ARTICLE IN PRESS

Discrete Mathematics ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Contents lists available at ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

A new arithmetic criterion for graphs being determined by their generalized Q-spectrum[☆]

Lihong Qiu, Yizhe Ji, Wei Wang [*]

School of Mathematics and Statistics, Xi'an Jiaotong University, No. 28 Xianning West Road, Xi'an, 710049, PR China

ARTICLE INFO

Article history:
Received 12 April 2018
Accepted 7 August 2018
Available online xxxx

Keywords:
Spectra of graphs
Cospectral graphs
Determined by spectrum
Q-spectrum

ABSTRACT

"Which graphs are *determined by their spectrum* (DS for short)?" is a fundamental question in spectral graph theory. It is generally very hard to show a given graph to be DS and few results about DS graphs are known in literature. In this paper, we consider the above problem in the context of the generalized Q-spectrum. A graph G is said to be *determined by the generalized Q-spectrum* (DGQS for short) if, for any graph H, H and G have the same Q-spectrum and so do their complements imply that H is isomorphic to G. We give a simple arithmetic condition for a graph being DGQS. More precisely, let G be a graph with adjacency matrix A and degree diagonal matrix D. Let $Q = A + D$ be the *signless Laplacian matrix* of G, and $W_Q(G) = [e, Qe, \dots, Q^{n-1}e]$ (e is the all-ones vector) be the *Q-walk matrix*. We show that if $\frac{\det W_Q(G)}{2^{\lfloor \frac{3n-2}{2} \rfloor}}$ (which is always an integer) is odd and square-free, then G is DGQS.

1. Introduction

Throughout this paper, we are only concerned with *simple graphs*, i.e., undirected graphs without multiple edges and loops. Given a graph G with (0,1)-adjacency matrix $A(G)$ and degree diagonal matrix $D(G)$, *the Laplacian matrix* and *the signless Laplacian matrix* (also called *Q-matrix*) can be defined as $L(G) = D(G) - A(G)$ and $Q(G) = A(G) + D(G)$, respectively. *The spectrum* of G consists of all the eigenvalues (including the multiplicities) of the corresponding matrix associated with G. So we may have adjacency spectrum, Laplacian spectrum, and Q-spectrum, denoted by $\mathrm{Spec}_A(G)$, $\mathrm{Spec}_L(G)$ and $\mathrm{Spec}_Q(G)$, respectively (see [3]).

Two graphs are *cospectral* if they share the same spectrum. A graph G is said to be *determined by the spectrum* (DS for short) if, for any graph H, G and H are cospectral implies that H is isomorphic to G. (Of course, the matrix associated with the graph should be clear from the context.)

"Which graphs are DS?" is a fundamental question in spectral graph theory. The problem dates back to more than 60 years ago and originates from chemistry. In 1956, Günthard and Primas [9] raised the question in a paper that relates the theory of graph spectra to Hückel's theory from chemistry. An analogue of the problem is also asked by Kac [11]: "Can one hear the shape of a drum?". Fisher [10] modelled the shape of the drum by a graph. Then the sound of that drum is characterized by the eigenvalues of the graph. Thus Kac's question is essentially the same as ours.

Another important motivation for the above problem comes from complexity theory. It is still a long standing open question whether graph isomorphism is a hard or an easy problem, despite the recent breakthrough result of Babai [1],

☆ This work is supported by National Natural Science Foundation of China (No. 11471005).
* Corresponding author.
E-mail address: wang_weiw@xjtu.edu.cn (W. Wang).

https://doi.org/10.1016/j.disc.2018.08.008
0012-365X/

claiming a quasipolynomial time algorithm for it. Since checking whether two graphs are cospectral can be done in polynomial time, the focus is on checking isomorphism between cospectral graphs.

Whereas it is comparatively easy to construct pairs of cospectral and non-isomorphic graphs, it is quite challenging to prove a given graph to be DS. Up to now, all the known DS graphs have very special properties, and the techniques (e.g., the eigenvalue interlacing technique) involved in proving them to be DS depend heavily on some special properties of the spectra of these graphs, and cannot be applied to general graphs. For the background and some known results about this problem, we refer the reader to [7,8] and the references therein.

In recent years, Wang and Xu [17,18] and Wang [15,16] considered the above problem in the context of the generalized adjacency spectrum. A graph G is *determined by the generalized adjacency spectrum* (DGAS for short) if, for any graph H, $\mathrm{Spec}_A(G) = \mathrm{Spec}_A(H)$ and $\mathrm{Spec}_A(\bar{G}) = \mathrm{Spec}_A(\bar{H})$ imply that H is isomorphic to G, where $\bar{G}$ and $\bar{H}$ denote the complement of the graphs G and H, respectively. Let $W(G) = [e, Ae, \dots, A^{n-1}e]$ be the *walk-matrix* of G (e is the all-one vector). In [15,16], Wang proved the following elegant result on DGAS graphs:

Theorem 1.1 (*Wang [15,16]*)**.** *If* $\det W(G)/2^{\lfloor n/2\rfloor}$ *(which is always an integer) is odd and square-free, then G is DGAS.*

The main objective of this paper is to show that a similar result holds for *the generalized Q-spectrum*. A graph G is said to be *determined by the generalized Q-spectrum* (DGQS for short) if, for any graph H, $\mathrm{Spec}_Q(G) = \mathrm{Spec}_Q(H)$ and $\mathrm{Spec}_Q(\bar{G}) = \mathrm{Spec}_Q(\bar{H})$ imply that H is isomorphic to G. We mention that it was Cvetković and Simić who initiated the study of Q-spectrum (see [4–6]), since it seems that the Q-spectrum has low spectral uncertainty. Subsequently, there are a few families of graphs that were shown to be DS with respect to the Q-spectrum, see e.g. [12,13,19]. However, all these graphs have special structures and no general result as Theorem 1.1 is known in literature.

