WEIGHTED FOURIER CERTIFICATES FOR MAXIMUM NULLITY IN GENERALIZED PETERSEN GRAPHS: RATIONAL CLASSIFICATION AND ARITHMETIC OBSTRUCTIONS

MOHIB AHMAD

ABSTRACT. For a graph G, the maximum nullity $M(G)$ of the real symmetric matrices described by G satisfies $M(G) \le Z(G)$, where $Z(G)$ is the zero forcing number. Alameda et al. proved $Z(P(n,k)) \le 2k+2$ for generalized Petersen graphs, and Krishnan recently corrected the published claim for $P(n,3)$ by showing $Z(P(12,3)) = 7$ and conjecturing $Z(P(n,3)) = 8$ for every $n \ge 13$. We construct weighted block-circulant matrices in $\mathcal{S}(P(n,k))$ and diagonalize them by the discrete Fourier transform. For $P(n,3)$ the singularity condition is encoded by an eighth-degree reciprocal polynomial $R_{p,q,\tau}$. Explicit root-of-unity certificates prove

$$M(P(n,3)) = Z(P(n,3)) = 8$$

whenever $10 \mid n$, $24 \mid n$, $28 \mid n$, or $42 \mid n$; these indices have natural density $1/6$.

We then determine the rational part of this construction completely. If $p, q, \tau \in \mathbb{Q}$, $\tau \neq 0$, and all eight roots of $R_{p,q,\tau}$ are distinct roots of unity, then exactly six parameter triples occur, with minimal moduli 10, 24, 40, and 42. Thus the modulus-28 certificate is genuinely algebraic. We also derive arithmetic obstructions from the Lam–Leung theorem on vanishing sums of roots of unity: any certificate at level n forces 27 to lie in the numerical semigroup generated by the prime divisors of n. In particular, no admissible prime level supports a constant-weight block-circulant certificate, and among levels $n = 2p$ with p odd prime only $n = 10$ occurs. These obstructions show that this certificate class cannot by itself settle the conjecture for all $n \ge 13$. A computer-assisted search, using numerical candidate generation followed by exact cyclotomic verification, finds no additional minimal modulus up to 420 beyond $10, 24, 28, 42$.

For general k, a signed specialization yields the following criterion: if $Q_k(z) = z^{2k+2} + z^{2k} + z^{k+1} + z^2 + 1$ divides $z^L - 1$, then $M(P(Lr,k)) = Z(P(Lr,k)) = 2k+2$ for every $r \ge 1$; in particular $M(P(120r,7)) = Z(P(120r,7)) = 16$.

1. INTRODUCTION

Let G be a finite simple graph. A set of initially blue vertices is a *zero forcing set* if repeated application of the colour-change rule—a blue vertex with exactly one white neighbour forces that neighbour blue—eventually colours every vertex blue. The minimum cardinality of such a set is the *zero forcing number* $Z(G)$. Zero forcing was introduced in connection with the minimum-rank problem for graph-described symmetric matrices, and the fundamental inequality

$$M(G) \le Z(G) \tag{1}$$

relates it to the maximum nullity $M(G)$; see [1] and the surveys [6, 3, 13].

For integers $n \ge 3$ and $1 \le k < n/2$, the *generalized Petersen graph* $P(n,k)$ has outer vertices $u_0, \dots, u_{n-1}$, inner vertices $v_0, \dots, v_{n-1}$, and edges

$$u_i u_{i+1}, \qquad u_i v_i, \qquad v_i v_{i+k},$$

Date: August 31, 2026.

2020 *Mathematics Subject Classification.* Primary 05C50; Secondary 15A03, 15A18, 11R18.

Key words and phrases. zero forcing number, maximum nullity, generalized Petersen graph, block-circulant matrix, Fourier diagonalization, cyclotomic polynomial, vanishing sums of roots of unity.

subscripts modulo n. These graphs originate with Watkins [12]; their ordinary adjacency spectrum was described by Gera and Stănică [7], who already used the 2×2 Fourier block decomposition that we generalize below.

Alameda et al. [2] proved the general upper bound

$$Z(P(n,k)) \le 2k+2 \tag{2}$$

for every admissible n, k, and used high-multiplicity eigenvalues of *ordinary* adjacency matrices to establish

$$M(P(15r,2)) = Z(P(15r,2)) = 6, \qquad M(P(24r,5)) = Z(P(24r,5)) = 12$$

for every $r \ge 1$. Rashidi, Shajareh Poursalavati and Tavakkoli [10] subsequently claimed the value 8 for $Z(P(n,3))$ whenever $n \ge 12$. Krishnan [8] identified the boundary counterexample $Z(P(12,3)) = 7$, established the upper bound $Z(P(n,3)) \le 8$ for $n \ge 9$, computed the zero forcing numbers for $7 \le n \le 20$, and formulated the corrected conjecture

$$Z(P(n,3)) = 8 \qquad (n \ge 13). \tag{3}$$

The unresolved content of (3) is therefore the uniform lower bound $Z(P(n,3)) \ge 8$. Our independent computation in Section 8 reproduces Krishnan's values through $n = 20$ and extends the exhaustive verification of (3) through $n = 27$.

The present paper attacks that lower bound through maximum nullity and then studies rigorous limitations of the resulting certificate class. The basic idea enlarges the adjacency-matrix certificate of [2]: instead of searching only for a high-multiplicity eigenvalue of the ordinary adjacency matrix, we choose nonzero edge weights, diagonal shifts, and Fourier modes simultaneously. This produces matrices in $\mathcal{S}(P(n,k))$ whose kernels can be certified mode by mode. Related maximum-nullity and zero-forcing questions for circulant graph families are studied by Duong et al. [5]. Here, instead, a 2×2 block-circulant matrix for generalized Petersen graphs is designed so that prescribed Fourier modes are singular through a reciprocal polynomial.

Results. Our first result is the positive one.

Theorem 1.1. *If n is divisible by at least one of* 10, 24, 28, 42, *then*

$$M(P(n,3)) = Z(P(n,3)) = 8.$$

Consequently the value in (3) *holds on a set of indices of natural density* $1/6$.

