Generalized Spectral Characterization of Graphs Revisited

Wei Wang*

School of Mathematics and Statistics
Xi'an Jiaotong University
Xi'an, P.R. China.

wang_weiw@mail.xjtu.edu.cn

Submitted: Sep 24, 2013; Accepted: Sep 27, 2013; Published: Oct 21, 2013
Mathematics Subject Classifications: 05C50

Abstract

A graph G is said to be *determined by its generalized spectrum* (DGS for short) if for any graph H, H and G are cospectral with cospectral complements implies that H is isomorphic to G. Wang and Xu (2006) gave some methods for determining whether a family of graphs are DGS. In this paper, we shall review some of the old results and present some new ones along this line of research.

More precisely, let A be the adjacency matrix of a graph G, and let $W = [e, Ae, \cdots, A^{n-1}e]$ (e is the all-one vector) be its *walk-matrix*. Denote by $\mathcal{G}_n$ the set of all graphs on n vertices with $\det(W) \neq 0$. We define a large family of graphs

$$\mathcal{F}_n = \{G \in \mathcal{G}_n | \frac{\det(W)}{2^{\lfloor n/2 \rfloor}} \text{ is square-free and } 2^{\lfloor n/2 \rfloor + 1} \nmid \det(W)\}$$

(which may have positive density among all graphs, as suggested by some numerical experiments). The main result of the paper shows that for any graph $G \in \mathcal{F}_n$, if there is a rational orthogonal matrix Q with $Qe = e$ such that $Q^T AQ$ is a (0,1)-matrix, then $2Q$ must be an integral matrix (and hence, Q has well-known structures). As a consequence, we get the conclusion that almost all graphs in $\mathcal{F}_n$ are DGS.

Keywords: Spectra of graphs; Cospectral graphs; Determined by spectrum

1 Introduction

Throughout the paper, we are only concerned with simple graphs. Let G be a simple graph with (0,1)-adjacency matrix A. *The spectrum* of G consists of all the eigenvalues

*Supported by National Natural Science Foundation of China 11071191.

(together with their multiplicities) of the matrix A. The spectrum of G together with that of its complement will be referred to as *the generalized spectrum* of G in the paper. For some terms and terminologies on graph spectra, see [1].

A graph G is said to be *determined by its spectrum* (DS for short), if any graph having the same spectrum as G is necessarily isomorphic to G (of course, the spectrum concerned should be specified).

The spectrum of a graph encodes useful combinatorial information about the given graph, and the relationship between the structural properties of a graph and its spectrum has been studied extensively over many years. A fundamental question in Spectral Graph Theory is: " Which graphs are DS?" The problem dates back to more than 50 years ago and originates from Chemistry, which has received a lot of attention from researchers in recent years. It turns out that, however, determining what kinds of graphs are DS is generally a very hard problem. For the background and some known results about this problem, we refer the reader to [2, 3] and the references therein.

In [5, 6], Wang and Xu gave a method for determining whether a graph G is determined by its generalized spectrum (DGS for short), by using some arithmetic properties of the walk-matrix associated with the given graph. In this paper, we review some of the previous results and further present some new results along this line of research, which significantly improves the results in [5, 6]. The new ingredient of the paper is the discovery that whether the determinant of the walk-matrix is square-free (for odd primes) is closely related to whether G is DGS.

The paper is organized as follows: In the next section, we review some previous results that will be needed in the sequel. In Section 3, we give a simple criterion for excluding odd primes. The case $p = 2$ is discussed in Section 4. Conclusions and open problems are given in Section 5.

2 Preliminaries

For convenience of the reader, in this section, we will briefly review some known results from [5, 6].

Let $W = [e, Ae, \cdots, A^{n-1}e]$ (e is the all-one vector) be the *walk-matrix* of a graph G. Then the (i, j)-th entry of W is the number of walks of G starting from vertex i with length $j - 1$. A graph G is called *controllable graph* if W is non-singular (see also [4]). It turns out that the arithmetic properties of $\det(W)$ is closely related to wether G is DGS or not, as we shall see later. Denote by $\mathcal{G}_n$ the set of all controllable graphs on n vertices. The following theorem lies at the heart of our discussions.

Theorem 1 (Wang and Xu [5])**.** *Let $G \in \mathcal{G}_n$. Then there exists a graph H that is cospectral with G w.r.t. the generalized spectrum if and only if there exists a rational orthogonal matrix Q such that $Q^T A(G)Q = A(H)$ and $Qe = e$.*

Define

$$\mathcal{Q}_G = \left\{ \begin{array}{c} Q \textit{ is a rational} \\ \textit{orthogonal matrix} \end{array} \middle| \begin{array}{c} Qe = e,\ Q^T A(G)Q \textit{ is a symmetric} \\ (0,1) - \textit{matrix with zero diagonal} \end{array} \right\},$$

where e is the all-one vector. The following theorem follows easily from Theorem 1.

