Sparse Integer Turnpike Beyond Fourier Positivity

Primitive Exponential-Degree Obstructions and Arithmetic Barriers

Marian Opial
Independent researcher
opialm@gmail.com

8 September 2026

Preliminary manuscript. All displayed theorems below are proved in the text and checked where indicated by exact, dependency-free programs. Priority and novelty claims remain subject to a comprehensive literature review. In particular, this paper does not prove NP-hardness, $P = NP$, or $P \neq NP$.

AI-assistance disclosure. Artificial-intelligence tools assisted with mathematical exploration, drafting, exact verification code, and typesetting. The named author reviewed the manuscript and accepts responsibility for its content and for the claims submitted for public archiving.

Abstract

For a finite set $S \subset \mathbb{Z}$, its integer Turnpike data record the multiplicity of every positive difference. In the dense frequency-vector encoding, realizability reduces to parity of self-reciprocal irreducible factors and is therefore decidable in polynomial time by ordinary polynomial factorization. Sparse binary-exponent encoding is different: the associated reciprocal polynomial can have exponentially large degree.

We construct an infinite family of sparse, coefficientwise nonnegative, Fourier-nonnegative, arithmetically admissible Turnpike instances with the fixed point count $n = 107{,}520$ that are nevertheless nonrealizable. Each instance contains, to odd multiplicity, a primitive noncyclotomic self-reciprocal irreducible of degree 2^k, while the sparse input length is $\Theta(k)$. Thus Fourier positivity, elementary count identities, and visible monomial-composition tests do not imply any polynomial bound on the degree of the remaining obstruction.

Several complementary results locate the residual difficulty. Under the Turnpike scalar identities, an integral Hermitian sum of squares collapses to one binary rank-one factor; a parity-safe multiplier cannot raise the square-root-total/center ratio; and a strictly Fourier-positive integer NO instance can lie in the midpoint of two YES instances. Every odd self-reciprocal factor has infinitely many reciprocal quadratic shadows modulo primes, with a density lower bound in terms of permutation rank, but cyclotomic examples rule out naive small-prime enumeration. Finally, a ramified quadratic trace gadget converts a Legendre symbol into the desired characteristic-zero reciprocal-parity bit while preserving Fourier positivity. A local-to-global counterexample shows why this gadget does not yet yield a hardness reduction.

1 Introduction

Let $S = \{s_1, \dots, s_n\} \subset \mathbb{Z}$. The integer Turnpike problem asks whether prescribed multiplicities

$$\lambda_d = \#\{\{i, j\} : i < j,\ |s_i - s_j| = d\}$$

come from such a set. It is a one-dimensional phase-retrieval problem and is closely connected with homometric sets and polynomial spectral factorization; see, for example, [6, 8, 1].

The encoding is decisive. A full vector $(\lambda_1, \dots, \lambda_D)$, including its zero entries, has length at least D. A sparse list of its nonzero entries stores the same distance D in only $O(\log D)$ bits. The first problem admits a direct polynomial-time factorization algorithm. The second can compactly encode reciprocal polynomials of exponentially large degree, and no conclusion for it follows from the dense algorithm.

The main result of this paper is a resistant NO family for the sparse encoding. The family is not a hardness reduction. Its role is sharper: it falsifies a natural structural escape route in which elementary Turnpike checks, Fourier nonnegativity, and composition stripping would force every remaining odd self-reciprocal factor to have polynomially bounded degree.

For clarity, the contributions have different novelty status.

Result	Role and status
Factor-parity criterion and dense polynomial-time algorithm	Standard algebra specialized to the line problem; included for a self-contained foundation.
Fourier-positive fixed-n family with primitive degree-2^k odd factors	Main candidate contribution.
Integral Hermitian-SOS collapse, neutral-multiplier bound, and convex midpoint counterexample	Elementary structural results; potentially useful beyond the construction.
Quadratic modular shadows and the permutation-rank density bound	Chebotarev consequence with a quantitative group-action formulation.
Ramified Legendre-to-parity lift	Candidate reduction component; explicitly incomplete globally.

2 Autocorrelation and the exact factor-parity criterion

Normalize a nonempty set so that $\min S = 0$ and $\max S = D$, and put

$$P_S(x) = \sum_{s \in S} x^s, \qquad P_S^*(x) = x^D P_S(x^{-1}).$$

The autocorrelation polynomial determined by the frequency data is

$$Q(x) = nx^D + \sum_{d=1}^{D} \lambda_d \big(x^{D-d} + x^{D+d}\big). \tag{1}$$

For a realization, $Q = P_S P_S^*$.