The proof is explicit: for each modulus we construct a fixed weighting whose Fourier determinant vanishes at eight prescribed roots of unity. The remaining results delimit the method.

Theorem 1.2 (Completeness over $\mathbb{Q}$; Theorem 5.1)**.** *Let $p, q, \tau \in \mathbb{Q}$ with $\tau \ne 0$, and suppose $R_{p,q,\tau}$ of* (7) *has eight distinct roots, all roots of unity. Then (p, q, τ) is one of the six triples of Table 2, and the modulus L is* 10, 24, 40 *or* 42.

Theorem 1.3 (Arithmetic obstructions; Theorems 6.2, 6.3, 6.4)**.** *Suppose $A_n(p, q, \tau)$ has nullity* 8 *for some real p, q and $\tau \ne 0$. Then* 27 *lies in the numerical semigroup generated by the primes dividing n; in particular n is not a power of* 2, *and n has an odd prime divisor at most* 23. *Moreover n is not prime, and if $n = 2p$ with p an odd prime then $p = 5$.*

The prime obstruction already shows that no collection of constant-weight block-circulant certificates of this form—finite or infinite—can prove (3) for all sufficiently large n. A computer-assisted search reported in Section 6.4 finds no additional minimal modulus through $n = 420$ beyond $10, 24, 28, 42$; this finite search is supporting evidence, not a global classification of algebraic certificates.

Our second positive result gives a reusable signed construction for arbitrary k.

Theorem 1.4. *Let $Q_k(z) = z^{2k+2} + z^{2k} + z^{k+1} + z^2 + 1$. If $Q_k(z)$ divides $z^L - 1$ in $\mathbb{Z}[z]$, then for every integer $r \geq 1$,*

$$M(P(Lr, k)) = Z(P(Lr, k)) = 2k + 2.$$

Since $Q_7(z) = \Phi_5(z)\Phi_{10}(z)\Phi_{24}(z)$, Theorem 1.4 yields the exact family $M(P(120r, 7)) = Z(P(120r, 7)) = 16$. Here and below Φ_m denotes the mth cyclotomic polynomial.

Organization. Section 2 develops the weighted Fourier certificate and the reciprocal polynomial for $P(n, 3)$. Section 3 gives the mode-selection criterion and a symmetry. Section 4 proves the explicit families and the density statement. Section 5 classifies all rational certificates. Section 6 proves the arithmetic obstructions and reports a computer-assisted finite search. Section 7 proves the signed criterion. Section 8 records the independent computation of $Z(P(n, 3))$. Section 9 discusses limitations and open problems.

2. Weighted Fourier certificates

For a graph G on N vertices let $\mathcal{S}(G)$ be the set of real symmetric $N \times N$ matrices $A = [a_{ij}]$ such that, for $i \neq j$,

$$a_{ij} \neq 0 \iff ij \in E(G),$$

with arbitrary diagonal entries. Thus $M(G) = \max\{\operatorname{null} A : A \in \mathcal{S}(G)\}$.

Let C_n be the cyclic shift defined by $C_n e_i = e_{i+1}$, indices modulo n. Put $\omega = e^{2\pi i/n}$ and

$$f_j = (1, \omega^{-j}, \omega^{-2j}, \ldots, \omega^{-(n-1)j})^T, \qquad 0 \leq j < n.$$

Then $C_n f_j = \omega^j f_j$. After normalization the f_j form an orthonormal Fourier basis, so every polynomial in C_n is unitarily diagonalized by that basis [4].

Lemma 2.1 (Fourier block decomposition)**.** *Let $a, b, c \in \mathbb{R} \setminus \{0\}$ and $d, e \in \mathbb{R}$. Define*

$$H_{n,k}(a, b, c, d, e) = \begin{pmatrix} dI_n + a(C_n + C_n^{-1}) & bI_n \\ bI_n & eI_n + c(C_n^k + C_n^{-k}) \end{pmatrix}. \tag{4}$$

Then $H_{n,k}(a, b, c, d, e) \in \mathcal{S}(P(n, k))$. Over $\mathbb{C}$ it is unitarily similar to the direct sum of the 2×2 matrices

$$B_j = \begin{pmatrix} d + a(\omega^j + \omega^{-j}) & b \\ b & e + c(\omega^{kj} + \omega^{-kj}) \end{pmatrix}, \qquad 0 \leq j < n, \tag{5}$$

and consequently $\operatorname{null} H_{n,k}(a, b, c, d, e) = \sum_{j=0}^{n-1} \operatorname{null} B_j$.

Proof. Since $1 \leq k < n/2$ we have $C_n^k \neq C_n^{-k}$, so the nonzero weights a, b, c in (4) occur precisely on the outer, spoke and inner edges of $P(n, k)$ respectively, and the off-diagonal zero pattern is correct. The vectors f_j simultaneously diagonalize C_n and all its powers; restricting (4) to the span of $(f_j, 0)^T$ and $(0, f_j)^T$ gives (5). A real matrix has the same rank over $\mathbb{R}$ and over $\mathbb{C}$, so the direct-sum decomposition computes its real nullity. □

2.1. A normalized three-parameter family.

For $p, q \in \mathbb{R}$ and $\tau \in \mathbb{R} \setminus \{0\}$ set $\varepsilon = \operatorname{sgn}(\tau)$, $\beta = \sqrt{|\tau|}$, and define

$$A_n(p, q, \tau) = \begin{pmatrix} pI_n + C_n + C_n^{-1} & \beta I_n \\ \beta I_n & \varepsilon\big(qI_n + C_n^3 + C_n^{-3}\big) \end{pmatrix}. \tag{6}$$

Since the three edge weights $1, \beta, \varepsilon$ are nonzero, $A_n(p, q, \tau) \in \mathcal{S}(P(n, 3))$. Define the reciprocal polynomial

$$R_{p,q,\tau}(z) = z^8 + pz^7 + z^6 + qz^5 + (pq - \tau)z^4 + qz^3 + z^2 + pz + 1. \tag{7}$$

Remark 2.2. The family (6) captures the singular-mode behavior of every constant-weight block-circulant matrix (4) for $k = 3$. Indeed, the Fourier determinant of (4) is

$$(d + ax)(e + cy) - b^2 = ac\left[\left(\frac{d}{a} + x\right)\left(\frac{e}{c} + y\right) - \frac{b^2}{ac}\right],$$

where $x = z + z^{-1}$ and $y = z^3 + z^{-3}$. Thus, with

$$p = d/a, \qquad q = e/c, \qquad \tau = b^2/(ac),$$

the general block is singular for exactly the same Fourier modes as the block of $A_n(p, q, \tau)$. Since both off-diagonal entries are nonzero, every singular 2×2 block has nullity one. Hence the two matrices have the same nullity. Consequently the obstructions in Section 6 apply to the entire constant-weight block-circulant class (4), not merely to a special normalization.