Theorem 2 (Wang and Xu [5]). *Let $G \in \mathcal{G}_n$. Then G is DGS iff the set $\mathcal{Q}_G$ contains only permutation matrices.*

By the theorem above, in order to determine whether a given graph $G \in \mathcal{G}_n$ is DGS or not, we have to determine those Q in $\mathcal{Q}_G$ explicitly. At first glance, this seems to be as difficult as the original problem. However, we manage to do so by introducing the following useful notion.

The *level* of a rational orthogonal matrix Q with $Qe = e$ is the smallest positive integer ℓ such that ℓQ is an integral matrix. Clearly, ℓ is the least common denominator of all the entries of the matrix Q. If $\ell = 1$, then Q is a permutation matrix.

Determining $\mathcal{Q}_G$ for all $G \in \mathcal{G}_n$ seems too ambitious. Next, we shall only consider those controllable graphs G such that the level of those $Q \in \mathcal{Q}_G$ equals either 1 or 2.

To illustrate the methods in [5, 6], first we give the relationships between the values of ℓ for matrices $Q \in \mathcal{Q}_G$ and properties of the walk-matrix W of G. Recall that an $n \times n$ matrix U with integer entries is called *unimodular* if $det(U) = \pm 1$. *The Smith Normal Form* (SNF in short) of an integral matrix M is of the form $diag(d_1, d_2, \cdots, d_n)$, where d_i is the i^{th} *elementary divisor* of the matrix M and $d_i | d_{i+1}$ $(i = 1, 2, \cdots, n-1)$ hold. It is well known that for every integral matrix M with full rank, there exist unimodular matrices U and V such that $M = USV = U diag(d_1, d_2, \cdots, d_n)V$, where S is the SNF of the matrix M. For a graph $G \in \mathcal{G}_n$, it is not difficult to show that d_n is the smallest positive integer ℓ such that ℓW^{-1} is an integral matrix.

Theorem 3 (Wang and Xu [5], Exclusion Criterion). *Let W be the walk-matrix of a graph $G \in \mathcal{G}_n$, and $Q \in \mathcal{Q}_G$ with level ℓ. Then we have:*
(a) $\ell | d_n$, where d_n is the n^{th} elementary divisor of the SNF of W.
(b) Let p be any prime factor of d_n. If $p | \ell$, then the following system of congruence equations must have a non-trivial solution ($x \not\equiv 0$ mod p).

$$W^T x \equiv 0, \ x^T x \equiv 0 \ (mod\ p). \tag{1}$$

Theorem 3 (a) shows that ℓ is a divisor of d_n, and hence all possible values of ℓ are finite for a given graph in $\mathcal{G}_n$ and can be effectively computed through calculating the SNF of W. While (b) shows that not all of the divisors of d_n can be a divisor of ℓ; let p be any prime factor of $d_n(G)$ and if (1) has no non-trivial solution, then p must not be a prime factor of ℓ, and it can be excluded from further consideration. Using this way, it can be expected that in most cases, many possibilities of the values of the divisors of d_n can be excluded.

Now we show how to check whether Eq. (1) has only trivial solutions. As an illustration, we shall restrict ourselves to the simplest case.

For convenience, we work with the finite field $\mathbf{F}_p$ in what follows. Suppose that $rank_p(W) = n-1$, where $rank_p(W)$ is the rank of W over the finite field $\mathbf{F}_p$. Consider the first equation of Eq. (1) as a system of linear equations over $\mathbf{F}_p$, then the set of solutions to the first equation of (1) forms a one-dimensional subspace of $\mathbf{F}_p^n$. We can write $x = k\xi$, for some $0 \neq \xi \in \mathbf{F}_p^n$ and $k = 0, \cdots, p-1$. So Eq. (1) has only trivial solution iff

$$\xi^T \xi \neq 0 \ in \ \mathbf{F}_p. \tag{2}$$

Let us give two examples which are taken from [6].

Let G_1 and G_2 be two graphs with the adjacency matrices being given as follows. It can easily be computed that $d_{12}(G_1) = 2 \cdot 17 \cdot 67 \cdot 8054231$, and $\xi^T \xi = 12, 25$ and 1492735 for each prime $p = 17, 67$ and 8054231 respectively, where ξ is defined as above. Thus, all the prime factors of $d_{12}(G_1)$ can be excluded except for $p = 2$. It can be computed that $d_{13}(G_2) = 2 \cdot 3^2 \cdot 5 \cdot 197 \cdot 263 \cdot 5821$, and $\xi^T \xi = 1, 0, 139, 101$ and 4298 for each prime $p = 3, 5, 197, 263$ and 5821. So all the prime factors of $d_{13}(G_2)$ can be excluded except for $p = 2, 5$.

$$\begin{bmatrix}
0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\
1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\
1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\
1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\
1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0
\end{bmatrix}
\quad
\begin{bmatrix}
0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\
1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\
0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\
1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\
1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\
0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\
0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\
1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\
0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\
1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0
\end{bmatrix}.$$

Nevertheless, it is not difficult to show that $p = 2$ is always a prime factor of d_n and cannot be excluded invariably. In [6], some further exclusion criterions are proposed to eliminate the possibility of $p = 2$. It can be show that $p = 2$ can be excluded for both graphs G_1 and G_2, by using the methods in [6]. Therefore G_1 is DGS. However, we do not know wether G_2 is DGS or not since $p = 5$ cannot be excluded using the existing method.