We call the elementary scalar conditions

$$\lambda_d \in \mathbb{Z}_{\geq 0}, \qquad \lambda_D = 1, \qquad \sum_{d=1}^{D} \lambda_d = \binom{n}{2} \tag{2}$$

basic admissibility. These conditions are necessary but, as we shall see, very far from sufficient. In centered Laurent notation

$$\mathcal{Q}(x) = x^{-D} Q(x) = n + \sum_{d=1}^{D} \lambda_d (x^d + x^{-d}),$$

every realization also satisfies the Fourier condition

$$\mathcal{Q}(e^{it}) = |P_S(e^{it})|^2 \geq 0 \qquad (t \in \mathbb{R}). \tag{3}$$

For a polynomial f with nonzero constant term, its reciprocal is $f^*(x) = x^{\deg f} f(x^{-1})$. An irreducible factor is self-reciprocal when it is associated to its reciprocal.

Theorem 2.1 (factor parity)**.** *Let $Q \in \mathbb{Z}[x]$ be monic and reciprocal of degree $2D$, with center coefficient n and $Q(1) = n^2$. Then $Q = PP^*$ for a point polynomial $P \in \{0,1\}[x]$ if and only if every self-reciprocal irreducible factor of Q occurs with even multiplicity.*

Proof. If $Q = PP^*$, a self-reciprocal irreducible appears equally in P and P^*, hence with even total multiplicity.

Conversely, factor Q over $\mathbb{Z}[x]$. Split each even self-reciprocal multiplicity in half. Reciprocity forces equal multiplicities on every non-self-reciprocal pair f, f^*; allocate those factors between an integral polynomial R and R^*. Thus $Q = RR^*$. Choose the global sign so that $R(1) = n$. If $R = \sum_i r_i x^i$, comparison of the center coefficient gives

$$\sum_i r_i^2 = n, \qquad \sum_i r_i = n.$$

Consequently $\sum_i r_i(r_i - 1) = 0$. Every summand is a nonnegative integer and vanishes only at $r_i \in \{0,1\}$. Hence R is a point polynomial. □

Corollary 2.2 (dense frequency Turnpike is in P)**.** *When the complete vector $(\lambda_1, \ldots, \lambda_D)$ is part of the input, Turnpike realizability is decidable in deterministic polynomial time.*

Proof. First check (2), construct (1), factor this degree-$2D$ integer polynomial, and apply Theorem 2.1. Polynomial-time factorization in degree and coefficient bit length follows from the LLL framework [3]. Since the dense input itself has D coordinates, the procedure is polynomial in its input length. □

Thus a polynomial-time many-one reduction from an NP-complete problem to this *dense* language would imply $P = NP$. Showing that one particular proposed mapping fails does not prove that no reduction exists: an unconditional proof of nonexistence would itself separate P from NP, assuming the target has fixed YES and NO instances.

3 A primitive Fourier-positive obstruction family

Throughout this section let $k \geq 4$ and $m = 2^{k-1}$, so $2m = 2^k$.

3.1 The irreducible core

Define

$$G_k(x) = x^{2m} + 2x^{2m-1} + 8x^m + 2x + 1. \tag{4}$$

Proposition 3.1. *For every $k \geq 4$, G_k is monic, irreducible over $\mathbb{Q}$, self-reciprocal, noncyclotomic, and not a monomial composition $x^a H(x^b)$ with $b > 1$. Moreover*

$$M(G_k) \leq 14, \qquad h(\alpha) \leq \frac{\log 14}{2^k}$$

for every root α, where M is Mahler measure and h is the absolute logarithmic height.

Proof. Modulo 2, Frobenius gives

$$G_k(x+1) \equiv (x+1)^{2^k} + 1 \equiv x^{2^k}.$$

Every nonleading coefficient of the translate is divisible by 2, while its constant coefficient is $G_k(1) = 14$, not divisible by 4. Eisenstein's criterion proves irreducibility.

Self-reciprocity is immediate. The exponent support contains 0 and 1, so the gcd of all exponent differences is 1; this excludes a visible monomial composition. On the unit circle, after centering,

$$e^{-imt} G_k(e^{it}) = 8 + 4\cos((m-1)t) + 2\cos(mt) \geq 2. \tag{5}$$

Thus G_k has no unit-circle root and is not cyclotomic. Finally the standard length bound gives $M(G_k) \leq \|G_k\|_1 = 14$. Because G_k is monic irreducible of degree 2^k, the height formula yields the stated bound. □

3.2 Fixed nonnegative blocks

For a centered Laurent polynomial, write $y = x + x^{-1} = 2\cos t$. Set

$$U(x) = 4 + 2(x + x^{-1}) + \sum_{d=2}^{7} (x^d + x^{-d}), \tag{6}$$

$$V(x) = 4 + 2(x + x^{-1}) + \sum_{d=2}^{9} (x^d + x^{-d}), \tag{7}$$

$$W(x) = 6 + \sum_{d=1}^{12} a_d (x^d + x^{-d}), \tag{8}$$

where

$$(a_1, \ldots, a_{12}) = (3, 3, 3, 3, 3, 2, 2, 2, 1, 1, 1, 1).$$

Their centers are $4, 4, 6$, and their values at 1 are $20, 24, 56$.