Lemma 2.3. *Let $z = \omega^j$ be an nth root of unity and let B_j be the Fourier block of $A_n(p, q, \tau)$. Then*

$$\det B_j = \varepsilon z^{-4} R_{p,q,\tau}(z). \tag{8}$$

Hence B_j is singular if and only if $R_{p,q,\tau}(z) = 0$, and every singular block has nullity exactly one.

Proof. By Lemma 2.1, $B_j = \begin{pmatrix} p + z + z^{-1} & \beta \\ \beta & \varepsilon(q + z^3 + z^{-3}) \end{pmatrix}$. Because $\beta^2 = |\tau| = \varepsilon\tau$, $\det B_j = \varepsilon\big[(p + z + z^{-1})(q + z^3 + z^{-3}) - \tau\big]$. Writing $p + z + z^{-1} = z^{-1}(z^2 + pz + 1)$ and $q + z^3 + z^{-3} = z^{-3}(z^6 + qz^3 + 1)$ and multiplying by z^4 gives

$$z^4\varepsilon^{-1} \det B_j = (z^2 + pz + 1)(z^6 + qz^3 + 1) - \tau z^4 = R_{p,q,\tau}(z),$$

which is (8). Since the off-diagonal entry is $\beta \neq 0$, a singular 2×2 block is nonzero and therefore has rank one. □

Proposition 2.4 (Root-of-unity certificate)**.** *Suppose $R_{p,q,\tau}$ has eight distinct roots and every root is an Lth root of unity. Then, for every integer $r \geq 1$,*

$$M(P(Lr, 3)) = Z(P(Lr, 3)) = 8,$$

and the matrix $A_{Lr}(p, q, \tau)$ has nullity exactly 8.

Proof. Put $n = Lr$. Every Lth root of unity is an nth root of unity, so the eight roots of $R_{p,q,\tau}$ give eight distinct singular Fourier blocks. Lemma 2.3 shows each contributes one kernel dimension, so

$$8 \leq \operatorname{null} A_n(p, q, \tau) \leq M(P(n, 3)) \leq Z(P(n, 3)) \leq 8,$$

the last inequality being (2). Equality holds throughout. As $R_{p,q,\tau}$ has degree eight and eight distinct roots, there are no further singular blocks. □

3. Selecting singular Fourier modes

The next criterion converts four conjugate pairs of desired Fourier modes into parameters p, q, τ.

Theorem 3.1 (Mode-selection criterion)**.** *Let $\theta_1, \ldots, \theta_4 \in (0, \pi)$ be distinct and set $a_i = -2\cos\theta_i$. Let e_j denote the jth elementary symmetric polynomial in $a_1, \ldots, a_4$. Assume*

$$e_2 = -3 \tag{9}$$

and

$$\tau = e_1(3e_1 + e_3) - e_4 \neq 0. \tag{10}$$

Set $p = e_1$ and $q = 3e_1 + e_3$. Then

$$R_{p,q,\tau}(z) = \prod_{i=1}^{4}\big(z^2 + a_i z + 1\big). \tag{11}$$

Consequently, if every $e^{i\theta_i}$ is an Lth root of unity, then $M(P(Lr,3)) = Z(P(Lr,3)) = 8$ for every $r \geq 1$.

Proof. A direct expansion gives

$$\prod_{i=1}^{4}(z^2 + a_i z + 1) = z^8 + e_1 z^7 + (4 + e_2)z^6 + (3e_1 + e_3)z^5 + (6 + 2e_2 + e_4)z^4 + (3e_1 + e_3)z^3 + (4 + e_2)z^2 + e_1 z + 1.$$

Under (9) the coefficients of z^6 and z^2 equal 1 and the central coefficient becomes e_4; the definitions of p, q, τ give $pq - \tau = e_4$, proving (11). Since $z^2 - 2\cos(\theta_i)z + 1 = (z - e^{i\theta_i})(z - e^{-i\theta_i})$, the roots are $e^{\pm i\theta_i}$, and the hypotheses make these eight roots distinct. Proposition 2.4 completes the proof. □

Remark 3.2. The constraint $e_2 = -3$ is not an auxiliary condition introduced for convenience: within the family (6) it is exactly the coefficient constraint forced by the fixed coefficients of z^6 and z^2 in (7). The condition $\tau \neq 0$ is likewise essential, being equivalent to requiring the spoke weight $\beta = \sqrt{|\tau|}$ to be nonzero.

The following elementary symmetry explains the paired rational certificates.

Lemma 3.3 (Reflection symmetry)**.** *For all p, q, τ,*

$$R_{p,q,\tau}(-z) = R_{-p,-q,\tau}(z).$$

Thus negating all roots sends (p, q, τ) to $(-p, -q, \tau)$. In particular, if the roots are Lth roots of unity and L is even, the reflected triple is again a certificate at modulus L; for general L the reflected roots are $2L$th roots of unity.

Proof. Replacing z by $-z$ in (7) negates the coefficients of z^7, z^5, z^3, z and fixes the rest; the central coefficient is unchanged because $(-p)(-q) - \tau = pq - \tau$. The statement about moduli is immediate from $(-z)^L = z^L$ when L is even. □

Example 3.4 (The modulus-24 certificate)**.** Take $\{\theta_i\} = \{\pi/4, \pi/3, 2\pi/3, 3\pi/4\}$. Then $\{a_i\} = \{-\sqrt{2}, -1, 1, \sqrt{2}\}$, so $\prod_i (t + a_i) = t^4 - 3t^2 + 2$, giving $e_1 = e_3 = 0$, $e_2 = -3$, $e_4 = 2$. Theorem 3.1 gives $(p, q, \tau) = (0, 0, -2)$ and the eight selected modes are 24th roots of unity. Equivalently $R_{0,0,-2}(z) = \Phi_3(z)\Phi_6(z)\Phi_8(z)$.