In the next section, we shall present a simple criterion for excluding primes $p > 2$.

3 A simple exclusion criterion for $p > 2$

In this section, we give a simple criterion for excluding primes $p > 2$, in terms of whether the exponent of p in $\det(W)$ is larger than one. The main result of this section is the following

Theorem 4. *Let $G \in \mathcal{G}_n$, $Q \in \mathcal{Q}_G$ with level ℓ, and p an odd prime. If $p | \det(W)$ and $p^2 \not| \det(W)$, then p cannot be a divisor of ℓ.*

Before presenting the proof of above theorem, we need several lemmas below. Note that the assumption that $p | \det(W)$ and $p^2 \not| \det(W)$ imply that $rank_p(W) = n - 1$. This fact will be used frequently in the sequel.

Lemma 5. *Let $G \in \mathcal{G}_n$, $Q \in \mathcal{Q}_G$ with level ℓ. Let p be an odd prime divisor of ℓ. Assume that $rank_p(W) = n-1$. Then we must have $rank_p(\ell Q) = 1$, and the following congruence equation has a solution z:*

$$Az \equiv \lambda_0 z,\ \ e^T z \equiv 0, z^T z \equiv 0,\ \ z \not\equiv 0\ (mod\ p) \tag{3}$$

for some integer λ_0.

Proof. The lemma follows immediately from the proof of the next lemma. □

Lemma 6. *Let $G \in \mathcal{G}_n$, $Q \in \mathcal{Q}_G$ with level ℓ. Let p be an odd prime divisor of ℓ. Assume that $rank_p(W) = n-1$ and $rank_p(\ell Q) = 1$, and the following congruent equation has a solution z:*

$$W^T z \equiv 0,\ \ z^T z \equiv 0,\ \ z \not\equiv 0\ (mod\ p), \tag{4}$$

Then $z^T Az \equiv \lambda_0 z^T z\ (mod\ p^2)$ holds, where λ_0 is an integer such that $Az \equiv \lambda_0 z\ (mod\ p)$ holds .

Proof. First we claim that there exists a column u of the integer matrix ℓQ and an integer vector β such that

$$u = z + p\beta; \tag{5}$$

$$u^T Au \equiv 0\ (\mathrm{mod}\ p^2); \tag{6}$$

$$u^T u \equiv 0\ (\mathrm{mod}\ p^2). \tag{7}$$

In fact, it is easy to see that there exists a column u of ℓQ such that $u \not\equiv 0\ (mod\ p)$. With such a u, we have $W^T u \equiv 0\ (\mathrm{mod}\ p), u^T u = \ell^2 \equiv 0\ (\mathrm{mod}\ p^2)$, and $u^T Au = 0$. So u is a solution of Eq. (4), and Eq. (5) holds for some integer β.

By Eq. (7) we have

$$(z + p\beta)^T (z + p\beta) \equiv z^T z + 2pz^T \beta \equiv 0\ (\mathrm{mod}\ p^2).$$

Since $Q \in \mathcal{Q}_G$, we get $Q^T AQ = B$, where B is the adjacency matrix of some graph H. By $AQ = QB$ we get

$$Au_i = \sum_{k=1}^{n} b_{ik} u_k, i = 1, 2, \cdots, n,$$

where u_i is the i-th column of ℓQ. Note that $rank_p(\ell Q) = 1$. Taking *mod p* on both sides of the equation above that contains u on the right side generates $Az \equiv \lambda_0 z\ (\mathrm{mod}\ p)$, for some integer λ_0.

Let $Az = \lambda_0 z + p\gamma$, where γ is an integer vector. Then it follows from Eq. (5) and (6) that

$$\begin{array}{rcl} (z + p\beta)^T A(z + p\beta) & \equiv & z^T Az + 2pz^T A\beta \\ & = & z^T (\lambda_0 z + p\gamma) + 2p(\lambda_0 z + p\gamma)^T \beta \\ & \equiv & \lambda_0 (z^T z + 2pz^T \beta) + pz^T \gamma \\ & \equiv & pz^T \gamma \\ & \equiv & 0\ (\mathrm{mod}\ p^2) \end{array}$$

Thus we have $z^T (Az - \lambda_0 z) = pz^T \gamma \equiv 0\ (\mathrm{mod}\ p^2)$. This completes the proof. □

Lemma 7. *Let $M = Udiag(d_1, d_2, \cdots, d_n)V = USV$, where S is the SNF of M, U and V are unimodular matrices and $d_i | d_{i+1}$ for $i = 1, 2, \cdots, n-1$. Then the system of congruence equations $Mx \equiv 0 \pmod{p^2}$ has a solution $x \not\equiv 0 \pmod{p}$ if and only if $p^2 | d_n$.*