Let G be a graph with signless Laplacian matrix Q. Define $W_Q(G) = [e, Qe, \dots, Q^{n-1}e]$ to be its *Q-walk-matrix*. It will soon be clear that $2^{\lfloor \frac{3n-2}{2}\rfloor}$ always divides $\det W_Q(G)$ (see Lemma 3.4) and hence $\det W_Q(G)/2^{\lfloor \frac{3n-2}{2}\rfloor}$ is always an integer.

The main result of the paper is the following

Theorem 1.2. *If* $\det W_Q(G)/2^{\lfloor \frac{3n-2}{2}\rfloor}$ *is odd and square-free, then G is DGQS.*

The main idea of the proof of Theorem 1.2 follows that of Wang [15,16]. It is noticed, however, several new ingenious ideas are needed to make the proof work.

The rest of the paper is organized as follows. In Section 2, we give some preliminary results that will be needed later in the paper. In Section 3, we present the proof of Theorem 1.2. In Section 4, we give some examples of DGQS graphs. Conclusions are given in Section 5.

2. Preliminaries

In this section, we shall give some preliminary results that will be needed later in the paper.

2.1. The main strategy

In this subsection, we shall describe our main strategy to prove a graph to be DGQS, which roughly follows the ideas from [15,16,18]. The following theorem is the starting point of our method, which gives a simple characterization of two graphs sharing the same generalized Q-spectrum. Next, we define e as the all one vector, and the following theorem is the analogue of a result for adjacency matrix obtained by Wang and Xu [18].

Theorem 2.1. *Let G be a graph such that $\det W_Q(G) \neq 0$. There exists H such that G and H are cospectral with respect to the generalized Q-spectrum if and only if there exists a rational orthogonal matrix U such that*

$$U^T Q(G) U = Q(H),\ Ue = e. \tag{1}$$

Proof. Suppose that there exists a rational orthogonal matrix U such that Eq. (1) holds. Note that

$$Q(\bar{G}) = D(\bar{G}) + A(\bar{G}) = J + (n-2)I - Q(G).$$

It follows that $U^T Q(\bar{G}) U = Q(\bar{H})$. Thus, we have $\mathrm{Spec}_Q(G) = \mathrm{Spec}_Q(H)$ and $\mathrm{Spec}_Q(\bar{G}) = \mathrm{Spec}_Q(\bar{H})$ and the sufficiency part of the lemma follows.

Next, we show the necessity part of the lemma is true. Note that

$$\begin{aligned}\det(\lambda I + tJ - Q(G)) &= \det(\lambda I - Q(G) + tee^T)\\ &= \det(\lambda I - Q(G))\det(I + t(\lambda I - Q(G))^{-1}ee^T)\\ &= (1 + te^T(\lambda I - Q(G))^{-1}e)\det(\lambda I - Q(G)),\end{aligned}$$

for any $\lambda \notin \sigma(Q(G))$, where $\sigma(Q(G))$ is the set of the eigenvalues of $Q(G)$ (without multiplicities). It follows that $\det(\lambda I + tJ - Q(G))$ is linear in t. Similarly, we have

$$\det(\lambda I + tJ - Q(H)) = (1 + te^T(\lambda I - Q(H))^{-1}e)\det(\lambda I - Q(H)).$$

Since $\mathrm{Spec}_Q(G) = \mathrm{Spec}_Q(H)$ and $\mathrm{Spec}_Q(\bar{G}) = \mathrm{Spec}_Q(\bar{H})$, we have $\det(\lambda I - Q(G)) = \det(\lambda I - Q(H))$, and $\det(\lambda I + J - Q(G)) = \det(\lambda I + J - Q(H))$. Then, $\det(\lambda I + tJ - Q(G)) = \det(\lambda I + tJ - Q(H))$ for any t. Thus,

$$e^T(\lambda I - Q(G))^{-1}e = e^T(\lambda I - Q(H))^{-1}e. \tag{2}$$

Since $Q(G)$ is a symmetric real matrix, it has a set of eigenvectors that form an orthonormal basis for $\mathbb{R}^n$. Group the eigenvectors with respect to the eigenvalues into matrices P_μ, where the subscripts represent the eigenvalues. We have the following spectral decomposition

$$(\lambda I - Q(G))^{-1} = \sum_{\mu\in\sigma(Q(G))} \frac{1}{\lambda - \mu} P_\mu P_\mu^T.$$

Define the matrices R_μ similarly for H, and there is a similar decomposition for H. Plugging into Eq. (2), we get

$$\sum_{\mu\in\sigma(Q(G))} \frac{\|P_\mu^T e\|^2}{\lambda - \mu} = \sum_{\mu\in\sigma(Q(H))} \frac{\|R_\mu^T e\|^2}{\lambda - \mu}.$$

This shows that the Euclidean norm of $P_\mu^T e$ and $R_\mu^T e$ is the same for each μ. Therefore, there exist orthogonal matrices H_μ such that $P_\mu^T e = H_\mu R_\mu^T e$. Finally, let

$$U = [P_{\mu_1}, P_{\mu_2}, \ldots, P_{\mu_s}][R_{\mu_1}H_{\mu_1}^T, R_{\mu_2}H_{\mu_2}^T, \ldots, R_{\mu_s}H_{\mu_s}^T]^T,$$

where $\sigma(Q(G)) = \{\mu_1, \mu_2, \ldots, \mu_s\}$. Direct calculation shows that U is an orthogonal matrix satisfying $Ue = e$ and $U^TQ(G)U = Q(H)$. Thus we have

$$U^TQ^i(G)e = Q^i(H)e, \text{ for } i = 0, 1, \ldots, n-1,$$

i.e., $U^TW_Q(G) = W_Q(H)$. Hence $U = W_Q(G)W_Q(H)^{-1}$ is a rational matrix satisfying Eq. (1).