4. Explicit certificates for step size three

Proposition 4.1. *For each row of Table 1, the polynomial $R_{p,q,\tau}$ has eight distinct roots, all of which are Lth roots of unity.*

Proof. Each identity follows by multiplying the displayed cyclotomic polynomials. The factors in each row are pairwise distinct and every factor divides $z^L - 1$, so the product has eight distinct roots, all Lth roots of unity. □

The remaining coverage modulus uses an algebraic certificate; note that its parameters are irrational, so it lies outside the scope of Theorem 5.1.

TABLE 1. Rational root-of-unity certificates for $P(n,3)$. The polynomial in each row is $R_{p,q,\tau}$ from (7). By Theorem 5.1 this list, together with the reflections supplied by Lemma 3.3, is complete.

L	(p,q,τ)	Cyclotomic factorization of $R_{p,q,\tau}(z)$
10	$(0,0,-1)$	$\Phi_5(z)\Phi_{10}(z)$
24	$(0,0,-2)$	$\Phi_3(z)\Phi_6(z)\Phi_8(z)$
40	$(1,1,-1)$	$\Phi_5(z)\Phi_8(z)$
42	$(0,1,-1)$	$\Phi_6(z)\Phi_7(z)$

Proposition 4.2 (The modulus-28 certificate)**.** *Let $\alpha = 2\cos(\pi/7)$, $p = 1-\alpha^2$, $q = \alpha$, $\tau = -1$. Then $R_{p,q,\tau}$ has the eight distinct roots*

$$e^{\pm i\pi/14}, \quad e^{\pm i\pi/7}, \quad e^{\pm 3i\pi/7}, \quad e^{\pm 13i\pi/14},$$

all of which are 28th roots of unity.

Proof. The number $\alpha = 2\cos(\pi/7)$ satisfies

$$\alpha^3 - \alpha^2 - 2\alpha + 1 = 0. \tag{12}$$

Let $\gamma = 2\cos(3\pi/7)$. Since $\gamma = \alpha^3 - 3\alpha$, relation (12) gives

$$\alpha + \gamma = \alpha^2 - 1, \qquad \alpha\gamma + 2 = \alpha + 1. \tag{13}$$

A direct expansion, reduced using (12), yields

$$R_{1-\alpha^2,\alpha,-1}(z) = \big(z^4 - \alpha z^2 + 1\big)\big(z^4 + (1-\alpha^2)z^3 + (\alpha+1)z^2 + (1-\alpha^2)z + 1\big).$$

Let $c = 2\cos(\pi/14)$; since $c^2 = 2 + \alpha$, $(z^2 - cz + 1)(z^2 + cz + 1) = z^4 - \alpha z^2 + 1$. Using (13),

$$(z^2 - \alpha z + 1)(z^2 - \gamma z + 1) = z^4 + (1-\alpha^2)z^3 + (\alpha+1)z^2 + (1-\alpha^2)z + 1.$$

The four quadratic factors have roots $e^{\pm i\pi/14}$, $e^{\pm 13i\pi/14}$, $e^{\pm i\pi/7}$, $e^{\pm 3i\pi/7}$ respectively; these are eight distinct 28th roots of unity. □

Theorem 4.3. *If n is a positive integer divisible by at least one of $10, 24, 28, 42$, then*

$$M(P(n,3)) = Z(P(n,3)) = 8.$$

Proof. If $10 \mid n$, $24 \mid n$ or $42 \mid n$, apply Proposition 2.4 with the corresponding row of Table 1. If $28 \mid n$, apply Proposition 2.4 and Proposition 4.2. Every listed modulus exceeds 6, so $P(n,3)$ is admissible. □

Corollary 4.4. *The set of positive integers divisible by at least one of $10, 24, 28, 42$ has natural density $1/6$.*

Proof. Let A, B, C be the sets of positive integers divisible by 10, by 24, and by 7 together with at least one of 4 or 6, respectively; then $A \cup B \cup C$ is the set in question. Their densities are $d(A) = \frac{1}{10}$, $d(B) = \frac{1}{24}$ and $d(C) = \frac{1}{7}\big(\frac{1}{4} + \frac{1}{6} - \frac{1}{12}\big) = \frac{1}{21}$. Furthermore $d(A \cap B) = \frac{1}{120}$, $d(A \cap C) = \frac{1}{105}$, $d(B \cap C) = \frac{1}{168}$ and $d(A \cap B \cap C) = \frac{1}{840}$. Inclusion–exclusion gives

$$\tfrac{1}{10} + \tfrac{1}{24} + \tfrac{1}{21} - \tfrac{1}{120} - \tfrac{1}{105} - \tfrac{1}{168} + \tfrac{1}{840} = \tfrac{140}{840} = \tfrac{1}{6}.$$ □

Remark 4.5. The modulus 40 of Table 1 is a genuine and distinct weighting but contributes no new indices, since $40 \mid n$ implies $10 \mid n$. We retain it because Theorem 5.1 shows it is one of only four rational moduli, and because it illustrates that different weighted certificates coexist on the same arithmetic family.

5. Classification of all rational certificates

We now show that Table 1 is complete over $\mathbb{Q}$. This converts the table from a list of examples into a classification, and explains why no further rational certificate was found.

Theorem 5.1. *Let $p, q, \tau \in \mathbb{Q}$ with $\tau \neq 0$, and suppose $R_{p,q,\tau}$ has eight distinct roots, all of which are roots of unity. Then $R_{p,q,\tau}$ is one of the six polynomials of Table 2, and the modulus L is 10, 24, 40 or 42.*

Table 2. All rational certificates. The six rows form three reflection-conjugate pairs under Lemma 3.3.