Proof. The equation $Mx \equiv 0 \pmod{p^2}$ is equivalent to $diag(d_1, d_2, \cdots, d_n)Vx \equiv 0 \pmod{p^2}$. Let $Vx = y$. Consider $diag(d_1, d_2, \cdots, d_n)y \equiv 0 \pmod{p^2}$. If $p^2 | d_n$, let $y = (0, 0, \cdots, 0, 1)^T$, then $x = V^{-1}y \not\equiv 0 \pmod{p}$ is a required solution to the original congruence equation. On the other hand, it is easy to see if $p^2 \nmid d_n$, then the equation has no solution x with $x \not\equiv 0 \pmod{p}$. □

As a simple consequence of the above lemma, we have

Corollary 8. *Suppose that $rank_p(W) = n - 1$, and $W^T z \equiv 0, z \not\equiv 0 \pmod{p}$. If there exists an integer vector x such that $W^T x \equiv \frac{W^T z}{p} \pmod{p}$, then $p^2 | \det(W)$.*

Lemma 9. *If $rank_p(W) = n - 1$, then we always have $rank_p(A - \lambda_0 I) \geqslant n - 2$.*

Proof. For contrary, suppose that there exist three vectors z, u and v which are linearly independent over $\mathbf{F}_p$ such that $(A - \lambda_0 I)z = 0, (A - \lambda_0 I)u = 0$ and $(A - \lambda_0 I)v = 0$, where we assume without loss of generality that $e^T z = 0$, $e^T u \neq 0$ and $e^T v \neq 0$. Then we can choose integers k and l with $ke^T u + le^T v = 0$, over $\mathbf{F}_p$. Let $w = ku + lv$. Then $e^T A^i w = 0$ and hence $W^T w = 0$ and $W^T z = 0$, which implies that $rank_p(W) \leqslant n - 2$, which contradicts the assumption that $rank_p(W) = n - 1$. □

It follows from Lemma 9 that $rank_p(A - \lambda_0 I) = n - 1$ or $n - 2$. Next, we shall distinguish this two cases in the following lemmas.

Lemma 10. *If $rank_p(A - \lambda_0 I) = n - 1$, then $p^2 | \det(W)$.*

Proof. Let z be an integral vector with $W^T z \equiv 0 \pmod{p}$. We prove the lemma by showing that the following congruence equation always has a solution x.

$$W^T x \equiv \frac{W^T z}{p} \pmod{p}. \tag{8}$$

Note that $z^T e = 0$ and $z^T (A - \lambda_0 I) = 0$, over $\mathbf{F}_p$. It follows that the all-one vector e can be written as the linear combinations of the columns of $A - \lambda_0 I$, i.e., there exists a column vector u such that

$$e = (A - \lambda_0 I)u, \text{ over } \mathbf{F}_p \tag{9}$$

It follows from Eq. (9) that there exists an integer vector β such that

$$e = (A - \lambda_0 I)u + p\beta. \tag{10}$$

Thus, we have

$$\begin{aligned} W &= [e, Ae, \cdots, A^{n-1}e] \\ &= [(A - \lambda_0 I)u + p\beta, A((A - \lambda_0 I)u + p\beta), \cdots, A^{n-1}((A - \lambda_0 I)u + p\beta)] \\ &= (A - \lambda_0 I)[u, Au, \cdots, A^{n-1}u] + p[\beta, A\beta, \cdots, A^{n-1}\beta] \\ &= (A - \lambda_0 I)X + p[\beta, A\beta, \cdots, A^{n-1}\beta], \end{aligned}$$

where $X := [u, Au, \cdots, A^{n-1}u]$.

It follows that

$$W^T z = X^T (A - \lambda_0 I) z + p[z^T \beta, z^T A\beta, \cdots, z^T A^{n-1}\beta]^T. \tag{11}$$

Since $W^T z \equiv 0, (A - \lambda_0 I)z \equiv 0,\ A^i z \equiv \lambda_0^i z\ (i = 0, 1, \cdots, n-1) \pmod p$, by Eq. (11) we have

$$\frac{W^T z}{p} \equiv X^T \frac{(A - \lambda_0 I)z}{p} + z^T \beta [1, \lambda_0, \cdots, \lambda_0^{n-1}]^T \pmod p. \tag{12}$$

Moreover, it follows from the fact that $rank_p(A - \lambda_0 I) = n - 1$, $z^T(A - \lambda_0 I) = 0$ and $z^T z = 0$, over $\mathbf{F}_p$, that z can be written as the linear combinations of the columns of $A - \lambda_0 I$, i.e., there exists a vector y such that $z = (A - \lambda_0 I)y$.