Lemma 3.2. *For every real t,*

$$U(e^{it}) \geq 0, \qquad V(e^{it}) \geq 0, \qquad W(e^{it}) > 0.$$

Proof. In the trace variable,

$$\begin{aligned} U(y) &= (y+2)q_7(y), & q_7(y) &= y^6 - y^5 - 4y^4 + 3y^3 + 4y^2 - 2y + 1, \\ V(y) &= (y+2)q_9(y), & q_9(y) &= y^8 - y^7 - 6y^6 + 5y^5 + 11y^4 - 7y^3 - 6y^2 + 2y + 2. \end{aligned}$$

Exact Sturm chains show that q_7, q_9 have no root on $(-2, 2)$, and their values at both endpoints are positive. The trace polynomial of W, with coefficients from constant term upward, is

$$(6, -7, -34, 41, 86, -61, -91, 37, 46, -10, -11, 1, 1).$$

Its exact Sturm chain likewise has no root on $(-2, 2)$, while its values at $-2, 0, 2$ are $4, 6, 56$. The complete endpoint sign certificates are in Appendix A. □

3.3 Separated dilations and factor avoidance

Take $(F_1, \dots, F_5) = (U, U, V, V, W)$, with respective radii $(7, 7, 9, 9, 12)$. For a threshold L, choose positive integers b_i successively as follows. Set $S_0 = 0$; after choosing $b_1, \dots, b_{i-1}$, select

$$b_i > L + 2S_{i-1}, \qquad S_i = S_{i-1} + r_i b_i, \tag{9}$$

and require that $G_k \nmid x^{r_i b_i} F_i(x^{b_i})$.

Lemma 3.3 (separation and avoidance)**.** *The scales in (9) can always be selected. With*

$$J_k(x) = \prod_{i=1}^{5} F_i(x^{b_i}),$$

every nonzero centered frequency of J_k has magnitude greater than L, the center coefficient is the product of the five center coefficients, and $G_k \nmid J_k$. If $L = O(m)$, all $b_i = O(m)$.

Proof. Convert a fixed block F of radius r to the ordinary degree-$2r$ polynomial $x^r F(x)$, and fix a root α of G_k. If $G_k \mid x^{rb} F(x^b)$, then α^b is one of its at most $2r$ nonzero roots. For a fixed root β, at most one positive b can satisfy $\alpha^b = \beta$; two such exponents would make α a root of unity, contrary to (5). Hence each block has at most $2r$ bad dilation exponents. Above any threshold, one of the next $2r + 1$ integers is good.

For frequency separation, consider a nonzero sum of selected block frequencies and take its largest index i with a nonzero contribution. Its magnitude is at least $b_i - S_{i-1} > L$. The same argument with $L = 0$ gives uniqueness of the zero-frequency representation, so center coefficients multiply. Since there are only five fixed-radius blocks, the recurrence and the bounded skips give $b_i = O(L) = O(m)$. □

In particular,

$$c := [x^0] J_k = 4^4 \cdot 6 = 1536, \qquad J_k(1) = 20^2\, 24^2\, 56 = 12{,}902{,}400, \tag{10}$$

and the deliberately tuned identity

$$14 J_k(1) = 13{,}440^2 \tag{11}$$

holds.

3.4 An eight-point overlap corrector

Put $T = 2m + 1$ and

$$\mathcal{A}_k = \{jT : 0 \le j < 5\} \cup \{jT + m : 0 \le j < 3\}. \tag{12}$$

This set has eight points, exactly three pairs at distance m, and no pair at distance $m - 1$. Indeed, the three within-cluster pairs give distance m, while the least new positive cross-cluster difference is $T - m = m + 1$. Let

$$A_k(x) = \sum_{a \in \mathcal{A}_k} x^a, \qquad B_k(x) = A_k(x) A_k(x^{-1})$$

in centered Laurent notation. Then

$$[x^0] B_k = 8, \quad [x^{\pm m}] B_k = 3, \quad [x^{\pm(m-1)}] B_k = 0. \tag{13}$$

Moreover $\operatorname{diam}(\mathcal{A}_k) = 4T = 8m + 4$.

