\frac{s-1}{\Delta_{\mathrm{lo}}} + 2\big) - 1 =: K_{\mathrm{hi}}$.

Every hypothesis of Lemma 4.1 holds with the exact rational parameters recorded in Table 1; each line is a finite rational inequality (verified explicitly in Lean by `norm_num`). Applying Theorem 3.5 completes the proof. □

5. Certified Integer Double-Squeeze for $7 < q < 8{,}100$

For a specific prime power $7 < q < 8{,}100$, using the actual prime factorization of $n = q - 1$ together with *both* lower sieves (7)–(8) and upper sieves (9)–(10) is dramatically stronger than the worst-case bounds of Section 4. To make the elimination of $7 < q < 8{,}100$ completely rigorous and directly verifiable inside Lean's kernel without floating-point arithmetic, we formulate all four tests in exact natural-number arithmetic.

TABLE 1. Exact verified rational parameters for Lemma 4.1 in Theorem 4.3 ($q \geq 8{,}100$, $r = \omega(q-1) \in \{1, \ldots, 7\}$). Here $s = |S|$, $\delta_{\mathrm{lo}} = \theta_{\mathrm{lo}}$ for $s = 0$ and $\delta_{\mathrm{lo}} = \Delta_{\mathrm{lo}}/3$ for $s > 0$, LHS $= \alpha_0 u_0^2$, and RHS $= (\theta_{\mathrm{lo}} - \alpha_0)(1 - \theta_{\mathrm{lo}})(1 - u_0^2)$.

r	s	n_{lo}	θ_{lo}	Δ_{lo}	K_{hi}	$\mathrm{sq}_{\mathrm{hi}}$	u_0	c_0	α_0	LHS < RHS
1	0	8,099	1/2	—	1	90	1/50	1/1000	1/40	$0.000010 < 0.237405$
2	0	8,099	1/3	—	3	90	1/20	1/1000	1/20	$0.000125 < 0.188417$
3	0	8,099	4/15	—	7	90	1/10	1/1000	1/10	$0.001000 < 0.121000$
4	2	8,099	8/35	23/35	301/23	90	15/100	1/1500	14/100	$0.003150 < 0.066789$
5	3	8,099	16/77	218/385	4606/218	90	235/1000	1/1500	191/1000	$0.010548 < 0.012568$
6	4	30,030	192/1001	2449/5005	77203/2449	174	19/100	1/4000	16/100	$0.005776 < 0.024779$
7	0	510,510	3072/17017	—	127	715	18/100	1/90000	153/1000	$0.004957 < 0.021826$

Given a candidate prime power $q \in [8, 8099]$ and $n = q - 1$:

(1) *Exact factorization and $\sqrt{q}$ ceiling.* Sort the distinct prime divisors of n as $p_0 < p_1 < \cdots < p_{r-1}$ (checked for primality, strict ordering, and complete exhaustion of n), compute $\varphi(n) = n \prod_i (p_i - 1)/p_i$, and set

$$\mathrm{sq}_{16} := \lfloor \sqrt{256q - 1} \rfloor + 1, \qquad \text{so that } \sqrt{q} \leq \frac{\mathrm{sq}_{16}}{16}.$$

(2) *Lower-sieve optimization over $s \in \{0, \ldots, r\}$.* For each s, let $E = \{p_0, \ldots, p_{r-s-1}\}$ and $S = \{p_{r-s}, \ldots, p_{r-1}\}$. In exact rational form $\Delta = D_{\mathrm{num}}/P_S$ (requiring $D_{\mathrm{num}} > 0$), $\theta(E) = \Phi_E/P_E$, and $L \leq L_n/L_d$ (reduced by gcd, using $\sqrt{q} \leq \mathrm{sq}_{16}/16$). Adding $\alpha(L_n/L_d - L) \leq n(L_n/L_d - L)$ (from $\alpha \leq n$ and $L_n/L_d \geq L$) to (7) gives $\alpha(n + L_n/L_d) \leq n(L_n/L_d + 1/\delta)$, which implies

$$\alpha \leq \left\lfloor \frac{nL_n\Phi_E D_{\mathrm{num}} + nL_d P_E P_S}{(nL_d + L_n)\Phi_E D_{\mathrm{num}}} \right\rfloor.$$

We retain the smallest upper bound α_{low} on α and the smallest reduced fraction L_n/L_d over all valid s.