Uniqueness of the matrix U follows by assuming ${U_1}^TQ(G)U_1 = {U_2}^TQ(G)U_2 = Q(H)$ and $U_1e = U_2e = e$, which generates $U_1^TW_Q(G) = U_2^TW_Q(G)$. Then the fact that $W_Q(G)$ is full rank gives $U_1 = U_2$. This completes the proof. □

Define

$$\Gamma(G) = \{U \in O_n(\mathbb{Q}) | U^TQ(G)U = Q(H) \text{ for some graph } H \text{ and } Ue = e\},$$

where $O_n(\mathbb{Q})$ denotes the set of all orthogonal matrices with rational entries.

Similarly, the following theorem is also the analogue of a result for adjacency matrix obtained by Wang and Xu [18].

Theorem 2.2. *Suppose* $\det W_Q(G) \neq 0$. *Then G is DGQS if and only if $\Gamma(G)$ contains only permutation matrices.*

Proof. Suppose $\Gamma(G)$ contains only permutation matrices, we show G is DGQS. For contradiction, suppose G is not DGQS. Then there exists a graph H that is cospectral with G w.r.t. the generalized Q-spectrum but non-isomorphic to G. By Theorem 2.1, there exists a rational orthogonal matrix U with $Ue = e$ such that $U^TQ(G)U = Q(H)$. Then $U \in \Gamma(G)$ but U is not a permutation matrix; a contradiction.

On the other hand, suppose G is DQGS, we show $\Gamma(G)$ contains only permutation matrices. For otherwise, suppose that there exists a rational orthogonal matrix in $\Gamma(G)$, say U_1, which is not a permutation matrix. Then it is easy to see that the graph H with Q-matrix $U_1^TQ(G)U_1$ is cospectral with G w.r.t. the generalized Q-spectrum but non-isomorphic to G (since if H and G are isomorphic, there exists a permutation matrix P such that $P^TQ(G)P = Q(H)$ and $Pe = e$, which contradicts the uniqueness of U_1). Thus, we got a contradiction. This completes the proof. □

By the above theorem, in order to show a given graph G is DGQS, we have to determine whether $\Gamma(G)$ contains only permutation matrices. In order to do so, we give the following definition.

Definition 2.1. Let U be an orthogonal matrix with rational entries. The level of U, denoted by $\ell(U)$ or simply ℓ, is the smallest positive integer k such that kU is an integral matrix.

Clearly, a rational orthogonal matrix U with $Ue = e$ is a permutation matrix if and only if $\ell(U) = 1$. Thus, for a given graph G, our main strategy in proving $\Gamma(G)$ contains only permutation matrices is to show that every $U \in \Gamma(G)$ has level $\ell = 1$.

2.2. The Smith Normal Form

When dealing with integral and rational matrices, the Smith Normal Form (SNF for short) is a useful tool. An integral matrix V of order n is called *unimodular* if $\det V = \pm 1$. The following theorem is well-known.

Theorem 2.3 (*See e.g.,* [2]). *For an integral matrix M, there exist unimodular matrices V_1 and V_2 such that $M = V_1SV_2$, where $S = \mathrm{diag}(d_1, d_2, \ldots, d_n)$ is the SNF with $d_i \mid d_{i+1}$ for $i = 1, 2, \ldots, n-1$, and d_i is called the ith elementary divisor.*

Note that the SNF of a matrix can be computed efficiently (see e.g. page 50 in [14]).

The following lemma plays a key role in the proof of Theorem 1.2.

Lemma 2.4 (*Wang [15]*). *Using the notations above, the system of congruence equations* $Mx \equiv 0 \pmod{p^2}$ *has a solution* $x \not\equiv 0 \pmod{p}$ *if and only if* $p^2 \mid d_n$.

Proof. The equation $Mx \equiv 0 \pmod{p^2}$ is equivalent to $\mathrm{diag}(d_1, d_2, \ldots, d_n)V_2x \equiv 0 \pmod{p^2}$. Let $V_2x = y$. Consider $\mathrm{diag}(d_1, d_2, \ldots, d_n)y \equiv 0 \pmod{p^2}$. On the one hand, If $p^2 \mid d_n$, let $y = (0, 0, \ldots, 0, 1)^T$, then $x = V_2^{-1}y \not\equiv 0 \pmod{p}$ 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 $x \not\equiv 0 \pmod{p}$. This completes the proof. □

2.3. A technical lemma

Finally, we present the following technical lemma, which plays a key role in the proof of Theorem 1.2.

Lemma 2.5. *Let G be a graph with signless Laplacian matrix Q. Then* $e^TQe \equiv 0 \pmod{4}$, *and* $e^TQ^ke \equiv 0 \pmod{8}$, *for any integer* $k \geq 2$,

Proof. Note that $Ae = De = d$, where $d = (d_1, d_2, \ldots, d_n)^T$ and d_i is the degree of the ith vertex. It follows that $Qe = (A + D)e = 2d$. Thus we have $e^TQe = 2d^Te = 4|E| \equiv 0 \pmod{4}$. Moreover, we have $e^TQ^2e = (Qe)^T(Qe) = 4d^Td \equiv 4(d_1 + d_2 + \cdots + d_n) \equiv 0 \pmod{8}$. Next, we show $e^TQ^ke \equiv 0 \pmod{8}$ for any $k \geq 3$.

Note that $Q = A + D$ and $Ae = De$. It follows that

$$e^TQ^ke = 4e^TD(A + D)^{k-2}De \equiv 4\mathrm{Tr}(D(A + D)^{k-2}D) \pmod{8}.$$

So it suffices to show $\mathrm{Tr}(D(A + D)^{k-2}D)$ is always even for $k \geq 3$.