3.5 The final instances

Use Lemma 3.3 with

$$L_k = \operatorname{diam}(\mathcal{A}_k) + m = 9m + 4.$$

Set $K_k = J_k B_k$. No noncentral frequency of J_k can contribute to the coefficients of K_k at $0, m, m-1$; hence

$$[x^0]K_k = 8c, \quad [x^{\pm m}]K_k = 3c, \quad [x^{\pm(m-1)}]K_k = 0. \tag{14}$$

Let $\mathcal{G}_k = x^{-m}G_k$ and form the centered product

$$\mathcal{Q}_k = \mathcal{G}_k J_k B_k. \tag{15}$$

Finally shift by its radius D_k to obtain the ordinary reciprocal polynomial $Q_k = x^{D_k}\mathcal{Q}_k$.

Theorem 3.4 (main construction)**.** *For every $k \geq 4$, the coefficients of Q_k define a coefficientwise-nonnegative, Fourier-nonnegative, basic-admissible sparse Turnpike instance for exactly*

$$\boxed{n = 107{,}520}$$

points, but the instance is not realizable. The obstruction includes the primitive irreducible self-reciprocal factor G_k, of degree 2^k, at odd multiplicity.

Proof. Every factor of $\mathcal{Q}_k$ has nonnegative integral coefficients and extreme coefficient 1. The shifted polynomial Q_k is therefore integral, monic, reciprocal, and coefficientwise nonnegative.

At 1, using (11) and $A_k(1) = 8$,

$$Q_k(1) = 14J_k(1)\,8^2 = (13{,}440 \cdot 8)^2 = 107{,}520^2.$$

The centered frequencies of $\mathcal{G}_k$ are 8 at zero, 2 at $\pm(m-1)$, and 1 at $\pm m$. Therefore

$$[x^0]\mathcal{Q}_k = 8(8c) + 4(0) + 2(3c) = 70c = 107{,}520.$$

Reciprocity now gives

$$\sum_{d=1}^{D_k} \lambda_d = \frac{Q_k(1) - [x^0]\mathcal{Q}_k}{2} = \binom{107{,}520}{2},$$

and the extreme coefficient gives $\lambda_{D_k} = 1$. Thus the instance is basic-admissible.

By Proposition 3.1, Lemma 3.2, and the definition of B_k,

$$\mathcal{Q}_k(e^{it}) = \mathcal{G}_k(e^{it})J_k(e^{it})|A_k(e^{it})|^2 \geq 0.$$

Finally G_k occurs once in the displayed core and does not divide J_k. Its multiplicity in $A_k A_k^*$ is even because G_k is self-reciprocal. Its total multiplicity in Q_k is therefore odd, so Theorem 2.1 proves nonrealizability. □

Corollary 3.5 (exponential obstruction degree)**.** *The expanded number of nonzero coefficients of Q_k is bounded by an absolute constant, every exponent has $O(k)$ bits, and*

$$\deg G_k = 2^k = \Theta(D_k).$$

Consequently the odd primitive obstruction degree is exponential in the sparse input length.

Proof. There are five fixed blocks and one eight-point corrector, so the support of their expanded product is bounded independently of k. Lemma 3.3 gives $D_k = O(m)$, while the core itself gives $D_k \geq m$. Hence $D_k = \Theta(m) = \Theta(2^k)$, and the binary exponent encoding has length $\Theta(k)$. □

This corollary rules out a polynomial obstruction-degree theorem under the conditions imposed here. It does not rule out algorithms that use stronger global conditions, such as the full collection of overlap inequalities, nor does it establish NP-hardness.

4 Three arithmetic barriers to easy legalization

4.1 Integral Hermitian sums of squares collapse

Real trigonometric nonnegativity alone admits spectral factorizations over $\mathbb{C}$, but the Turnpike scalar identities are much more rigid over $\mathbb{Z}$.

Theorem 4.1 (integral Hermitian-SOS collapse)**.** *Let $\mathcal{Q}$ be a centered reciprocal Laurent polynomial with center coefficient n and $\mathcal{Q}(1) = n^2$. Then*

$$\mathcal{Q}(x) = \sum_j R_j(x)R_j(x^{-1}), \quad R_j \in \mathbb{Z}[x],$$

if and only if $\mathcal{Q}(x) = P(x)P(x^{-1})$ for a point polynomial $P \in \{0,1\}[x]$.