(3) *Upper-sieve sharpening of α.* For each prefix $E_t = \{p_0, \ldots, p_{t-1}\}$ $(1 \leq t \leq r)$, writing $L_{E_t} \leq L_{e,\mathrm{num}}/16$ with $L_{e,\mathrm{num}} = (2^t - 1)\mathrm{sq}_{16} + 16$, inequality (9) gives

$$n - \alpha \geq \left\lceil \frac{(\varphi(n) - 1)\, P_{E_t}\, n \cdot 16}{\Phi_{E_t}\,(16n + L_{e,\mathrm{num}})} \right\rceil,$$

yielding an upper bound $\alpha \leq \alpha_{\mathrm{up}}(t)$. Setting $\mathrm{bestA} := \min(\alpha_{\mathrm{low}}, \min_{1 \leq t \leq r} \alpha_{\mathrm{up}}(t))$, we have $k \leq k_{\max} := \mathrm{bestA} - 1$ (and if $\mathrm{bestA} = 0$, $k < \alpha \leq 0$ is immediately impossible).

(4) *Dirac cut and double-squeeze over a.* From (6), $a \leq b$ and $a + b + k = n$ force $a \leq \lfloor n/2 \rfloor$ and $a \geq a_{\mathrm{lo}} := \max(1, \varphi(n) - k_{\max})$. If $2\varphi(n) > n + k_{\max}$ or $a_{\mathrm{lo}} > \lfloor n/2 \rfloor$, no admissible (a, b, k) exists. Otherwise, we split the integer interval $[a_{\mathrm{lo}}, \lfloor n/2 \rfloor]$ into two regimes:

- *Large a (lower-sieve cut (8)):* Suppose $L_n < nL_d$ and for some threshold $a_{\mathrm{cut}} \in [a_{\mathrm{lo}}, \lfloor (n - k_{\max})/2 \rfloor]$ we have

$$L_n^2 (a_{\mathrm{cut}} + k_{\max})(n - a_{\mathrm{cut}}) < n^2 L_d^2\, a_{\mathrm{cut}}(n - k_{\max} - a_{\mathrm{cut}}). \tag{14}$$

  By the identity $(a_{\mathrm{cut}} + k_{\max})(n - a_{\mathrm{cut}}) = a_{\mathrm{cut}}(n - k_{\max} - a_{\mathrm{cut}}) + k_{\max} n$, inequality (14) rearranges to $(n^2 L_d^2 - L_n^2)\, a_{\mathrm{cut}}(n - k_{\max} - a_{\mathrm{cut}}) > L_n^2 k_{\max} n$. For any admissible (a, b, k) with $a \geq a_{\mathrm{cut}}$, since $n^2 L_d^2 - L_n^2 > 0$ and $ab = a_{\mathrm{cut}}(n - k - a_{\mathrm{cut}}) + (a - a_{\mathrm{cut}})(b - a_{\mathrm{cut}}) \geq a_{\mathrm{cut}}(n - k_{\max} - a_{\mathrm{cut}})$, this contradicts (13) (with $L \leq L_n/L_d$ and $k \leq k_{\max}$). Thus every $a \geq a_{\mathrm{cut}}$ is eliminated at once.
- *Small a (upper-sieve cut (10)):* For each remaining integer $a \in [a_{\mathrm{lo}}, a_{\mathrm{cut}} - 1]$ (or all $a \in [a_{\mathrm{lo}}, \lfloor n/2 \rfloor]$ if no a_{cut} satisfies (14)), write $M := a + k_{\max} \geq a + k$, and observe

$b = n - (a + k) \le n - \varphi(n)$ and $b + k = n - a$. For any prefix $E_t = \{p_0, \dots, p_{t-1}\}$, set $\mathrm{lhs}_0 := nP_{E_t}(\varphi(n) - 1)$ and $\mathrm{rhs}_0 := n\Phi_{E_t}M$. Whenever $\mathrm{lhs}_0 > \mathrm{rhs}_0$ and

$$\big(16(\mathrm{lhs}_0 - \mathrm{rhs}_0)\big)^2 a > (\Phi_{E_t} L_{e,\mathrm{num}})^2 (n - \varphi(n))\, M\, (n - a), \tag{15}$$

squaring (10) yields a strict contradiction, eliminating that value of a.