For the ease of presentation, we define $\mathscr{X}$ as the free monoid generated by $\{a, d\}$, and $\mathscr{X}_m = \{X \in \mathscr{X} \mid \text{the length of X} \textit{ is } \text{m}\}$. Define a mapping τ on $\mathscr{X}_m$ which reverses the order of elements of $X \in \mathscr{X}_m$, i.e., $X^\tau = M_1M_2 \ldots M_m$, where M_i is the $(m - i + 1)$-th character of X, $i = 1, 2, \ldots, m$. Denote by $\underline{X} = M_1M_2 \ldots M_m$ the product of the string of matrices in X, where $M_i = A$ if the ith character of X is a, and $M_i = D$ if the ith character of X is d, for $i = 1, 2, \ldots, m$. It is easy to see $X^\tau \in \mathscr{X}_m$ is uniquely determined by X and $\underline{X}^T = \underline{X^\tau}$.

Using the notations above, we have

$$\mathrm{Tr}(D(A + D)^{k-2}D) = \sum_{X \in \mathscr{X}_{k-2}} \mathrm{Tr}(D\underline{X}D).$$

Note that $\mathrm{Tr}(D\underline{X}D) = \mathrm{Tr}((D\underline{X}D)^T) = \mathrm{Tr}(D\underline{X^\tau}D)$. Then we have

$$\sum_{\substack{X \in \mathscr{X}_{k-2} \\ X \neq X^\tau}} \mathrm{Tr}(D\underline{X}D) \equiv 0 \pmod{2}.$$

It follows that

$$\mathrm{Tr}(D(A + D)^{k-2}D) \equiv \sum_{\substack{X \in \mathscr{X}_{k-2} \\ X = X^\tau}} \mathrm{Tr}(D\underline{X}D) \pmod{2}.$$

We distinguish the following two cases:

Case 1. k is even. Using that $De = Ae$, note that

$$\begin{aligned} \mathrm{Tr}(D\underline{X^\tau}AA\underline{X}D) &= \mathrm{Tr}(A\underline{X}DD\underline{X^\tau}A) \\ &\equiv e^TA\underline{X}DD\underline{X^\tau}Ae \\ &= e^TD\underline{X}DD\underline{X^\tau}De \\ &\equiv \mathrm{Tr}(D\underline{X}DD\underline{X^\tau}D) \pmod{2}. \end{aligned}$$

Thus

$$\begin{aligned} \mathrm{Tr}(D(A + D)^{k-2}D) &\equiv \sum_{\substack{X \in \mathscr{X}_{k-2} \\ X = X^\tau}} \mathrm{Tr}(D\underline{X}D) \\ &= \sum_{X \in \mathscr{X}_{k/2-2}} \mathrm{Tr}(D\underline{X^\tau}(AA + DD)\underline{X}D) \\ &\equiv \sum_{X \in \mathscr{X}_{k/2-2}} \mathrm{Tr}(D\underline{X}DD\underline{X^\tau}D) + \sum_{X \in \mathscr{X}_{k/2-2}} \mathrm{Tr}(D\underline{X^\tau}DD\underline{X}D) \end{aligned}$$

Please cite this article in press as: L. Qiu, et al., A new arithmetic criterion for graphs being determined by their generalized Q-spectrum, Discrete Mathematics (2018), https://doi.org/10.1016/j.disc.2018.08.008.

$$
\begin{aligned}
&= 2 \sum_{X \in \mathscr{X}_{k/2-2}} \mathrm{Tr}(D\underline{X}DD\underline{X}^{\tau}D) \\
&\equiv 0 \pmod 2.
\end{aligned}
$$

Case 2. k is odd. Note that

$$
\begin{aligned}
\mathrm{Tr}(D\underline{X}^{\tau}A\underline{X}D) &= \mathrm{Tr}(\underline{X}DD\underline{X}^{\tau}A) \\
&= \sum_{i,j=1}^{n} (\underline{X}DD\underline{X}^{\tau})_{ij}(A)_{ij} \\
&= 2 \sum_{1 \le i < j \le n} (\underline{X}DD\underline{X}^{\tau})_{ij}(A)_{ij} \\
&\equiv 0 \pmod 2.
\end{aligned}
$$

It follows that

$$
\begin{aligned}
\mathrm{Tr}(D(A+D)^{k-2}D) &\equiv \sum_{\substack{X \in \mathscr{X}_{k-2} \\ X = X^{\tau}}} \mathrm{Tr}(D\underline{X}D) \\
&= \sum_{X \in \mathscr{X}_{(k-3)/2}} \mathrm{Tr}(D\underline{X}^{\tau}(A+D)\underline{X}D) \\
&\equiv \sum_{X \in \mathscr{X}_{(k-3)/2}} \mathrm{Tr}(D\underline{X}^{\tau}D\underline{X}D) \pmod 2.
\end{aligned}
$$

Notice that $\mathrm{Tr}(D\underline{X}^{\tau}D\underline{X}D) \equiv \mathrm{Tr}(D\underline{X}^{\tau}DD\underline{X}D) \equiv \mathrm{Tr}(D\underline{X}D\underline{X}^{\tau}D) \pmod 2$. Therefore, we have

$$
\begin{aligned}
\mathrm{Tr}(D(A+D)^{k-2}D) &\equiv \sum_{X \in \mathscr{X}_{(k-3)/2}} \mathrm{Tr}(D\underline{X}^{\tau}D\underline{X}D) \\
&= \sum_{\substack{X \in \mathscr{X}_{(k-3)/2} \\ X = X^{\tau}}} \mathrm{Tr}(D\underline{X}^{\tau}D\underline{X}D) \\
&\equiv \sum_{\substack{X \in \mathscr{X}_{(k-3)/2} \\ X = X^{\tau}}} (e^{T}D\underline{X}^{\tau}D)(D\underline{X}De) \\
&\equiv \sum_{\substack{X \in \mathscr{X}_{(k-3)/2} \\ X = X^{\tau}}} e^{T}D\underline{X}De \\
&\equiv \mathrm{Tr}(D(A+D)^{(k-3)/2}D) \pmod 2
\end{aligned}
$$

Now, it is easy to show by induction on k that $e^{T}D(A+D)^{k-2}De$ is even.