Proof. Only the reverse implication is nontrivial. Write $R_j = \sum_i r_{j,i}x^i$, and set

$$b_j = \sum_i r_{j,i}^2, \qquad s_j = \sum_i r_{j,i}.$$

Comparing the center and the value at 1 gives $\sum_j b_j = n$ and $\sum_j s_j^2 = n^2$. Since $|r| \le r^2$ for an integer r,

$$n^2 = \sum_j s_j^2 \le \sum_j b_j^2 \le \left(\sum_j b_j\right)^2 = n^2.$$

Equality in the last inequality forces at most one b_j to be nonzero, so $\mathcal{Q}(x) = R(x)R(x^{-1})$. Equality in $|R(1)| \le \sum_i |r_i| \le \sum_i r_i^2$ forces all nonzero coefficients to have a common sign and absolute value 1. A global sign change makes R binary. □

Thus every Fourier-positive basic-admissible NO instance lies outside the *integral* Hermitian-SOS cone even though it belongs to the real nonnegative trigonometric cone.

4.2 No neutral ratio-raising multiplier

For a centered reciprocal Laurent polynomial M with $M(1) > 0$, define

$$\rho(M) = \frac{\sqrt{M(1)}}{[x^0]M}.$$

Call M *parity-safe* if every self-reciprocal irreducible factor has even multiplicity, equivalently if $M(x) = E(x)E(x^{-1})$ over $\mathbb{Z}$ in centered notation.

Proposition 4.2 (neutral-multiplier bound)**.** *If M is parity-safe, then $\rho(M) \le 1$. Hence every reciprocal integer multiplier with $\rho(M) > 1$ imports an odd self-reciprocal factor.*

Proof. Write $E = \sum_i e_i x^i$. Then $[x^0]M = \sum_i e_i^2$ and $\sqrt{M(1)} = |\sum_i e_i|$. Therefore

$$\sqrt{M(1)} \le \sum_i |e_i| \le \sum_i e_i^2 = [x^0]M.$$

□

This explains why the ratio-raising blocks in the main construction are suited to building a NO family but cannot serve as a neutral, input-independent shell for both branches of a many-one reduction.

4.3 A strictly positive NO midpoint

Proposition 4.3 (convexity barrier)**.** *The frequency vector*

$$n = 4, \quad D = 8, \quad \lambda = (1, 1, 0, 1, 0, 1, 1, 1)$$

is not realizable, although its Fourier spectrum is strictly positive and it is the midpoint of two realizable integer frequency vectors.

Proof. The two point sets

$$S_1 = \{0, 1, 7, 8\}, \qquad S_2 = \{0, 2, 4, 8\}$$

have frequency vectors

$$(2, 0, 0, 0, 0, 1, 2, 1), \qquad (0, 2, 0, 2, 0, 1, 0, 1),$$

whose midpoint is λ.

If λ were realized, normalize its points to $0 < a < b < 8$. The five nonmaximal distances would be $a, b, b-a, 8-a, 8-b$, with sum $16+b-a$. Their prescribed multiset is $\{1, 2, 4, 6, 7\}$, of sum 20, so $b - a = 4$. The only cases $(a, b) = (1, 5), (2, 6), (3, 7)$ give respectively

$$\{1, 3, 4, 5, 7\}, \quad \{2, 2, 4, 6, 6\}, \quad \{1, 3, 4, 5, 7\},$$

never the target.

Let P_i be the point polynomial of S_i. The midpoint spectrum is $\frac{1}{2}(|P_1(e^{it})|^2 + |P_2(e^{it})|^2)$, hence nonnegative. It is strictly positive because $P_1 = (1 + x)(1 + x^7)$ and $P_2 = 1 + x^2 + x^4 + x^8$ have no common unit-circle zero: at $x = -1$, $P_2 = 4$; under $x^7 = -1$, the second polynomial reduces to $x^4 + x^2 - x + 1$, whose gcd with $x^7 + 1$ is 1. □

Accordingly, no convex relaxation whose projected feasible region contains the convex hull of all realizable autocorrelations can exactly characterize integer Turnpike realizability.

5 Quadratic shadows modulo primes

The high-degree obstruction in Theorem 3.4 need not remain high degree after reduction modulo a suitable prime.

Theorem 5.1 (quadratic shadow)**.** *Let $g \in \mathbb{Z}[x]$ be irreducible and self-reciprocal, with no root at ± 1. For infinitely many unramified primes p, the reduction of g contains an irreducible reciprocal quadratic*

$$x^2 - ax + 1 \in \mathbb{F}_p[x].$$

If g occurs to odd multiplicity in an integer polynomial Q, then, outside a finite set of additional primes, this quadratic shadow also occurs to odd multiplicity in Q mod p.