The soundness of every step above is proved unconditionally in Lean (`checkAnalyticQ_sound` and `checkAllBelow8100_sound`), and executing the boolean decision procedure over all integers $8 \le q \le 8{,}099$ (skipping non-prime-powers by certifying a prime divisor $d \mid q$ such that stripping all powers of d leaves a cofactor $\neq 1$) yields:

Proposition 5.1 (Certified Range Reduction below 8,100)**.** *For every prime power $7 < q < 8{,}100$ not appearing in the 44-element set*

$$\begin{aligned}\mathcal{E}_{44} := \big\{&9, 11, 13, 16, 19, 23, 25, 27, 29, 31, 37, 41, 43, 49, 61, 67, 71, 79, 103, 121, 127, 151,\\ &169, 181, 211, 241, 271, 331, 361, 421, 463, 547, 571, 631, 661, 841, 991, 1051, 1471,\\ &1681, 2311, 2731, 3571, 4621\big\}\end{aligned}$$

and every non-primitive $a_0 \in \mathbb{F}_q^\times$, the graph $G(\mathbb{F}_q, a_0)$ is Hamiltonian.

Notice the striking arithmetic structure of $\mathcal{E}_{44}$: its largest element is $q = 4{,}621$ (where $q - 1 = 4{,}620 = 2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$ has $\omega(n) = 5$ and minimal $\theta(\mathcal{P}(n)) = 16/77$), and every $q \in \mathcal{E}_{44}$ is either a prime (34 cases: 10 with $p \equiv 1 \pmod 4$ and 24 with $p \equiv 3 \pmod 4$), a prime square p^2 (8 cases, all $\equiv 1 \pmod 4$: $p \in \{3, 5, 7, 11, 13, 19, 29, 41\}$), or one of the two higher prime powers $q = 16 = 2^4$ and $q = 27 = 3^3$.

6. Explicit Constructions for the 44 Exceptional Finite Fields

To finish the proof of Theorem 1.1, we construct explicit Hamiltonian cycles in $G(\mathbb{F}_q, -1)$ and $G(\mathbb{F}_q, +1)$ for every $q \in \mathcal{E}_{44}$. Since any two finite fields of the same cardinality are isomorphic, it suffices to exhibit cycles in a concrete model of $\mathbb{F}_q$ (or directly in an arbitrary finite field of cardinality q).

6.1. Algebraic constructions for $\mathbb{F}_{16}$ and $\mathbb{F}_{27}$.

For $q = 16$ and $q = 27$, we give completely self-contained, isomorphism-free constructions working directly in any finite field F of cardinality 16 or 27.

Proposition 6.1 ($\mathbb{F}_{16}$)**.** *Theorem 1.1(1) and (2) hold for any finite field F of cardinality* 16*.*

Proof. Since $|F| = 16 = 2^4$, $\mathrm{char}\, F = 2$ (so $-1 = +1$ and (1) $\iff$ (2)). Let g_0 be any generator of $F^\times$, so $g_0^{15} = 1$. Over $\mathbb{F}_2$,

$$x^{15} + 1 = (x^4 + x + 1)(x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1)(x^2 + x + 1)(x + 1).$$