Factorization	p	q	τ	L
$\Phi_5\Phi_{10}$	0	0	-1	10
$\Phi_3\Phi_6\Phi_8$	0	0	-2	24
$\Phi_5\Phi_8$	1	1	-1	40
$\Phi_8\Phi_{10}$	-1	-1	-1	40
$\Phi_6\Phi_7$	0	1	-1	42
$\Phi_3\Phi_{14}$	0	-1	-1	42

Proof. Every root of $R := R_{p,q,\tau}$ is a root of unity, hence an algebraic integer; as R is monic with rational coefficients, $R \in \mathbb{Z}[z]$. Each monic irreducible factor of R over $\mathbb{Q}$ has a root of unity as a root and is therefore a cyclotomic polynomial. Since the eight roots are distinct, these factors are pairwise distinct and each occurs to the first power, so

$$R = \prod_{m \in S} \Phi_m, \qquad \sum_{m \in S} \varphi(m) = 8$$

for a set S of distinct positive integers.

We first exclude $m \in \{1, 2\}$. As $\Phi_1(0) = -1$ and $\Phi_m(0) = 1$ for $m \geq 2$, while $R(0) = 1$, we get $1 \notin S$. If $2 \in S$ then $\sum_{m \in S,\, m \geq 3} \varphi(m) = 8 - \varphi(2) = 7$, which is impossible because $\varphi(m)$ is even for every $m \geq 3$. Hence every $m \in S$ satisfies $m \geq 3$.

Consequently S is a set of distinct integers $m \geq 3$ with $\varphi(m) \leq 8$; the possibilities are $\varphi(m) = 2$ for $m \in \{3, 4, 6\}$, $\varphi(m) = 4$ for $m \in \{5, 8, 10, 12\}$, $\varphi(m) = 6$ for $m \in \{7, 9, 14, 18\}$ and $\varphi(m) = 8$ for $m \in \{15, 16, 20, 24, 30\}$. Since $\varphi(m) \geq 2$ on this list and only three values of m give $\varphi(m) = 2$, the partitions of 8 that can occur are 8, $6 + 2$, $4 + 4$ and $4 + 2 + 2$.

Because every Φ_m with $m \geq 2$ is palindromic, so is R; the shape of (7) therefore imposes the single further condition

$$[z^6]R = 1,$$

the equality $[z^2]R = 1$ being automatic. Checking this condition across the finitely many admissible sets S leaves exactly fourteen candidates. Of these, eight have $\tau = pq - [z^4]R = 0$ and are excluded by hypothesis, namely

$$\Phi_3\Phi_9,\ \Phi_6\Phi_9,\ \Phi_4\Phi_9,\ \Phi_3\Phi_{18},\ \Phi_6\Phi_{18},\ \Phi_4\Phi_{18},\ \Phi_3\Phi_4\Phi_{12},\ \Phi_4\Phi_6\Phi_{12},$$

and the remaining six are those of Table 2. Their moduli are the least common multiples of the indices appearing, namely 10, 24, 40, 40, 42, 42. □

Corollary 5.2. *The set of indices covered by rational certificates is exactly $\{n : 10 \mid n \text{ or } 24 \mid n \text{ or } 42 \mid n\}$, whose natural density is $31/210$. The modulus 28 of Theorem 4.3 is therefore genuinely algebraic within the present constant-weight block-circulant class: it cannot be realized*

by rational parameters in (6)*, and it is precisely what raises the coverage density from* 31/210 *to* 1/6.

Proof. By Theorem 5.1 the rational moduli are $10, 24, 40, 42$, and $40 \mid n$ implies $10 \mid n$, so the covered set is as stated. Inclusion–exclusion with $\operatorname{lcm}(10,24) = 120$, $\operatorname{lcm}(10,42) = 210$, $\operatorname{lcm}(24,42) = 168$ and $\operatorname{lcm}(10,24,42) = 840$ gives

$$\tfrac{1}{10} + \tfrac{1}{24} + \tfrac{1}{42} - \tfrac{1}{120} - \tfrac{1}{210} - \tfrac{1}{168} + \tfrac{1}{840} = \tfrac{84+35+20-7-4-5+1}{840} = \tfrac{124}{840} = \tfrac{31}{210}.$$

Comparison with Corollary 4.4 gives $\frac{1}{6} - \frac{31}{210} = \frac{140-124}{840} = \frac{2}{105}$ for the gain contributed by the modulus 28. □

6. Arithmetic obstructions and computational search

Theorem 5.1 settles the rational case. We now bound the algebraic case, where the parameters may lie in a number field, as they do in Proposition 4.2. Throughout this section $\zeta = \zeta_n = e^{2\pi i/n}$ and, for $k \in \mathbb{Z}$,

$$\eta_k = \zeta^k + \zeta^{-k} = 2\cos(2\pi k/n).$$

By Theorem 3.1 and Remark 3.2, a certificate at level n is exactly a choice of four distinct modes $m_1, \dots, m_4$ with $0 < m_i < n/2$ such that, writing $c_i = \eta_{m_i}$,

$$\sum_{i<l} c_i c_l = -3 \qquad \text{and} \qquad \tau \neq 0. \tag{14}$$

(The modes $z = \pm 1$ cannot occur: R is palindromic, so $R(z) = z^4 \widetilde{R}(z + z^{-1})$ with $\widetilde{R}$ of degree four, and $z = \pm 1$ corresponds to $z + z^{-1} = \pm 2$, a double root of R, contradicting distinctness.)

6.1. **Degenerate configurations.** We first identify a structured source of excluded solutions of $e_2 = -3$.

Proposition 6.1. *If $\tau = 0$, then*

$$R_{p,q,0}(z) = (z^2 + pz + 1)(z^6 + qz^3 + 1).$$

The six roots of the second factor are closed under multiplication by a primitive cube root of unity. Consequently, if all roots of $R_{p,q,0}$ are nth roots of unity, then $3 \mid n$.

Proof. The factorization follows by direct expansion of (7) with $\tau = 0$. The roots of $z^6 + qz^3 + 1$ are the cube roots of the two roots w_1, w_2 of $w^2 + qw + 1$, so that set is closed under multiplication by ζ_3. If all these roots are nth roots of unity, then ζ_3 is a quotient of two nth roots of unity and hence $3 \mid n$. □

6.2. **A semigroup obstruction.** The constraint (14) is a vanishing sum of roots of unity, and the Lam–Leung theorem [9] therefore applies. Recall its statement: if $\zeta_1 + \cdots + \zeta_w = 0$ with each ζ_t an Nth root of unity, then w lies in the numerical semigroup $\langle p_1, \dots, p_r \rangle$ generated by the distinct primes dividing N.