Proof. Let α be a root. Self-reciprocity makes α^{-1} a conjugate, so the embedding $\alpha \mapsto \alpha^{-1}$ extends to an element of the Galois group of the splitting field. Its permutation on the roots contains the transposition $\alpha \leftrightarrow \alpha^{-1}$. Chebotarev's density theorem [7] supplies infinitely many primes whose Frobenius lies in the corresponding conjugacy class. The two-cycle then yields a degree-two irreducible factor, and its roots are mutual inverses, so its constant term is 1. Excluding primes dividing discriminants, leading coefficients, and relevant resultants preserves multiplicity and coprimality, proving the last assertion. □

There is also a group-theoretic density estimate. Let a transitive group G act on the root set Ω, and let $\iota(\alpha) = \alpha^{-1}$. For $\sigma \in G$, define

$$F(\sigma) = \#\{\alpha \in \Omega : \sigma\alpha = \iota\alpha\}.$$

Let r be the permutation rank, the number of G-orbits on Ω^2.

Proposition 5.2 (permutation-rank density)**.** *With uniform $\sigma \in G$, one has*

$$\mathbb{E}F = 1, \qquad \mathbb{E}F^2 \le r, \qquad \Pr(F > 0) \ge \frac{1}{r}.$$

Consequently the Chebotarev density of primes exposing at least one reciprocal quadratic shadow is at least $1/r$.

Proof. For each α, transitivity gives exactly $|G|/|\Omega|$ elements sending α to $\iota\alpha$, proving $\mathbb{E}F = 1$. For the second moment, an ordered pair contributes precisely when its orbital is preserved by coordinatewise inversion. Each preserved orbital contributes one to the expectation, so $\mathbb{E}F^2$ is the number of such orbitals and is at most r. Cauchy–Schwarz gives $\Pr(F > 0) \ge (\mathbb{E}F)^2/\mathbb{E}F^2 \ge 1/r$. □

This is an existence and density theorem, not a polynomial-time prime-search theorem. A sharp obstruction to naive enumeration is already cyclotomic. For an odd prime q, a reciprocal quadratic factor of Φ_{2q} mod p requires Frobenius to act as inversion on a primitive $2q$-th root. Since $(\mathbb{Z}/2q\mathbb{Z})^\times$ has a unique element of order two,

$$p \equiv -1 \pmod{2q}, \qquad p \ge 2q - 1.$$

When q is stored in binary, the first exposing prime can therefore be exponentially large in numeric value, although its bit length is only $O(\log q)$. Effective discovery of suitable primes for general noncyclotomic sparse factors remains open in this approach.

6 A ramified characteristic-zero parity lift

The trace substitution $y = x + x^{-1}$ converts an irreducible trace factor $h(y)$ into the reciprocal lift $x^{\deg h}h(x + x^{-1})$. In the field $K = \mathbb{Q}[y]/(h)$, its behavior is controlled by one square class.

Lemma 6.1 (trace-square criterion)**.** *Suppose $h \in \mathbb{Q}[y]$ is irreducible and $h(2)h(-2) \neq 0$. The reciprocal lift $x^{\deg h}h(x+x^{-1})$ is irreducible and self-reciprocal exactly when $\Delta = y^2 - 4$ is nonsquare in $K = \mathbb{Q}[y]/(h)$. When Δ is a square in K, the lift factors as a non-self-reciprocal pair $f f^*$.*

Proof. Over K, a lifted root satisfies

$$x^2 - yx + 1 = 0,$$

whose discriminant is Δ. If Δ is nonsquare, adjoining x doubles the degree, so the degree-$2\deg h$ lift is irreducible. If Δ is square, the two roots $(y \pm \sqrt{\Delta})/2$ already lie in K, are mutual inverses, and their degree-$\deg h$ minimal polynomials form the pair f, f^*. □

This gives the following direct Legendre-symbol gadget.

Proposition 6.2 (ramified Legendre-to-parity lift)**.** *Let p be odd, let $c > 0$, and suppose $p \nmid c(a^2-4)$. Define*

$$H_{a,c}(y) = (y-a)^2 - pc(y^2-4).$$

Its discriminant is

$$\operatorname{disc} H_{a,c} = 4pc\big(a^2 - 4 + 4pc\big). \tag{16}$$

If $\left(\frac{a^2-4}{p}\right) = -1$, then $H_{a,c}$ is irreducible and its reciprocal lift contains an odd self-reciprocal obstruction over $\mathbb{Q}$. For every nonzero square residue $a^2 - 4 \bmod p$, one can instead choose $c > 0$, $p \nmid c$, so that the lift splits into a reciprocal pair. In both cases $H_{a,c}(y) \geq 0$ for $y \in [-2, 2]$.