Since $\mathrm{ord}(g_0) = 15$, g_0 cannot be a root of $x+1$, x^2+x+1, or $x^4+x^3+x^2+x+1$ (which divide $x-1$, $x^3 - 1$, $x^5 - 1$). Thus either $g := g_0$ or $g := g_0^{-1}$ is a primitive element of F satisfying $g^4 = g + 1$. From $g^4 = g + 1$, $g^{15} = 1$, and $2 = 0$, we obtain the Zech-logarithm table

k	1	2	3	4	6	8	9	12
$z(k)$ with $g^k + 1 = g^{z(k)}$	4	8	14	1	13	2	7	11

Every exponent $z(k)$ in the bottom row is coprime to 15, so $g^k + 1$ is primitive for each listed k. Define $a(i) := g^{e_i}$ using the permutation

$$(e_0, \dots, e_{14}) = (0, 1, 2, 4, 5, 3, 6, 10, 7, 9, 14, 13, 8, 11, 12)$$

of $\mathbb{Z}/15\mathbb{Z}$. The cyclic adjacent sums $(e_i + e_{i+1}) \bmod 15$ are

$$(1, 3, 6, 9, 8, 9, 1, 2, 1, 8, 12, 6, 4, 8, 12),$$

every one of which lies in $\{1, 2, 3, 4, 6, 8, 9, 12\}$. Hence $a(i)a(i+1) \pm 1 = g^{(e_i+e_{i+1}) \bmod 15} + 1$ is primitive for all $i \in \mathbb{Z}/15\mathbb{Z}$. □

Proposition 6.2 ($\mathbb{F}_{27}$)**.** *Theorem 1.1(1) and (2) hold for any finite field F of cardinality 27.*

Proof. Here $\operatorname{char} F = 3$ and $|F^\times| = 26$. Let g_0 be any generator of $F^\times$, so $g_0^{13} = -1$ and $g_0 + 1 \neq 0$. Over $\mathbb{F}_3$, $x^{13} + 1$ factors completely into $(x + 1)$ and the four primitive cubics:

$$x^{13} + 1 = (x + 1)(x^3 - x + 1)(x^3 - x^2 + x + 1)(x^3 + x^2 - x + 1)(x^3 - x^2 + 1).$$

Direct polynomial division modulo 3 shows that taking $g = g_0$, g_0^7, g_0^5, or $g_0^{-1} = g_0^{25}$ according to which of the four cubics vanishes at g_0 yields a primitive element $g \in F^\times$ satisfying $g^3 - g + 1 = 0$ and $g^{13} = -1$. From these relations we compute the Zech logarithms for $g^k - 1 = g^{z_-(k)}$ and $g^k + 1 = g^{z_+(k)}$:

k	1	3	4	8	9	10	12	20	23	24	25
$z_-(k)$	3	9	7	25	1	11	21	17	19	23	15
k	1	2	3	5	6	9	15	18	19	20	24
$z_+(k)$	9	21	1	17	11	3	25	7	23	5	19

Every entry $z_\pm(k)$ is odd and not divisible by 13, hence coprime to 26. For $a_0 = -1$, define $a(i) := g^{e_i^-}$ with

$$e^- = (0, 4, 23, 6, 2, 25, 10, 13, 17, 21, 8, 12, 15, 19, 5, 18, 7, 20, 3, 9, 1, 11, 16, 14, 22, 24);$$

the cyclic adjacent sums $(e_i^- + e_{i+1}^-) \bmod 26$ are

$$(4, 1, 3, 8, 1, 9, 23, 4, 12, 3, 20, 1, 8, 24, 23, 25, 1, 23, 12, 10, 12, 1, 4, 10, 20, 24),$$

all in the domain of z_-. For $a_0 = +1$, define $b(i) := g^{e_i^+}$ with

$$e^+ = (0, 1, 2, 3, 17, 18, 6, 14, 4, 5, 15, 13, 16, 12, 19, 22, 23, 9, 10, 25, 7, 8, 11, 20, 21, 24);$$

the cyclic adjacent sums $(e_i^+ + e_{i+1}^+) \bmod 26$ are

$$(1, 3, 5, 20, 9, 24, 20, 18, 9, 20, 2, 3, 2, 5, 15, 19, 6, 19, 9, 6, 15, 19, 5, 15, 19, 24),$$

all in the domain of z_+. Hence both permutations have all adjacent products ∓ 1 primitive. □

6.2. **Prime fields (34 cases) and quadratic extensions (8 cases).** For each of the 34 prime exceptions $p \in \mathcal{E}_{44}$, we represent $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$; for each of the 8 prime-square exceptions $q = p^2 \in \mathcal{E}_{44}$, we represent $\mathbb{F}_{p^2}$ as the quadratic extension $\mathbb{F}_p[x]/(x^2 - d)$ using a verified non-square $d \in \mathbb{F}_p^\times$, encoding $u + v\sqrt{d}$ $(0 \leq u, v < p)$ as the single integer $u + pv \in \{0, \ldots, p^2 - 1\}$.