It is easy to show that $W^T y \equiv e^T y[1, \lambda_0, \cdots, \lambda_0^{n-1}]^T \pmod p$. In fact, this follows from the following congruence equations:

$$\begin{aligned} z &\equiv (A - \lambda_0 I)y \pmod p, \\ e^T Ay &\equiv \lambda_0 e^T y + e^T z \equiv \lambda_0 e^T y \pmod p, \\ &\cdots\cdots \\ e^T A^{n-1} y &\equiv \lambda_0^{n-1} e^T y \pmod p. \end{aligned}$$

Now we show that $e^T y \not\equiv 0 \pmod p$. For otherwise, if $e^T y \equiv 0 \pmod p$, then it follows that $W^T y = 0$ over $\mathbf{F}_p$. Note that $W^T z = 0$ over $\mathbf{F}_p$. Moreover, y and z are linearly independent. It follows that $rank_p(W) \leqslant n - 2$, which contradicts the fact that $rank_p(W) = n - 1$.

Thus, there exists an integer k such that

$$z^T \beta \equiv k e^T y \pmod p, \tag{13}$$

Moreover, it follows from the facts that $z^T \frac{(A-\lambda_0 I)z}{p} \equiv 0,\ z^T(A - \lambda_0 I) \equiv 0, \pmod p$ and $rank_p(A - \lambda_0 I) = n - 1$ that the vector $\frac{(A-\lambda_0 I)z}{p}$ can be written as the linear combinations of the columns of $A - \lambda_0 I$, i.e., there exists a vector v such that

$$\frac{(A - \lambda_0 I)z}{p} \equiv (A - \lambda_0 I)v.$$

Note that $W^T \equiv X^T(A - \lambda_0 I) \pmod p$. Therefore, we have

$$\begin{aligned} \frac{W^T z}{p} &\equiv X^T \frac{(A - \lambda_0 I)z}{p} + kW^T y \\ &\equiv W^T v + kW^T y \\ &\equiv W^T(v + ky) \qquad \pmod p. \end{aligned}$$

By Cor. 8, the lemma follows. □

Lemma 11. *Let $rank_p(W) = n-1$. Suppose that $rank_p(A-\lambda_0 I) = n-2$. Then $rank_p([A-\lambda_0 I, z]) = n-1$.*

Proof. Since $rank_p(A-\lambda_0 I) = n-2$, there are two vectors z and y which are linearly independent such that $Az = \lambda_0 z$ and $Ay = \lambda_0 y$ with $e^T z = 0$, over $\mathbf{F}_p$.

Suppose the lemma does not hold. Then we have that z can be written as the linear combinations of the columns of $A - \lambda_0 I$. Thus, there exists a vector x such that $z = (A-\lambda_0 I)x$, i.e.,

$$Ax = z + \lambda_0 x,$$

$$A^2 x = Az + \lambda_0 z + \lambda_0^2 x,$$

$$\cdots\cdots$$

$$A^{n-1}x = A^{n-2}z + \lambda_0 A^{n-3}z + \cdots + \lambda_0^{n-3}Az + \lambda_0^{n-2}z + \lambda_0^{n-1}x.$$

Now choose k and l, not all zero, such that $e^T w = 0$, where $w = kx + ly$.

Then, we have

$$e^T A^i w = ke^T A^i x + le^T A^i y = ke^T(A^i z + \lambda_0 A^{i-1}z + \cdots + \lambda_0^{i-1}Az + \lambda_0^{i-1}z) + \lambda_0^i(ke^T x + le^T y) = 0,$$

for $i = 0, 1, \cdots, n-1$, i.e., $W^T w = 0$.

Now we show that x, y and z are linearly independent. Suppose $ax + by + cz = 0$. Then left-multiplying both sides of the above equality by $(A - \lambda_0 I)$ gives $az = 0$, which implies $a = 0$. By assumption that y and z are linearly independent, we have $b = c = 0$.

Therefore, z and w are linearly independent. Moreover, we have $W^T z = 0$ and $W^T w = 0$. This contradicts the fact that $rank_p(W) = n-1$. □

Lemma 12. *Suppose that $rank_p(A-\lambda_0 I) = n-2$. Then $p^2 | det(W)$*

Proof. Note that $rank_p(W) = n-1$ and $rank_p(A-\lambda_0 I) = n-2$. By Lemma 11, we get that z cannot be expressed as the linear combinations of the column vectors of $A - \lambda_0 I$, over $\mathbf{F}_p$, and hence $rank_p([A-\lambda_0, z]) = n-1$. Moreover, $z^T e = 0$ and $z^T[A-\lambda_0 I, z] = 0$, it follows that the all-one vector e can be expressed as the linear combinations of the column vectors of $A - \lambda_0 I$ and z, i.e., there exist an vector u and an integer k such that

$$e = (A-\lambda_0 I)u + kz, \ \textit{over } \mathbf{F}_p.$$

That is,

$$e = (A-\lambda_0 I)u + kz + p\beta, \ \textit{over } \mathbf{Z}.$$

It follows that

$$\begin{aligned}
Ae &= A(A-\lambda_0 I)u + kAz + pA\beta = (A-\lambda_0 I)Au + kAz + pA\beta. \\
A^2 e &= A^2(A-\lambda_0 I)u + kA^2 z + pA^2\beta = (A-\lambda_0 I)A^2 u + kA^2 z + pA^2\beta. \\
&\cdots\cdots\cdots\cdots\cdots \\
A^{n-1}e &= A^{n-1}(A-\lambda_0 I)u + kA^{n-1}z + pA^{n-1}\beta = (A-\lambda_0 I)A^{n-1}u + kA^{n-1}z + pA^{n-1}\beta.
\end{aligned}$$