Proof. In $K = \mathbb{Q}[y]/(H_{a,c})$,

$$y^2 - 4 = \frac{(y-a)^2}{pc}. \tag{17}$$

If $a^2 - 4$ is a nonresidue modulo p, the integer $a^2 - 4 + 4pc$ cannot be a rational square, and (16) has odd p-adic valuation. Thus $H_{a,c}$ is irreducible. Its quadratic field $\mathbb{Q}(\sqrt{pc(a^2-4+4pc)})$ is not $\mathbb{Q}(\sqrt{pc})$, so pc is not a square in K. Relation (17) makes Δ nonsquare, yielding an irreducible self-reciprocal lift.

If $a^2 - 4$ is a nonzero square modulo p, choose $b \equiv \sqrt{a^2-4} \pmod{p}$ with the same parity as a, and replace b by $b + 2pt$. One can choose t so that

$$c = \frac{b^2 - a^2 + 4}{4p} > 0, \qquad p \nmid c.$$

Then the final factor in (16) is b^2, and $K = \mathbb{Q}(\sqrt{pc})$. Hence pc, and therefore Δ, is a square in K; the reciprocal lift splits. Finally, on $[-2, 2]$,

$$H_{a,c}(y) = (y-a)^2 + pc(4 - y^2) \geq 0.$$

□

The small polynomial

$$h(y) = y^2 + 12, \qquad x^2 h(x + x^{-1}) = x^4 + 14x^2 + 1$$

is a strictly positive, coefficientwise nonnegative seed with an odd self-reciprocal obstruction. Indeed, in $\mathbb{Q}(\sqrt{-3})$ the element $y^2 - 4 = -16$ is not a square. This seed is not a Turnpike instance because its center and total do not satisfy the scalar identities.

The ramified gadget solves only a local lifting problem. Local square behavior does not bundle automatically. For example, with $p = 7$ and $A = y^2 - 1$, both roots $a = \pm 1$ modulo 7 have $a^2 - 4 = -3 = 4$, a square, yet

$$A(y)^2 - 7(y^2 - 4) = y^4 - 9y^2 + 29 \tag{18}$$

is irreducible over $\mathbb{Q}(\sqrt{7})$. Indeed, a factorization of this even quartic would require either $\sqrt{-35}$ (factoring as a polynomial in y^2) or $\sqrt{29}$ (a symmetric quadratic factorization), neither of which lies in $\mathbb{Q}(\sqrt{7})$. If $y^2 - 4$ were square in its trace field, the identity $(y^2-1)^2 = 7(y^2-4)$ would put $\sqrt{7}$ in that field, contradicting irreducibility over $\mathbb{Q}(\sqrt{7})$. Thus unintended global odd factors remain the exact obstruction to a hardness reduction.

7 What the results do and do not settle

The dense problem is in P, while the sparse binary-exponent problem is not settled here. Theorem 3.4 establishes that sparse inputs can hide a primitive, noncyclotomic, exponentially high-degree obstruction even after Fourier positivity and the elementary Turnpike identities are imposed. It therefore closes one proposed route to a general sparse algorithm, not the algorithmic question itself.

Nor does the construction prove hardness. By Proposition 4.2, a positive multiplier that repairs the necessary center/total ratio cannot in general be parity-neutral. By Fourier nonnegativity, every unit-circle zero has even multiplicity, so roots-of-unity assignment factors cannot themselves be the final odd obstruction. And Proposition 6.2 transports a local modular bit into characteristic zero, but (18) blocks the naive global product.

A successful reduction would need an input-dependent *conditional norm switch*: a sparse legal polynomial Q_φ such that all nonsignal factors are paired in both branches, while an off-unit irreducible self-reciprocal factor occurs oddly in exactly one branch. Equivalently, it must implement intersection (Boolean AND) on factor support modulo two without creating uncontrolled odd critical factors. Ordinary multiplication only performs XOR on multiplicity-parity vectors. Addition and differentiation can implement common-zero conditions, but introduce new factors whose parity is not controlled.

The main concrete open directions are therefore:

1. determine whether stronger overlap or shift-gcd inequalities exclude the family of Theorem 3.4, or whether analogous families can be made to pass them all;
2. find an effective, polynomial-bit method for locating quadratic shadows of the high-degree noncyclotomic factors that arise in sparse input;
3. globalize the ramified lift with a norm identity that makes every nonsignal factor even; or
4. develop a sparse algorithm that tests the trace-square condition $y^2 - 4 \in (\mathbb{Q}[y]/H_{\mathrm{odd}})^{\times 2}$ without constructing the exponentially dense odd part H_{odd}.