In each case, we supply:

(1) A verified generator $g \in \mathbb{F}_q^\times$ (checked via $g^{q-1} = 1$ and $g^{(q-1)/r} \neq 1$ for every prime $r \mid (q - 1)$), from which the complete primitive-element bitmask is generated by iterating g^t over all $1 \leq t \leq q - 1$ coprime to $q - 1$.

(2) An explicit Hamiltonian cycle $(v_0, v_1, \ldots, v_{q-2})$ in $G(\mathbb{F}_q, a_0)$ (packed 24 entries per base-q natural number for compact storage), verified in a single linear pass checking that: (i) the cycle has length $q - 1$, (ii) the visited-vertex bitmask equals $2^q - 2$ (covering $\{1, \ldots, q - 1\}$ bijectively), and (iii) $v_i v_{i+1} + a_0$ (indices modulo $q - 1$) lies in the primitive-element bitmask for every $0 \leq i < q - 1$.

By Lemma 2.1(a), the 10 primes $p \equiv 1 \pmod 4$ and all 8 prime squares $p^2 \equiv 1 \pmod 4$ reuse their $a_0 = -1$ cycle directly to prove $a_0 = +1$. The 24 primes with $p \equiv 3 \pmod 4$ receive dedicated verified cycles for both $a_0 = -1$ and $a_0 = +1$. Table 2 lists all 44 exceptional fields, their algebraic models, verified generators, prime factorizations of $q - 1$, and construction methods for both conjectures.

Table 2: Complete census of the 44 exceptional prime powers $q \in \mathcal{E}_{44}$ ($7 < q < 8{,}100$, $\max q = 4{,}621$). For prime squares $q = p^2$, the generator code $u + pv$ represents $u + v\sqrt{d} \in \mathbb{F}_p[x]/(x^2 - d)$.