Combining Cases 1 and 2, we have $e^{T}Q^{k}e \equiv 4\mathrm{Tr}(DQ^{k-2}D) \equiv 0 \pmod 8$ $(k \ge 2)$. This completes the proof. □

3. The proof of Theorem 1.2

In this section, we present the proof of Theorem 1.2. For every $U \in \Gamma(G)$ with level ℓ, we shall show that the condition of Theorem 1.2 implies that $\ell = 1$. For this purpose, we shall show that any prime p is not a divisor of ℓ. This will be done in two cases: $p = 2$ and p is an odd prime.

For the ease of presentation, we define $\mathscr{F}_{Q,n}$ to be set of all graphs on n vertices such that $\frac{\det W_Q(G)}{2^{\lfloor \frac{3n-2}{2} \rfloor}}$ is odd and square-free. Moreover, the Q-walk matrix $W_Q(G)$ 'collapses', in the sense that the rank of $W_Q(G)$ becomes one in contrast that the rank of the walk matrix $W(G)$ is $\lceil n/2 \rceil$ (see [16]), over the finite field $\mathbb{F}_2$. So we define *the modified Q-walk matrix*, denoted by $\tilde{W}_Q(G)$ or simply $\tilde{W}_Q$, to be $[e, \frac{Qe}{2}, \ldots, \frac{Q^{n-1}e}{2}]$. Since $Q(G)e = A(G)e + D(G)e = 2A(G)e$. It is clear that $\tilde{W}_Q(G)$ is an integral matrix, which plays a similar role as that of $W(G)$ in [15,16], as we shall see later.

In what follows, we shall use the finite field notation $\mathbb{F}_p$ and mod p (for a prime p) interchangeably, and shall use $\mathrm{rank}_p(M)$ to denote the rank of an integral M over $\mathbb{F}_p$.

3.1. The case p is an odd prime

In this subsection, we shall deal with the case that p is an odd prime of ℓ. The main result of this section is the following

Theorem 3.1. *Let $G \in \mathscr{F}_{Q,n}$ and $U \in \Gamma(G)$ with level ℓ. Then for any odd prime p, we have $p \nmid \ell$.*

Before presenting the proof of Theorem 3.1, we need the following lemma.

Lemma 3.2. *Let $U \in \Gamma(G)$ with level ℓ. Suppose p is a prime divisor of ℓ. Then there exists an integral vector $v \not\equiv 0 \pmod p$ such that*

$$v^TQ^k(G)v \equiv 0 \pmod{p^2},\ \tilde{W}_Q^T(G)v \equiv 0 \pmod p, \tag{3}$$

for any $k \geq 0$.

Proof. Let $\bar{U} = \ell U$. Then $\bar{U}$ is an integral matrix. Let H be a graph such that $U^TQ(G)U = Q(H)$ and $Ue = e$. It follows from Eq. (1) that $U^TQ^k(G)e = Q(H)^ke$, and hence $U^T\frac{Q^k(G)e}{2} = \frac{Q(H)^ke}{2}$, for any $k \geq 1$. Thus, we have $U^T\tilde{W}_Q(G) = \tilde{W}_Q(H)$. Let v be any column of $\bar{U}$ with $v \not\equiv 0 \pmod p$ (such a v must exist due to the definition of ℓ). With such a v we have $\tilde{W}_Q^T(G)v \equiv 0 \pmod p$. Moreover, it follows from $\bar{U}^TQ^k(G)\bar{U} = \ell^2Q^k(H) \equiv 0 \pmod{p^2}$ that $v^TQ^k(G)v \equiv 0 \pmod{p^2}$, for any $k \geq 0$. This completes the proof. □

Now we present the proof of Theorem 3.1:

Proof. Suppose on the contrary that $p \mid \ell$. By Lemma 3.2 and the fact $p^2 \nmid \det(\tilde{W}_Q)$, we have $\mathrm{rank}_p(\tilde{W}_Q) = n-1$. It follows from $\bar{U}^T\tilde{W}_Q \equiv 0 \pmod p$ and the definition of ℓ that $\mathrm{rank}_p(\bar{U}) = 1$. Then there exists an integral vector γ such that $v\gamma^T \equiv \bar{U} \pmod p$, where v is the vector satisfying Eq. (3). Let v be the lth column of $\bar{U}$. Let $U^TQ(G)U = Q(H)$ for some graph H. Then

$$Q(G)v = \bar{U}Q(H)_l \equiv v(\gamma^TQ(H)_l) = \lambda_0 v \pmod p,$$

where $Q(H)_l$ denotes the lth column of $Q(H)$ and $\lambda_0 = \gamma^TQ(H)_l$ is an integer. It follows that $\mathrm{rank}_p(Q(G)-\lambda_0 I) \neq n$. Next let $Q = Q(G)$, we distinguish the following three cases:

Case 1. $\mathrm{rank}_p(Q-\lambda_0 I) = n-1$. Note that $v^Tv \equiv 0 \pmod p$ and $v^Te \equiv 0 \pmod p$ and $v^T(Q-\lambda_0 I) \equiv 0 \pmod p$. It follows that there exist integral vectors y and u such that $v \equiv (Q-\lambda_0 I)y \pmod p$ and $e \equiv (Q-\lambda_0 I)u \pmod p$. It follows that $e = (Q-\lambda_0 I)u + p\beta$ for some integral vector β.