Theorem 6.2. *Suppose $A_n(p, q, \tau)$ has nullity 8 for some real p, q and some $\tau \neq 0$. Then*

$$27 \in \langle\, p : \ p \text{ prime}, \ p \mid n \,\rangle.$$

In particular:

1. *n is not a power of 2;*
2. *if $n = p^s$ is a prime power, then $p = 3$;*
3. *n has an odd prime divisor $p \leq 23$.*

Proof. Expanding $c_i c_l = (\zeta^{m_i} + \zeta^{-m_i})(\zeta^{m_l} + \zeta^{-m_l})$ into four terms, the first equation of (14) becomes

$$\sum_{i<l} \Big(\zeta^{m_i+m_l} + \zeta^{-m_i-m_l} + \zeta^{m_i-m_l} + \zeta^{m_l-m_i} \Big) + 3 \cdot \zeta^0 = 0,$$

a vanishing sum of $6 \cdot 4 + 3 = 27$ nth roots of unity, each with coefficient 1. By [9], 27 lies in the numerical semigroup generated by the primes dividing n.

For (i), 27 is odd and $\langle 2 \rangle$ contains only even numbers. For (ii), $27 \in \langle p \rangle$ forces $p \mid 27$, so $p = 3$. For (iii), write $27 = \sum_j a_j p_j$ with $a_j \geq 0$; since 27 is odd some odd prime p_j occurs with $a_j \geq 1$, and then $p_j \leq 27$, so $p_j \leq 23$. □

6.3. **Prime and semiprime levels.** The prime case is already excluded by Theorem 6.2. For the more delicate case $n = 2p$ we use the following standard fact: for an odd prime p the numbers $\eta_1, \ldots, \eta_{(p-1)/2}$ (formed with ζ_p) constitute a $\mathbb{Q}$-basis of the maximal real subfield $\mathbb{Q}(\zeta_p)^+$, and

$$\sum_{k=1}^{(p-1)/2} \eta_k = \sum_{k=1}^{p-1} \zeta_p^k = -1. \tag{15}$$

See [11, Ch. 2]. We also use repeatedly the product rule $\eta_a \eta_b = \eta_{a+b} + \eta_{a-b}$, together with $\eta_{-k} = \eta_k$ and $\eta_0 = 2$.

Corollary 6.3. *If n is prime, then no constant-weight block-circulant certificate exists; that is, there are no real p, q and $\tau \neq 0$ for which $A_n(p, q, \tau)$ has nullity 8.*

Proof. If $n = p$ is prime, Theorem 6.2 gives $27 \in \langle p \rangle$, hence $p \mid 27$ and therefore $p = 3$. But $P(3, 3)$ is not an admissible generalized Petersen graph. □

Theorem 6.4. *Let $n = 2p$ with p an odd prime. If a constant-weight block-circulant certificate exists at level n, then $p = 5$ and $n = 10$.*

Proof. The admissible modes are distinct elements of $\{1, \ldots, p-1\}$ and $c_m = 2\cos(\pi m/p)$. Since $\zeta_{2p} = -\zeta_p^{(p+1)/2}$, we have $\zeta_{2p}^m = (-1)^m \zeta_p^{m(p+1)/2}$, so

$$c_m = \delta_m \, \eta_{j(m)}, \qquad \delta_m = (-1)^m, \quad j(m) \equiv \tfrac{p+1}{2} m \pmod{p},$$

with $j(m)$ folded into $\{1, \ldots, (p-1)/2\}$ and η formed with ζ_p. The map $m \mapsto (j(m), \delta_m)$ is a bijection from $\{1, \ldots, p-1\}$ onto $\{1, \ldots, \frac{p-1}{2}\} \times \{\pm 1\}$: indeed $j(p-m) = -j(m)$ folds to $j(m)$, while m and $p - m$ have opposite parity.

Write $c_i = \delta_i \eta_{j_i}$ for the four chosen modes. Then $c_i c_l = \delta_i \delta_l (\eta_{j_i + j_l} + \eta_{j_i - j_l})$, where $j_i + j_l \in \{2, \ldots, p-1\}$ is never $\equiv 0$, and $j_i - j_l \equiv 0$ exactly when $j_i = j_l$. Using $\eta_0 = 2 = -2 \sum_k \eta_k$ from (15) and expanding in the basis $\{\eta_k\}$, write $\sum_{i<l} c_i c_l = \sum_k A_k \eta_k$. By (15) and the $\mathbb{Q}$-linear independence of the η_k, the constraint forces $A_k = 3$ for all k, hence

$$\sum_k A_k = \tfrac{3(p-1)}{2}. \tag{16}$$

A pair with $j_i \neq j_l$ contributes $2\delta_i \delta_l$ to $\sum_k A_k$; a pair with $j_i = j_l$ has $\delta_i = -\delta_l$ and contributes $(-1)\big(1 - 2 \cdot \frac{p-1}{2}\big) = p - 2$. Let Z be the number of pairs with $j_i = j_l$ and $D = \sum \delta_i \delta_l$ over the remaining pairs; then (16) becomes

$$Z(p-2) + 2D = \tfrac{3(p-1)}{2}.$$

Since each value of j is taken by at most two modes, $Z \in \{0, 1, 2\}$.

If $Z = 2$ the modes are $(j, +), (j, -), (j', +), (j', -)$ and the four cross pairs carry signs $+, -, -, +$, so $D = 0$ and $2(p-2) = \frac{3(p-1)}{2}$, giving $p = 5$.

If $Z = 1$ the modes are $(j,+),(j,-),(j_2,\delta_2),(j_3,\delta_3)$, whose five cross pairs carry signs $\delta_2,\delta_3,-\delta_2,-\delta_3,\delta_2\delta_3$, so $D = \delta_2\delta_3 = \pm 1$ and $(p-2)\pm 2 = \frac{3(p-1)}{2}$, giving $p = 3$ or $p = -5$; neither yields an admissible $n \geq 7$.