Therefore,

$$\begin{aligned} W &= [e, Ae, \cdots, A^{n-1}e] \\ &= (A-\lambda_0 I)[u, Au, \cdots, A^{n-1}u] + k[z, Az, \cdots, A^{n-1}z] + p[\beta, A\beta, \cdots, A^{n-1}\beta] \\ &= (A-\lambda_0 I)X + k[z, Az, \cdots, A^{n-1}z] + p[\beta, A\beta, \cdots, A^{n-1}\beta], \ over\ \mathbf{Z}, \end{aligned}$$

where $X = [u, Au, \cdots, A^{n-1}u]$. It follows that

$$\begin{aligned} \frac{W^T z}{p} &= X^T \frac{(A-\lambda_0 I)z}{p} + k[\frac{z^T z}{p}, \frac{z^T Az}{p}, \cdots, \frac{z^T A^{n-1} z}{p}]^T \\ &+ [\beta^T z, \cdots, \beta^T A^{n-1} z]^T \ \ (over\ \mathbf{Z}) \\ &\equiv X^T \frac{(A-\lambda_0 I)z}{p} + k\frac{z^T z}{p}[1, \lambda_0, \cdots, \lambda_0^{n-1}]^T + \beta^T z[1, \lambda_0, \cdots, \lambda_0^{n-1}]^T \pmod p \end{aligned}$$

The congruence equation follows from the facts that $\frac{z^T A^i z}{p} - \frac{\lambda_0^i z^T z}{p} \equiv 0$ and $A^i z \equiv \lambda_0^i z \pmod p$.

Moreover, $z^T \frac{(A-\lambda_0 I)z}{p} \equiv 0$ and $z^T[A-\lambda_0 I, z] \equiv 0 \pmod p$. It follows that there exist a vector α and an integer m such that

$$\frac{(A-\lambda_0 I)z}{p} \equiv (A-\lambda_0 I)\alpha + mz \pmod p \tag{14}$$

$$\begin{aligned} X^T \frac{(A-\lambda_0 I)z}{p} &\equiv X^T(A-\lambda_0 I)\alpha + mX^T z \\ &\equiv W^T\alpha - kz^T\alpha[1, \lambda_0, \cdots, \lambda_0^{n-1}]^T + mX^T z \\ &\equiv W^T\alpha + (mu^T z - kz^T\alpha)[1, \lambda_0, \cdots, \lambda_0^{n-1}]^T \pmod p \end{aligned}$$

Thus

$$\frac{W^T z}{p} \equiv W^T\alpha + (k\frac{z^T z}{p} + \beta^T z + mu^T z - kz^T\alpha)[1, \lambda_0, \cdots, \lambda_0^{n-1}]^T \pmod p \tag{15}$$

Let y be a vector with $(A-\lambda_0)y = 0$ that is linearly independent with z. Then we must have $e^T y \not\equiv 0 \pmod p$. For otherwise, if $e^T y \equiv 0 \pmod p$, then it follows $W^T y \equiv 0$. Note $W^T z = 0$, $W^T y = 0$ and y and z are linearly independent, over $\mathbf{F}_p$. This contradicts the fact that $rank_p(W) = n-1$.

It follows that there exists an integer l such that

$$k\frac{z^T z}{p} + \beta^T z + mu^T z - kz^T\alpha \equiv le^T y \pmod p.$$

Thus, we have

$$\frac{W^T z}{p} \equiv W^T\alpha + le^T y[1, \lambda_0, \cdots, \lambda_0^{n-1}]^T \equiv W^T\alpha + lW^T y \equiv W^T(\alpha + ly) \pmod p \tag{16}$$

By Cor. 8, the lemma follows. □

Now, we are ready to present the proof of Theorem 4.

Proof of Theorem 4. Combining Lemmas 5-7,9-12 and Cor. 8, Theorem 4 follows immediately. $\square$

Let us give a few remarks to end this section.

i) Result in Theorem 4 is the best possible in the sense that if $p > 2$ has exponent larger than one, then Theorem 4 may not be true. The following is a counterexample.

Let the adjacency matrix of graph G be given as below. It can easily be computed that

$$det(W) = 2^6 \times 3^2 \times 157 \times 1361 \times 2237.$$

The exponent of $p = 3$ in the standard prime decomposition $det(W)$ is equal to 2, and $p = 3$ cannot be excluded. Actually, let Q be a rational orthogonal matrix given as below. Then $Q \in \mathcal{Q}_G$ with level $\ell = 3$, since it can be easily verified that $Q^T A Q$ is a $(0, 1)$-matrix.

$$A = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \end{bmatrix},$$

$$Q = \frac{1}{3} \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 & 0 & 0 \\ 2 & -1 & -1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 \\ 1 & 1 & 1 & 2 & -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 2 & -1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & -1 & 2 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & -1 & 2 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 \\ 1 & 1 & 1 & -1 & -1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

ii) By Theorem 4, for graph G_2 in the previous example, $p = 5$ can also be excluded since the $5 | \det(W)$ and $5^2 \nmid \det(W)$. Thus, G_2 is also DGS.