Thus, we have

$$\begin{aligned}\tilde{W}_Q &= [e, \frac{Qe}{2}, \dots, \frac{Q^{n-1}e}{2}]\\ &= (Q-\lambda_0 I)[u, \frac{Qu}{2}, \dots, \frac{Q^{n-1}u}{2}] + p[\beta, \frac{Q\beta}{2}, \dots, \frac{Q^{n-1}\beta}{2}]\\ &= (Q-\lambda_0 I)X + p[\beta, \frac{Q\beta}{2}, \dots, \frac{Q^{n-1}\beta}{2}],\end{aligned}$$

where $X := [u, \frac{Qu}{2}, \dots, \frac{Q^{n-1}u}{2}]$ (note that X need not be an integral matrix, but $X \pmod p$ is meaningful since p is an odd prime). It follows that

$$\tilde{W}_Q^Tv = X^T(Q-\lambda_0 I)v + p[v^T\beta, \frac{v^TQ\beta}{2}, \dots, \frac{v^TQ^{n-1}\beta}{2}]^T.$$

Moreover, since $\frac{p+1}{2} \times 2 \equiv 1 \pmod p$, we get $\frac{p+1}{2} \equiv \frac{1}{2} \pmod p$. Thus,

$$\frac{\tilde{W}_Q^Tv}{p} \equiv X^T\frac{(Q-\lambda_0 I)v}{p} + v^T\beta[1, \frac{(p+1)\lambda_0}{2}, \dots, \frac{(p+1)\lambda_0^{n-1}}{2}]^T \pmod p.$$

Since $v^Tv \equiv 0 \pmod{p^2}$, we have $v^T\frac{(Q-\lambda_0 I)v}{p} \equiv 0 \pmod p$. Further notice that $v^T(Q-\lambda_0 I) \equiv 0 \pmod p$, and $\mathrm{rank}_p(Q-\lambda_0 I) = n-1$. It follows that there exists an integral vector x such that

$$\frac{(Q-\lambda_0 I)v}{p} \equiv (Q-\lambda_0 I)x \pmod p.$$

Moreover, note that

$$v \equiv (Q-\lambda_0 I)y \pmod p,$$

$$\frac{e^TQy}{2} \equiv \frac{(p+1)\lambda_0}{2}e^Ty + \frac{p+1}{2}e^Tv \equiv \frac{(p+1)\lambda_0}{2}e^Ty \pmod p,$$

$$\frac{e^TQ^2y}{2} \equiv \frac{(p+1)\lambda_0}{2}e^TQy + \frac{p+1}{2}e^TQv \equiv \frac{(p+1)\lambda_0^2}{2}e^Ty \pmod p,$$

$$\cdots\cdots$$

$$\frac{e^T Q^{n-1} y}{2} \equiv \frac{(p+1)\lambda_0^{n-1}}{2} e^T y \pmod p.$$

From the above congruence equations, we can get

$$\tilde{W}_Q y \equiv e^T y[1, \frac{(p+1)\lambda_0}{2}, \ldots, \frac{(p+1)\lambda_0^{n-1}}{2}] \pmod p.$$

Now we show that $e^T y \not\equiv 0 \pmod p$. For otherwise, if $e^T y \equiv 0 \pmod p$, then $\tilde{W}_Q^T y \equiv 0 \pmod p$. Note that $\tilde{W}_Q^T v \equiv 0 \pmod p$ and $\mathrm{rank}_p(\tilde{W}_Q) = n-1$. Thus, y and v are linearly dependent over $\mathbb{F}_p$. However, this is a contradiction. In fact, assume there exist k_1 and k_2 such that $k_1 y + k_2 v = 0$, over $\mathbb{F}_p$. Left multiplying both sides by $Q - \lambda_0 I$ gives that $k_1 v = 0$. Thus we get $k_1 = 0$, since $v \neq 0$. It follows from $k_2 y = 0$ and $y \neq 0$ that $k_2 = 0$. Thus, there exists an integer t such that $v^T \beta \equiv t e^T y \pmod p$.

Note that $\tilde{W}_Q^T \equiv X^T (Q - \lambda_0 I) \pmod p$. Therefore, we obtain

$$\frac{\tilde{W}_Q^T v}{p} \equiv \tilde{W}_Q^T x + t\tilde{W}_Q^T y \pmod p.$$

Thus,

$$\tilde{W}_Q^T (v - px - pty) \equiv 0 \pmod{p^2}.$$

It follows from Lemma 2.4 that $p^2 \mid \det(\tilde{W}_Q)$, which contradicts the assumption of Theorem 1.2.

Case 2. $\mathrm{rank}_p(Q - \lambda_0 I) = n-2$. Now we show that v cannot be expressed as linear combinations of the column vectors of $Q - \lambda_0 I$ over $\mathbb{F}_p$. For otherwise, if there exists an integral vector w such that $(Q - \lambda_0 I)w \equiv v \pmod p$, then

$$\frac{e^T Q^k w}{2} \equiv \frac{e^T Q^{k-1} v}{2} + \frac{\lambda_0 e^T Q^{k-1} w}{2} \equiv \frac{\lambda_0^k e^T w}{2} \pmod p,$$

for any $k \geq 1$. Moreover, since $\mathrm{rank}_p(Q - \lambda_0 I) = n-2$, there exists a vector y such that $(Q - \lambda_0 I)y \equiv 0 \pmod p$, and $e^T y \not\equiv 0 \pmod p$. It is easy to see that v, w and y are linearly independent. Let $\alpha = (e^T y)w - (e^T w)y$. Then $\alpha \not\equiv 0 \pmod p$, $e^T \alpha \equiv 0 \pmod p$, and $\frac{e^T Q^k \alpha}{2} \equiv e^T y \frac{\lambda_0^k e^T w}{2} - e^T w \frac{\lambda_0^k e^T y}{2} \equiv 0 \pmod p$. Therefore, $\tilde{W}_Q^T \alpha \equiv 0 \pmod p$, which contradicts the fact that $\mathrm{rank}_p(\tilde{W}_Q) = n-1$.