If $Z = 0$ then $D = \sum_{i<l}\delta_i\delta_l = \frac{(\sum_i \delta_i)^2-4}{2} \in \{-2,0,6\}$, and $2D = \frac{3(p-1)}{2}$ gives $p = 9$, $p = 1$ or a negative value; none is an odd prime.

Hence $p = 5$, and the modulus 10 of Table 1 is realized. □

6.4. **Computer-assisted search.** The arithmetic obstructions do not determine all possible algebraic levels. We therefore performed a finite search. For each n under consideration, the program enumerates three-mode subsets, uses floating-point evaluation only to generate possible fourth modes, and then verifies every retained candidate *exactly* in $\mathbb{Z}[\zeta_n]$ by reduction modulo Φ_n. The same exact arithmetic is used to test $\tau \neq 0$ and to reduce a configuration to its minimal level

$$L = \operatorname{lcm}_i\big(n/\gcd(n,m_i)\big).$$

For $9 \leq n \leq 140$, this search finds primitive non-degenerate certificates at exactly the levels

$$10,\ 24,\ 28,\ 40,\ 42,\ 60,\ 84.$$

The levels 40, 60, and 84 contribute no new divisibility families because they are multiples of 10, 10, and 42, respectively. Extending the search to $n \leq 420$ while skipping levels already covered by $10, 24, 28, 42$ finds no additional minimal modulus.

Because the candidate-generation stage uses floating-point screening, we do not use the absence of further hits as a proof of nonexistence. The exact positive certificates, the rational classification, and the arithmetic obstructions proved above are independent of this search. The code and recorded outputs are supplied for reproducibility.

7. A signed certificate for general step size

A particularly simple specialization of Lemma 2.1 works for arbitrary k. Define

$$S_{n,k} = \begin{pmatrix} C_n + C_n^{-1} & I_n \\ I_n & -(C_n^k + C_n^{-k}) \end{pmatrix} \in \mathcal{S}(P(n,k)), \tag{17}$$

and $Q_k(z) = z^{2k+2} + z^{2k} + z^{k+1} + z^2 + 1$.

Theorem 7.1 (Signed-circulant certificate)**.** *Suppose $Q_k(z)$ divides $z^L - 1$ in $\mathbb{Z}[z]$. Then, for every integer $r \geq 1$, $M(P(Lr,k)) = Z(P(Lr,k)) = 2k+2$, and $S_{Lr,k}$ has nullity exactly $2k+2$.*

Proof. Because $\deg Q_k = 2k+2$, the divisibility assumption forces $L \geq 2k+2$, so $P(Lr,k)$ is admissible. For z an nth root of unity, the corresponding Fourier block of (17) is

$$\begin{pmatrix} z + z^{-1} & 1 \\ 1 & -(z^k + z^{-k}) \end{pmatrix},$$

with determinant

$$-(z+z^{-1})(z^k+z^{-k}) - 1 = -z^{-(k+1)}Q_k(z). \tag{18}$$

Since $z^L - 1$ is squarefree in characteristic zero, so is every divisor of it; thus Q_k has exactly $2k+2$ distinct roots, all Lth roots of unity. If $n = Lr$ these are nth roots of unity, so (18) gives $2k+2$ singular Fourier blocks, each nonzero because its off-diagonal entries equal 1 and hence each contributing one kernel dimension. Therefore

$$2k+2 \leq \operatorname{null} S_{n,k} \leq M(P(n,k)) \leq Z(P(n,k)) \leq 2k+2,$$

the last inequality being (2). The degree of Q_k shows there are no additional singular blocks. □

For $k = 3$ we get $Q_3(z) = z^8 + z^6 + z^4 + z^2 + 1 = \Phi_5(z)\Phi_{10}(z)$, recovering the modulus-10 certificate.

Corollary 7.2. *For every integer $r \geq 1$, $M(P(120r, 7)) = Z(P(120r, 7)) = 16$.*

Proof. A direct factorization gives $Q_7(z) = z^{16} + z^{14} + z^8 + z^2 + 1 = \Phi_5(z)\Phi_{10}(z)\Phi_{24}(z)$, and $\operatorname{lcm}(5, 10, 24) = 120$. Apply Theorem 7.1. □

Remark 7.3. For $k = 2$ one has $Q_2 = \Phi_5\Phi_6$, so Theorem 7.1 gives

$$M(P(30r, 2)) = Z(P(30r, 2)) = 6.$$

This is contained in the stronger family $M(P(15r, 2)) = Z(P(15r, 2)) = 6$ of [2] and therefore serves only as a consistency check on the signed construction.

8. Small zero forcing numbers for generalized Petersen graphs

Krishnan [8] computed $Z(P(n, 3))$ exhaustively for $7 \leq n \leq 20$. We independently implemented the same finite search and reproduced those values; we then extended the computation through $n = 27$. For each n, subsets are tested in increasing cardinality and the colour-change rule is iterated to closure. The results are collected in Table 3.

Table 3. Zero forcing numbers of $P(n, 3)$, by exhaustive search over all vertex subsets. For every n in the range $13 \leq n \leq 27$ a minimum zero forcing set is given by eight consecutive outer vertices.

n	7	8	9	10	11	12	13	14	15	16	17
$Z(P(n, 3))$	6	6	6	8	7	7	8	8	8	8	8
n	18	19	20	21	22	23	24	25	26	27	
$Z(P(n, 3))$	8	8	8	8	8	8	8	8	8	8	

The entries through $n = 20$ agree with Krishnan [8]. Only $n = 12$ contradicts the published range $n \geq 12$ of Rashidi et al.; the value $Z(P(11, 3)) = 7$ lies outside that claimed range. The new finite verification is that $Z(P(n, 3)) = 8$ also for $21 \leq n \leq 27$. In particular, the prime values $n = 13, 17, 19, 23$ satisfy the zero-forcing conjecture even though Corollary 6.3 shows that no constant-weight block-circulant maximum-nullity certificate of the present type exists at those levels.