q	Field model	q mod 4	g	$\mathcal{P}(q-1)$	$a_0 = -1$	$a_0 = +1$
9	$\mathbb{F}_3[\sqrt{2}]$	1	$1+\sqrt{2}$ (code 4)	$\{2\}$	Cycle	Lemma 2.1(a)
11	$\mathbb{F}_{11}$	3	2	$\{2,5\}$	Cycle	Dedicated cycle
13	$\mathbb{F}_{13}$	1	2	$\{2,3\}$	Cycle	Lemma 2.1(a)
16	$\mathbb{F}_2[x]/(x^4+x+1)$	0	x	$\{3,5\}$	Prop. 6.1	Lemma 2.1(b)
19	$\mathbb{F}_{19}$	3	2	$\{2,3\}$	Cycle	Dedicated cycle
23	$\mathbb{F}_{23}$	3	5	$\{2,11\}$	Cycle	Dedicated cycle
25	$\mathbb{F}_5[\sqrt{2}]$	1	$2+\sqrt{2}$ (code 7)	$\{2,3\}$	Cycle	Lemma 2.1(a)
27	$\mathbb{F}_3[x]/(x^3-x+1)$	3	x	$\{2,13\}$	Prop. 6.2	Prop. 6.2
29	$\mathbb{F}_{29}$	1	2	$\{2,7\}$	Cycle	Lemma 2.1(a)
31	$\mathbb{F}_{31}$	3	3	$\{2,3,5\}$	Cycle	Dedicated cycle
37	$\mathbb{F}_{37}$	1	2	$\{2,3\}$	Cycle	Lemma 2.1(a)
41	$\mathbb{F}_{41}$	1	6	$\{2,5\}$	Cycle	Lemma 2.1(a)
43	$\mathbb{F}_{43}$	3	3	$\{2,3,7\}$	Cycle	Dedicated cycle
49	$\mathbb{F}_7[\sqrt{3}]$	1	$1+\sqrt{3}$ (code 8)	$\{2,3\}$	Cycle	Lemma 2.1(a)
61	$\mathbb{F}_{61}$	1	2	$\{2,3,5\}$	Cycle	Lemma 2.1(a)
67	$\mathbb{F}_{67}$	3	2	$\{2,3,11\}$	Cycle	Dedicated cycle
71	$\mathbb{F}_{71}$	3	7	$\{2,5,7\}$	Cycle	Dedicated cycle
79	$\mathbb{F}_{79}$	3	3	$\{2,3,13\}$	Cycle	Dedicated cycle
103	$\mathbb{F}_{103}$	3	5	$\{2,3,17\}$	Cycle	Dedicated cycle
121	$\mathbb{F}_{11}[\sqrt{2}]$	1	$2+\sqrt{2}$ (code 13)	$\{2,3,5\}$	Cycle	Lemma 2.1(a)
127	$\mathbb{F}_{127}$	3	3	$\{2,3,7\}$	Cycle	Dedicated cycle
151	$\mathbb{F}_{151}$	3	6	$\{2,3,5\}$	Cycle	Dedicated cycle
169	$\mathbb{F}_{13}[\sqrt{2}]$	1	$2+\sqrt{2}$ (code 15)	$\{2,3,7\}$	Cycle	Lemma 2.1(a)
181	$\mathbb{F}_{181}$	1	2	$\{2,3,5\}$	Cycle	Lemma 2.1(a)
211	$\mathbb{F}_{211}$	3	2	$\{2,3,5,7\}$	Cycle	Dedicated cycle
241	$\mathbb{F}_{241}$	1	7	$\{2,3,5\}$	Cycle	Lemma 2.1(a)
271	$\mathbb{F}_{271}$	3	6	$\{2,3,5\}$	Cycle	Dedicated cycle
331	$\mathbb{F}_{331}$	3	3	$\{2,3,5,11\}$	Cycle	Dedicated cycle
361	$\mathbb{F}_{19}[\sqrt{2}]$	1	$2+\sqrt{2}$ (code 21)	$\{2,3,5\}$	Cycle	Lemma 2.1(a)
421	$\mathbb{F}_{421}$	1	2	$\{2,3,5,7\}$	Cycle	Lemma 2.1(a)
463	$\mathbb{F}_{463}$	3	3	$\{2,3,7,11\}$	Cycle	Dedicated cycle
547	$\mathbb{F}_{547}$	3	2	$\{2,3,7,13\}$	Cycle	Dedicated cycle
571	$\mathbb{F}_{571}$	3	3	$\{2,3,5,19\}$	Cycle	Dedicated cycle
631	$\mathbb{F}_{631}$	3	3	$\{2,3,5,7\}$	Cycle	Dedicated cycle
661	$\mathbb{F}_{661}$	1	2	$\{2,3,5,11\}$	Cycle	Lemma 2.1(a)
841	$\mathbb{F}_{29}[\sqrt{2}]$	1	$4+\sqrt{2}$ (code 33)	$\{2,3,5,7\}$	Cycle	Lemma 2.1(a)
991	$\mathbb{F}_{991}$	3	6	$\{2,3,5,11\}$	Cycle	Dedicated cycle
1051	$\mathbb{F}_{1051}$	3	7	$\{2,3,5,7\}$	Cycle	Dedicated cycle
1471	$\mathbb{F}_{1471}$	3	6	$\{2,3,5,7\}$	Cycle	Dedicated cycle
1681	$\mathbb{F}_{41}[\sqrt{3}]$	1	$4+\sqrt{3}$ (code 45)	$\{2,3,5,7\}$	Cycle	Lemma 2.1(a)
2311	$\mathbb{F}_{2311}$	3	3	$\{2,3,5,7,11\}$	Cycle	Dedicated cycle
2731	$\mathbb{F}_{2731}$	3	3	$\{2,3,5,7,13\}$	Cycle	Dedicated cycle

q	Field model	$q \bmod 4$	g	$\mathcal{P}(q-1)$	$a_0 = -1$	$a_0 = +1$
3571	$\mathbb{F}_{3571}$	3	2	$\{2, 3, 5, 7, 17\}$	Cycle	Dedicated cycle
4621	$\mathbb{F}_{4621}$	1	2	$\{2, 3, 5, 7, 11\}$	Cycle	Lemma 2.1(a)