8 Exact computational verification

No floating-point calculation is used in the proof of the main family. The accompanying scripts use Python's exact integers and rational numbers. In particular:

- `verify_fourier_positive_turnpike_family.py` constructs the Sturm chains, checks the tuned constants, verifies the eight-point corrector, and checks the translated Eisenstein congruences for sample k;
- `verify_trace_square_criterion.py` checks trace substitutions and split/nonsplit examples;
- `verify_ramified_legendre_lift.py` checks the discriminant identity, both residue branches, the positive seed, and the bundling counterexample; and
- `verify_cyclotomic_shadow_barrier.py` checks the congruence condition for the cyclotomic small-prime obstruction.

These programs are validation aids rather than substitutes for the proofs.

A Exact Sturm certificates

Zeros are omitted in the usual count of sign variations. The exact endpoint signs of the Sturm chains used in Lemma 3.2 are:

Polynomial	Endpoint	Signs	Variations
q_7	-2	$+,-,+,-,-,-,-$	3
q_7	2	$+,+,+,+,-,+,-$	3
q_9	-2	$+,-,+,-,+,+,+,+,+$	4
q_9	2	$+,+,+,+,+,-,+,-,+$	4
W	-2	$+,-,+,-,+,-,-,+,+,+,+,+,+$	6
W	2	$+,+,+,+,+,+,+,-,+,-,+,-,+$	6

The endpoint values are

$$q_7(-2) = 29, \quad q_7(2) = 5, \qquad q_9(-2) = 46, \quad q_9(2) = 6,$$

and $W(-2) = 4, W(0) = 6, W(2) = 56$. Equal variation counts show that no root lies in $(-2, 2)$; the positive values fix the sign.

B A corrected maximum-frequency statement

For a set in $\{0, 1, \ldots, D\}$, one always has

$$\lambda_N \leq D + 1 - N.$$

If equality holds, then every possible pair $(i, i+N)$, $0 \leq i \leq D-N$, is present. This does *not* imply that all smaller distances attain their maxima. For example,

$$S = \{1, 2, 3, 4, 8, 9, 10, 11\}, \qquad D = 10,$$

has $\lambda_7 = 4 = D + 1 - 7$, but $\lambda_1 = 6 < 10$. If $N \leq (D+1)/2$, however, equality forces the two endpoint intervals to cover the entire ambient interval, and then S is complete.

C A diagnostic for proposed SUBSET-SUM mappings

A many-one reduction must compute its target instance before knowing a source solution. Therefore a construction that first assumes which input items are selected and then writes the corresponding frequency vector is circular. There is also a useful invariant check: a four-point Turnpike vector must have total frequency $\binom{4}{2} = 6$. A proposed vector of the form

$$(2 + A + C, 0, 1, 2, 1)$$

has total $6 + A + C$, and so cannot encode four points when $A, C > 0$. Likewise a genuine pair contributes one unit vector at its distance; an edge with weight $A{+}1$ represents $A{+}1$ coincident pairs, not an indivisible SUBSET-SUM item. These observations invalidate that particular construction, but, as noted after Corollary 2.2, they are not a proof that no reduction exists.

References

[1] R. Beinert and G. Plonka, Ambiguities in one-dimensional discrete phase retrieval from Fourier magnitudes, *Journal of Fourier Analysis and Applications* 21 (2015), 1169–1198. doi:10.1007/s00041-015-9405-2.

[2] M. Giesbrecht and D. S. Roche, Detecting lacunary perfect powers and computing their roots, *Journal of Symbolic Computation* 46 (2011), 1242–1259. doi:10.1016/j.jsc.2011.08.005.

[3] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász, Factoring polynomials with rational coefficients, *Mathematische Annalen* 261 (1982), 515–534. doi:10.1007/BF01457454.

[4] M. Opial, *Generalized Difference Sets—An Algorithmic Approach*, master's thesis, Comenius University in Bratislava, 2017.

[5] D. A. Plaisted, New NP-hard and NP-complete polynomial and integer divisibility problems, *Theoretical Computer Science* 31 (1984), 125–138. doi:10.1016/0304-3975(84)90130-0.

[6] J. Rosenblatt and P. D. Seymour, The structure of homometric sets, *SIAM Journal on Algebraic and Discrete Methods* 3 (1982), 343–350. doi:10.1137/0603035.

[7] J.-P. Serre, *Topics in Galois Theory*, second edition, Research Notes in Mathematics 1, A K Peters, 2008.

[8] S. S. Skiena, W. D. Smith, and P. Lemke, Reconstructing sets from interpoint distances, in *Proceedings of the 22nd Annual ACM Symposium on Theory of Computing*, 1990, pp. 332–339. doi:10.1145/100216.100258.