9. Discussion and open problems

The certificates above contribute to the corrected $P(n, 3)$ problem in two ways. First, they establish the missing lower bound $Z(P(n, 3)) \geq 8$ on four divisibility families whose union has density $1/6$, without enumerating seven-element vertex sets. Second, Theorem 5.1 classifies the rational certificates completely, while Theorems 6.2–6.4 give rigorous arithmetic limitations on algebraic certificates. The finite search of Section 6.4 complements these theorems with computational evidence about small moduli.

Limits of the constant-weight certificate class. Every fixed root-of-unity certificate of Proposition 2.4 propagates only to multiples of a base modulus $L > 1$, so any finite collection of such certificates misses infinitely many indices. Theorem 6.3 strengthens this decisively: for n prime, *no* constant-weight block-circulant matrix in $\mathcal{S}(P(n, 3))$ has nullity 8, whatever weights are chosen and whether or not they are rational. Since the primes are infinite, even an infinite family of certificates of this type cannot establish (3). Thus a maximum-nullity

proof covering prime levels must leave the present constant-weight block-circulant class—for example by allowing edge weights to vary with the vertex index—or use a different family of graph-described matrices. A direct zero-forcing lower bound would of course bypass maximum nullity entirely. This answers negatively the question of whether the present constant-weight mode-selection construction can produce certificates for every sufficiently large n.

Open problems.

Question 9.1. Is $M(P(n,3)) = 8$ for every $n \geq 13$? Corollary 6.3 shows that, for prime n, any witnessing matrix must fall outside the present constant-weight block-circulant class, so the maximum-nullity form of (3) remains open.

Question 9.2. Do periodic (rather than constant) edge weightings help? If $m \mid n$ and the weights are m-periodic, the matrix is block-circulant over $\mathbb{Z}_{n/m}$ with blocks of size $2m$, and the singularity conditions become determinants of $2m \times 2m$ matrices. Does this enlarged class realize moduli beyond $\{10, 24, 28, 42\}$?

Question 9.3. Are $10, 24, 28, 42$ the only minimal moduli that produce new divisibility families in the present real constant-weight certificate class? The computer-assisted search found no additional minimal modulus through 420, but its floating-point screening stage prevents this finite observation from serving as a nonexistence proof. Theorem 6.2 restricts the admissible prime divisors but does not by itself give a finite bound.

Question 9.4. For which integers $k \geq 1$ is Q_k a product of distinct cyclotomic polynomials, equivalently a divisor of $z^L - 1$ for some L?

Reproducibility

The supplementary material contains exact symbolic checks of the determinant identity, the mode-selection expansion, the rational cyclotomic factorizations, the modulus-28 algebraic identity, and the signed certificates. It also contains the finite enumeration used in the rational classification, the computer-assisted modulus search of Section 6.4, and the exhaustive zero-forcing program used for Table 3. No theorem in the paper relies on numerical optimization.

Declarations

Funding. The author received no specific funding for this work.
Competing interests. The author declares no competing interests.
Data and code availability. No external dataset is used; the supplementary scripts accompany the manuscript.

References

[1] AIM Minimum Rank–Special Graphs Work Group, *Zero forcing sets and the minimum rank of graphs*, Linear Algebra Appl. **428** (2008), no. 7, 1628–1648, https://doi.org/10.1016/j.laa.2007.10.009.

[2] J. S. Alameda, E. Curl, A. Grez, L. Hogben, O. Kingston, A. Schulte, D. Young, and M. Young, *Families of graphs with maximum nullity equal to zero forcing number*, Spec. Matrices **6** (2018), no. 1, 56–67, https://doi.org/10.1515/spma-2018-0006.

[3] F. Barioli, W. Barrett, S. M. Fallat, H. T. Hall, L. Hogben, B. L. Shader, P. van den Driessche, and H. van der Holst, *Zero forcing parameters and minimum rank problems*, Linear Algebra Appl. **433** (2010), no. 2, 401–411, https://doi.org/10.1016/j.laa.2010.03.008.

[4] P. J. Davis, *Circulant Matrices*, 2nd ed., AMS Chelsea Publishing, Providence, RI, 1994.

[5] L. Duong, B. K. Kroschel, M. Riddell, K. N. Vander Meulen, and A. Van Tuyl, *Maximum nullity and zero forcing of circulant graphs*, Spec. Matrices **8** (2020), no. 1, 221–234, https://doi.org/10.1515/spma-2020-0106.

[6] S. M. Fallat and L. Hogben, *The minimum rank of symmetric matrices described by a graph: A survey*, Linear Algebra Appl. **426** (2007), no. 2–3, 558–582, https://doi.org/10.1016/j.laa.2007.05.036.

[7] R. Gera and P. Stănică, *The spectrum of generalized Petersen graphs*, Australas. J. Combin. **49** (2011), 39–45.

[8] A. Krishnan, *A correction to the zero forcing number of the generalized Petersen graphs* $P(n, 3)$, arXiv:2607.19412 (2026), https://doi.org/10.48550/arXiv.2607.19412.

[9] T. Y. Lam and K. H. Leung, *On vanishing sums of roots of unity*, J. Algebra **224** (2000), no. 1, 91–109, https://doi.org/10.1006/jabr.1999.8089.

[10] S. Rashidi, N. Shajareh Poursalavati, and M. Tavakkoli, *Computing the zero forcing number for generalized Petersen graphs*, J. Algebra Comb. Discrete Struct. Appl. **7** (2020), no. 2, 183–193, https://doi.org/10.13069/jacodesmath.729465.

[11] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Graduate Texts in Mathematics **83**, Springer, New York, 1997.

[12] M. E. Watkins, *A theorem on Tait colorings with an application to the generalized Petersen graphs*, J. Combin. Theory **6** (1969), no. 2, 152–164, https://doi.org/10.1016/S0021-9800(69)80116-X.

[13] D. Young, *Techniques for determining equality of the maximum nullity and the zero forcing number of a graph*, Electron. J. Linear Algebra **37** (2021), 295–315, https://doi.org/10.13001/ela.2021.4967.

Independent Researcher
Email address: mhbamdm@gmail.com
URL: https://orcid.org/0009-0001-8170-8179