Proof of Theorem 1.1. Let $\mathbb{F}_q$ be any finite field with $q > 7$. Since $q > 7$, neither -1 nor $+1$ is primitive in $\mathbb{F}_q$ (as $(-1)^2 = 1$ and $1^1 = 1$, whereas $q - 1 \geq 7 > 2$).

- If $q \geq 8{,}100$, Theorem 4.3 gives Hamiltonian cycles in both $G(\mathbb{F}_q, -1)$ and $G(\mathbb{F}_q, +1)$.
- If $7 < q < 8{,}100$ and $q \notin \mathcal{E}_{44}$, Proposition 5.1 gives Hamiltonian cycles in both $G(\mathbb{F}_q, -1)$ and $G(\mathbb{F}_q, +1)$.
- If $q \in \mathcal{E}_{44}$, Propositions 6.1 and 6.2, Section 6.2, Table 2, and Lemma 2.1 establish both parts of Theorem 1.1. □

7. Formal Verification in Lean 4

Both parts of Theorem 1.1 have been completely formalized and machine-checked in Lean 4.33.1 with Mathlib, matching the exact public problem statements `OeisA229232.conjecture_4` ($a_0 = -1$) and `OeisA229232.conjecture_5` ($a_0 = +1$) in `FormalConjectures.OEIS.«229232»` (`formal-conjectures` commit `9097e2f90e66`).

7.1. Repository and verification artifacts.

The two standalone proof files are publicly archived in `saientropy/open-math-agents`:

- `proofs/OeisA229232.conjecture_4.lean` (commit `e6e59ccc`, 6,935 lines, 456.7 KiB): proves `theorem OMA.solution : type_of% @OeisA229232.conjecture_4`.
- `proofs/OeisA229232.conjecture_5.lean` (commit `64c0bd65`, 6,951 lines, 457.7 KiB): proves `theorem OMA.solution : type_of% @OeisA229232.conjecture_5`.

Both files pass strict automated auditing (`tools/lint.py` and `tools/check.sh`): zero warnings, zero `sorry`, zero `native_decide`, no custom axioms, and `#print axioms OMA.solution` reports strictly the three standard Lean/Mathlib axioms:

```
[propext, Classical.choice, Quot.sound].
```

Every computational certificate—the range sweep `below8100_ok` ($8 \leq q \leq 8{,}099$) and all 42 packed cycle checks `check_9` through `check_4621`—is evaluated inside Lean's trusted kernel via `decide +kernel` (so no unverified compiler or external oracle is trusted).

7.2. Architecture of the Lean formalization.

Each standalone proof file is organized into four self-contained layers inside `namespace Solver3`:

(1) *Graph Theory (lines* 28–1704*,* 1,677 *lines):* Formalization of simple paths, cycles, reachability avoiding a separator, Göring's edge-deletion induction for Vertex-Menger's theorem (`Solver3.menger`), and the Chvátal–Erdős vertex-cut theorem (`Solver3.chvatal_erdos`).

(2) *Character Theory, Sieves, and* $q \geq 8{,}100$ *(lines* 1706–4166*,* 2,461 *lines):* Twisted Jacobi-sum bounds (`norm_twisted_sum_eq_jacobi`, `norm_jacobiSum_one_nontrivial`, `norm_jacobiSum_le_sqrt`), variance-sharpened Expander Mixing (`expander_mixing`), E-free and Cohen–Huczynska–Trudgian sieve Fourier bounds (`ctSieve_fourier_bounds`, `indE_fourier_bounds`), minimum degree (`degree_ge_totient_sub_one`), master analytic criterion (`exists_circ_perm_of_analytic`), and unconditional coverage for $q \geq 8{,}100$ (`ce_of_const_bounds`, `omega_ge_eight_contradiction`, `analytic_ge_8100`).