4 Some discussions on $p = 2$

As mentioned previously, the case $p = 2$ is more involved to deal with. Let us try to explain this through the following lemmas.

Lemma 13 (c.f. Wang [7]). *$e^T A^k e$ is even for every positive integer k.*

Proof. Note that

$$e^T A^k e = Tr(A^k) + \sum_{i \neq j} A^k = Tr(A^k) + 2\sum_{i<j} A^k \equiv Tr(A^k) \pmod 2.$$

$Tr(A^k) = Tr(AA^{k-1}) = \sum_{i,j} a_{ij}b_{ij} = 2\sum_{i<j} a_{ij}b_{ij}$, where $B := A^{k-1}$. Thus the lemma follows. $\square$

Lemma 14 (c.f. Wang [7]). *$rank_2(W) \leqslant \lceil \frac{n}{2} \rceil$.*

Proof. Suppose n is even. Then it follows from Lemma 4.1 that $W^T W = 0$ over $\mathbf{F}_2$. $2rank_2(W) = rank_2(W^T) + rank_2(W) \leqslant n$. Thus we have $rank_2(W) \leqslant n/2 = \lceil \frac{n}{2} \rceil$.

If n is odd. Let $\hat{W}$ be the matrix obtained from W by deleting the first column. Then $W^T \hat{W} = 0$ over $\mathbf{F}_2$. Note $rank_2(W) + rank_2(\hat{W}) \leqslant n$ and $rank_2(\hat{W}) \geqslant rank_2(W) - 1$. It follows that $rank_2(W) \leqslant (n+1)/2 = \lceil \frac{n}{2} \rceil$. $\square$

By Lemma 14, the system of linear equations in Eq. (1) has a set of solutions with dimension at least $\lfloor n/2 \rfloor$, and it not difficult to show that it is always possible to choose some of the solutions to meet the second requirement in Eq. (1).

Moreover, by Lemma 14, the following corollary follows immediately.

Corollary 15. *Let $\det(W) = \epsilon 2^{\alpha} p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ ($\epsilon = \pm 1$) be the standard decomposition of $det(W)$ into prime factors . Then $\alpha \geqslant \lfloor \frac{n}{2} \rfloor$.*

For any graph $G \in \mathcal{G}_n$, the number of d_i which is even in the SNF $S = diag(d_1, d_2, \cdots, d_n)$ of W must be at leat $\lfloor n/2 \rfloor$. Next, we are interested in a specific family of controllable graphs

$$\mathcal{F}_n = \{G \in \mathcal{G}_n | \frac{\det(W)}{2^{\lfloor n/2 \rfloor}} \text{ is square-free and } 2^{\lfloor n/2 \rfloor + 1} \not| \det(W)\}.$$

By Cor. 15, for every graph in $\mathcal{F}_n$, the SNF of W must be like $S = diag(1, \cdots, 1, 2, \cdots, 2, 2b)$, where b is an odd square-free integer and the number of 2's is exactly $\lfloor n/2 \rfloor$ in the diagonal of W.

Let $G \in \mathcal{F}_n$. Let $Q \in \mathcal{Q}_G$ with level ℓ and p be any prime divisor of ℓ. Then by Theorem 3 (a), we have $p | 2b$. If $p > 2$, then by Theorem 4, we have $p \not| \ell$. Therefore, $\ell = 1$ or $\ell = 2$. Next, we present a simple exclusion criterion for $\ell = 2$, which significantly simplifies the method in [6].

Lemma 16. *Let $G \in \mathcal{G}_n$. Let $Q \in \mathcal{Q}_G$ with level $\ell = 2$. Then there exists a (0,1)-vector u with four non-zero entries '1' such that*

$$u^T A^k u \equiv 0 \ (mod\ 4)\ , k = 1, 2, \cdots, n-1. \tag{17}$$

Moreover, u satisfies $W^T u \equiv 0, u \not\equiv 0 \ (mod\ 2)$

Proof. $Q \in \mathcal{Q}_G$ implies that $Q^T A Q = B$, where B is a (0,1)-matrix. Let $\bar{u}$ be the i-th column of $2Q$. It follows from $Q^T A^k Q = B^k$ that $\bar{u}^T A^k \bar{u} = 4(B^k)_{i,i} \equiv 0 \ (mod\ 4)$. It follows from the facts $\ell = 2$ and $Qe = e$ that the four non-zero entries of $\bar{u}$ are $1, 1, 1$, and -1, respectively. Let $u = \bar{u} + 2e_j$ (e_j denotes the j-th standard basis of $\mathbf{R}^n$) be a $(0,1)$-vector with four non-zero entries '1' . Then

$$u^T A^k u = \bar{u}^T A^k \bar{u} + 4\bar{u}^T A^k e_j + 4e_j^T A^k e_j \equiv 0 \ (\mathrm{mod}\ 4).$$