Denote by $[Q - \lambda_0 I, v]$ the matrix obtained by adding the column v to $Q - \lambda_0 I$. Thus, we have $\mathrm{rank}_p([Q - \lambda_0 I, v]) = n-1$. Note that $v^T e \equiv 0 \pmod p$ and $v^T [Q - \lambda_0 I, v] \equiv 0 \pmod p$. It follows that there exist integral vectors u, β and an integer s such that

$$e = (Q - \lambda_0 I)u + sv + p\beta.$$

Thus, we have

$$\begin{aligned}
\tilde{W}_Q &= [e, \frac{Qe}{2}, \ldots, \frac{Q^{n-1}e}{2}] \\
&= (Q - \lambda_0 I)[u, \frac{Qu}{2}, \ldots, \frac{Q^{n-1}u}{2}] + s[v, \frac{Qv}{2}, \ldots, \frac{Q^{n-1}v}{2}] + p[\beta, \frac{Q\beta}{2}, \ldots, \frac{Q^{n-1}\beta}{2}] \\
&= (Q - \lambda_0 I)X + s[v, \frac{Qv}{2}, \ldots, \frac{Q^{n-1}v}{2}] + p[\beta, \frac{Q\beta}{2}, \ldots, \frac{Q^{n-1}\beta}{2}],
\end{aligned}$$

where $X := [u, \frac{Qu}{2}, \ldots, \frac{Q^{n-1}u}{2}]$.

It follows that

$$\frac{\tilde{W}_Q^T v}{p} \equiv X^T \frac{(Q - \lambda_0 I)v}{p} + (\frac{s}{p} v^T v + v^T \beta)[1, \frac{(p+1)\lambda_0}{2}, \ldots, \frac{(p+1)\lambda_0^{n-1}}{2}]^T \pmod p.$$

It follows from the facts that $v^T \frac{(Q - \lambda_0 I)v}{p} \equiv 0 \pmod p$, and $v^T [Q - \lambda_0 I, v] \equiv 0 \pmod p$, and $\mathrm{rank}_p[Q - \lambda_0 I, v] = n-1$ that there exist an integral vector x and an integer m such that

$$\frac{(Q - \lambda_0 I)v}{p} \equiv (Q - \lambda_0 I)x + mz \pmod p.$$

Moreover, since $e^T y \not\equiv 0 \pmod p$, there exists an integer t such that $\frac{s}{p} v^T v + v^T \beta + m u^T v - s v^T x \equiv t e^T y \pmod p$.

Note that $\tilde{W}_Q^T \equiv X^T(Q-\lambda_0 I)+s[v, \frac{Qv}{2}, \dots, \frac{Q^{n-1}v}{2}]^T \pmod p$. We obtain

$$\begin{aligned}\frac{\tilde{W}_Q^T v}{p} &\equiv X^T\frac{(Q-\lambda_0 I)v}{p}+(\frac{s}{p}v^Tv+v^T\beta)[1,\frac{(p+1)\lambda_0}{2},\dots,\frac{(p+1)\lambda_0^{n-1}}{2}]^T\\ &\equiv X^T(Q-\lambda_0 I)x+mX^Tv+(\frac{s}{p}v^Tv+v^T\beta)[1,\frac{(p+1)\lambda_0}{2},\dots,\frac{(p+1)\lambda_0^{n-1}}{2}]^T\\ &\equiv \tilde{W}_Q^T x+(\frac{s}{p}v^Tv+v^T\beta+mu^Tv-sv^Tx)[1,\frac{(p+1)\lambda_0}{2},\dots,\frac{(p+1)\lambda_0^{n-1}}{2}]^T\\ &\equiv \tilde{W}_Q^T x+te^Ty[1,\frac{(p+1)\lambda_0}{2},\dots,\frac{(p+1)\lambda_0^{n-1}}{2}]^T\\ &\equiv \tilde{W}_Q^T x+t\tilde{W}_Q^T y \pmod p.\end{aligned}$$

Thus,

$$\tilde{W}_Q^T(v-px-pty)\equiv 0 \pmod{p^2}.$$

It follows from Lemma 2.4 that $p^2 \mid \det(\tilde{W}_Q)$; a contradiction.

Case 3. $\mathrm{rank}_p(Q-\lambda_0 I)<n-2$. Then there exist at least three linearly independent integral vectors, say v, w and y such that $(Q-\lambda_0 I)v=(Q-\lambda_0 I)w=(Q-\lambda_0 I)y=0$, over $\mathbb{F}_p$. Without loss of generality assume that $e^Tw\not\equiv 0 \pmod p$, and $e^Ty\not\equiv 0 \pmod p$. Let $\alpha=(e^Ty)w-(e^Tw)y$. Then $\alpha\not\equiv 0\pmod p$, $e^T\alpha\equiv 0\pmod p$, and $\frac{e^TQ^k\alpha}{2}\equiv e^Ty\frac{\lambda_0^ke^Tw}{2}-e^Tw\frac{\lambda_0^ke^Ty}{2}\equiv 0\pmod p$. Therefore, $\tilde{W}_Q^T\alpha\equiv 0\pmod p$. Note that $\tilde{W}_Q^Tv\equiv 0\pmod p$ and v and α are linearly independent. We got a contradiction since $\mathrm{rank}_p(\tilde{W}_Q)=n-1$.

Combining the Cases 1–3, the proof is complete. □

3.2. The case $p=2$

In this subsection, we consider the case $p=2$. The main result of the subsection is the following

Theorem 3.3. *Let $G\in\mathscr{F}_{Q,n}$. Let $U\in\Gamma(G)$ with level ℓ, then ℓ is odd.*

Before presenting the proof of above theorem, we need several lemmas below.