(3) *Certified Integer Double-Squeeze for* $7 < q < 8{,}100$ *(lines* 4168–5195*,* 1,028 *lines):* Prime-factorization validator, integer lower/upper sieve checkers, soundness theorems (`lowerSieveParams_sound`, `upperAlphaUb_sound`, `upperKillsA_sound`, `lowerCutHolds_contradiction`, `checkAnalyticQ_sound`, `checkAllBelow8100_sound`), and the kernel certificate `below8100_ok`.

(4) *Exception Verifiers, Packed Cycles, and Main Theorem (lines* 5197–6935 *in* `conjecture_4.lean`*; lines* 5197–6951 *in* `conjecture_5.lean`*):* Ring-equivalence transport (`exists_circ_perm_of_ringEquiv`), sign transport (`exists_plus_one_of_minus_one_mod4`, `exists_plus_one_of_minus_one_even`), algebraic $\mathbb{F}_{16}$ and $\mathbb{F}_{27}$ proofs (`exists_circ_perm_gf16`, `exists_circ_perm_gf27_minus`, `exists_circ_perm_gf27_plus`), prime and quadratic-extension cycle verifiers (`exists_circ_perm_zmod_of` `exists_circ_perm_quad_of_checkCycleQuad`), the 42 packed cycles with `decide +kernel` proofs, the 44-branch dispatcher (`exists_circ_perm_of_mem_except44`), and `OMA.solution`.

Use of AI and formal verification

Under the direction of Sai Smaran S B, AI agents (Antigravity using Gemini and Claude models) were used for proof discovery, for writing the Lean formalizations, and for drafting this manuscript. An AI assistant also helped edit the exposition and prepare this version. The Lean artifacts establish the two stated main theorems; kernel verification of those files does not by itself verify the prose, the references, or claims about the history of the problem. The proof sources are available at `https://github.com/saientropy/open-math-agents` at the revisions identified above.

Acknowledgments

The formalization and computational verification were carried out using Lean 4.33.1, Mathlib, and the `formal-conjectures` benchmark suite.

References

[1] V. Chvátal and P. Erdős, *A note on Hamiltonian circuits*, Discrete Math. **2** (1972), 111–113.
[2] S. D. Cohen and S. Huczynska, *The primitive normal basis theorem—without a computer*, J. London Math. Soc. (2) **67** (2003), 41–56.
[3] S. D. Cohen and S. Huczynska, *The strong primitive normal basis theorem*, Acta Arith. **143** (2010), 299–332.
[4] S. D. Cohen, T. Oliveira e Silva, and T. Trudgian, *A proof of the conjecture of Cohen and Mullen on sums of primitive roots*, Math. Comp. **84** (2015), 2979–2986.
[5] F. Göring, *Short proof of Menger's theorem*, Discrete Math. **219** (2000), 295–296.
[6] R. Lidl and H. Niederreiter, *Finite Fields*, 2nd ed., Encyclopedia of Mathematics and its Applications, vol. 20, Cambridge University Press, Cambridge, 1997.
[7] X.-Q. Luo and Y.-F. She, *A Conjecture on Circular Permutations over Finite Fields*, preprint, `arXiv:2610.06289` [math.CO] (2026).
[8] OEIS Foundation Inc., *The On-Line Encyclopedia of Integer Sequences*, Sequence A229232, `https://oeis.org/A229232`.
[9] Z.-W. Sun, preprint version 5, Conjecture 3.9, `https://arxiv.org/abs/1309.1679v5` (2013).
[10] Z.-W. Sun, *Some new problems in additive combinatorics*, preprint, `arXiv:1309.1679` [math.NT] (2013); published in Nanjing Univ. J. Math. Biquarterly **36** (2019), 134–155.

Duke University
Email address: `sai.smaran@duke.edu`