The last assertion follows from the fact that $Q^T A^k Q = B^k$ and $Qe = e$ imply that $W^T Q$ is an integral matrix. Thus $W^T u \equiv 0, u \not\equiv 0 \ (\mathrm{mod}\ 2)$ holds. □

Lemma 16 gives a simple way to eliminate the possibility of $\ell = 2$. First, solve the system of linear equations $W^T x = 0$ with additional requirement that x has four non-zero entries 1, over $\mathbf{F}_2$, to get a solution set S. This can be done through checking $\binom{n}{4}$ possibilities. Then for each solution x check whether Eq. (17) holds. If every $x \in S$ does not satisfy Eq. (17), then $\ell \neq 2$ and hence $\ell = 1$, i.e., G is DGS.

Let us give an example for illustration. Let $G = G_1$ be the first graph given in Section 2. Clearly $G \in \mathcal{F}_n$. It can be easily computed by Mathematica 5.0 that the corresponding solution set is $S = \{(0,1,0,1,0,1,0,1,0,0,0,0)^T, (0,0,1,0,1,0,1,0,1,0,0,0)^T, (1,0,0,0,1,0,1,0,0,1,0,0)^T, (1,0,1,0,0,0,0,0,1,1,0,0)^T, (1,0,1,0,0,0,1,0,0,0,1,0)^T, (1,0,0,0,1,0,0,0,1,0,1,0)^T, (0,0,1,0,1,0,0,0,0,1,1,0)^T, (0,0,0,0,0,0,1,0,1,1,1,0)^T, (1,0,1,0,1,0,0,0,0,0,0,1)^T, (1,0,0,0,0,0,1,0,1,0,0,1)^T, (0,0,1,0,0,0,1,0,0,1,0,1)^T, (0,0,0,0,1,0,0,0,1,1,0,1)^T, (0,0,0,0,1,0,1,0,0,0,1,1)^T, (0,0,1,0,0,0,0,0,1,0,1,1)^T, (1,0,0,0,0,0,0,0,0,1,1,1)^T\}$

However, none of $x \in S$ satisfies Eq. (17). Thus G is DGS.

We remark, though Lemma 16 is a sufficient condition to exclude the case $\ell = 2$, our numerical experiments do suggest that it is always necessary for graphs $G \in \mathcal{F}_n$.

5 Concluding remarks and open problems

We have reviewed some previous results on the topic of characterizing a graph by both its spectrum and the spectrum of its complement. Then we have presented a simple new exclusion criterion for excluding odd primes. The case $p = 2$ has also been discussed.

As it turns out, the arithmetic properties of $\det(W)$ is closely related to whether a given controllable graphs is DGS. Actually, we have the following

Conjecture (Wang [7]): *Every graph in $\mathcal{F}_n$ is DGS.*

For a given graph $G \in \mathcal{F}_n$, $Q \in \mathcal{Q}_G$ with level ℓ. We have shown that either $\ell = 1$ or $\ell = 2$. However, some additional efforts have to be made to eliminate the possibility of $\ell = 2$.

Finally, we remark that it can be shown (see [8]) that almost every graphs in $\mathcal{F}_n$ is DGS. In view of the simple definition of $\mathcal{F}_n$, it suggests a possible way to show that DGS-graphs have positive density via proving $\mathcal{F}_n$ has positive density (numerical experiments show that $\mathcal{F}_n$ has density nearly 0.2). This needs further investigations in the future.

References

[1] D. M. Cvetković, M. Doob, H. Sachs, *Spectra of Graphs*, Academic Press, NewYork, 1982.

[2] E. R. van Dam, W. H. Haemers, *Which graphs are determined by their spectrum?* Linear Algebra Appl., **373** (2003) 241–272.

[3] E. R. van Dam, W. H. Haemers, *Developments on spectral characterizations of graphs*, Discrete Mathematics, **309** (2009) 576–586.

[4] C.D. Godsil,*Controllable subsets in graphs*, Annals of Combinatorics, **16** (2012) 733–744.

[5] W. Wang, C. X. Xu, *A sufficient condition for a family of graphs being determined by their generalized spectra*, European J. Combin., **27** (2006) 826–840.

[6] W. Wang, C.X. Xu, *An excluding algorithm for testing whether a family of graphs are determined by their generalized spectra, Linear Algebra and its Appl.*, **418** (2006) 62–74.

[7] W. Wang, *On the Spectral Characterization of Graphs*, Phd Thesis, Xi'an Jiaotong University, 2006. (In Chinese)

[8] W. Wang, C.X. Xu, *On the asymptotic behaviors of graphs determined by their generalized spectra*, Discrete Math., **310** (2010) 70–76