Lemma 3.4. *Let $G\in\mathscr{F}_{Q,n}$. Then $\mathrm{rank}_2(\tilde{W}_Q(G))\le\lceil\frac{n}{2}\rceil$.*

Proof. First suppose n is even. Then it follows from Lemma 2.5 that

$$\tilde{W}_Q^T\tilde{W}_Q=\begin{bmatrix} e^Te & \frac{e^TQe}{2} & \cdots & \frac{e^TQ^{n-1}e}{2}\\ \frac{e^TQe}{2} & \frac{e^TQ^2e}{4} & \cdots & \frac{e^TQ^ne}{4}\\ \vdots & \vdots & \ddots & \vdots\\ \frac{e^TQ^{n-1}e}{2} & \frac{e^TQ^ne}{4} & \cdots & \frac{e^TQ^{2n-2}e}{4}\end{bmatrix}\equiv 0 \pmod 2. \tag{4}$$

It follows that $2\mathrm{rank}_2(\tilde{W}_Q)=\mathrm{rank}_2(\tilde{W}_Q^T)+\mathrm{rank}_2(\tilde{W}_Q)\le n$. Thus we have $\mathrm{rank}_2(\tilde{W}_Q)\le\frac{n}{2}=\lceil\frac{n}{2}\rceil$.

Now suppose n is odd. Let $\bar{W}_Q$ be the matrix obtained from $\tilde{W}_Q$ by doubling the first column. Then it follows from Lemma 2.5 that

$$\tilde{W}_Q^T\bar{W}_Q=\begin{bmatrix} 2e^Te & \frac{e^TQe}{2} & \cdots & \frac{e^TQ^{n-1}e}{2}\\ e^TQe & \frac{e^TQ^2e}{4} & \cdots & \frac{e^TQ^ne}{4}\\ \vdots & \vdots & \ddots & \vdots\\ e^TQ^{n-1}e & \frac{e^TQ^ne}{4} & \cdots & \frac{e^TQ^{2n-2}e}{4}\end{bmatrix}\equiv 0 \pmod 2. \tag{5}$$

Note $\mathrm{rank}_2(\tilde{W}_Q)+\mathrm{rank}_2(\bar{W}_Q)\le n$ and $\mathrm{rank}_2(\bar{W}_Q)\ge\mathrm{rank}_2(\tilde{W}_Q)-1$. It follows that $\mathrm{rank}_2(\tilde{W}_Q)\le\frac{n+1}{2}=\lceil\frac{n}{2}\rceil$.

This completes the proof. □

Lemma 3.5. *Let $G \in \mathscr{F}_{Q,n}$. Then the SNF of $\tilde{W}_Q$ is $S = \mathrm{diag}(\underbrace{1, 1, \ldots, 1}_{\lceil \frac{n}{2} \rceil}, \underbrace{2, 2, \ldots, 2, 2b}_{\lfloor \frac{n}{2} \rfloor})$, where b is an odd square-free integer.*

Proof. Since $\det W_Q(G)/2^{\lfloor \frac{3n-2}{2} \rfloor}$ is odd and square-free, we have $\det \tilde{W}_Q = \pm 2^{\lfloor \frac{n}{2} \rfloor} p_1 p_2 \cdots p_s$, where p_i's are distinct odd primes for each i. Thus the SNF of $\tilde{W}_Q$ can be written as $S = \mathrm{diag}(1, 1, \ldots, 1, 2^{l_1}, 2^{l_2}, \ldots, 2^{l_t} b)$, where $b = p_1 p_2 \ldots p_s$ is an odd square-free integer. It follows from Lemma 3.4 that $\mathrm{rank}_2(\tilde{W}_Q(G)) \le \lceil \frac{n}{2} \rceil$, i.e., $n - t \le \lceil \frac{n}{2} \rceil$. Thus, we have $t \ge n - \lceil \frac{n}{2} \rceil = \lfloor \frac{n}{2} \rfloor$. Moreover, we have $l_1 + l_2 + \cdots + l_t = \lfloor \frac{n}{2} \rfloor$, since $\det(\tilde{W}_Q) = \pm \det(S)$. It follows that $l_1 = l_2 = \cdots = l_t = 1$ and $t = \lfloor \frac{n}{2} \rfloor$. □

Lemma 3.6 (*Cf.* [15]). *Let $G \in \mathscr{F}_{Q,n}$ and $U \in \Gamma(G)$ with level ℓ. Then ℓ divides the n-the elementary divisor $d_n = 2b$ of $\tilde{W}_Q$, where b is odd and square-free.*

Proof. By the assumption, $U^T Q(G) U = Q(H)$ for some graph H. It follows that

$$U^T Q^i(G) e = Q^i(H) e, \text{ for } i = 0, 1, \ldots, n-1,$$

and hence, $U^T \frac{Q^i(G)e}{2} = \frac{Q^i(H)e}{2}$ for $i = 1, 2, \ldots, n-1$. So we have $U^T \tilde{W}_Q(G) = \tilde{W}_Q(H)$ and $U^T = \tilde{W}_Q(H) \tilde{W}_Q(G)^{-1}$. Suppose $S = \mathrm{diag}(d_1, d_2, \ldots, d_n)$ is the SNF of $\tilde{W}_Q(G)$ and $\tilde{W}_Q(G) = V_1 S V_2$, where V_1 and V_2 are unimodular matrices. Then we have that

$$d_n U^T = \tilde{W}_Q(H) V_2^{-1} \mathrm{diag}(d_n/d_1, d_n/d_2, \ldots, d_n/d_{n-1}, 1) V_1^{-1}$$

is an integral matrix. Thus the lemma follows from the definition of ℓ. □

For convenience, next, we fix some notations. Let $\hat{W}_Q$ be the matrix defined as follows:

$$\hat{W}_Q = \begin{cases} [e, \dfrac{Qe}{2}, \ldots, \dfrac{Q^{\lfloor \frac{n}{2} \rfloor - 1} e}{2}], & \text{if } n \text{ is even;} \\ [\dfrac{Qe}{2}, \dfrac{Q^2 e}{2}, \ldots, \dfrac{Q^{\lfloor \frac{n}{2} \rfloor} e}{2}], & \text{if } n \text{ is odd.} \end{cases}$$

The following lemma plays an important role in the proof of Theorem 3.3, the proof which is totally different from that in [16].

Lemma 3.7. *Let $G \in \mathscr{F}_{Q,n}$. Then we have* $\mathrm{rank}_2(\hat{W}_Q) = \lfloor \frac{n}{2} \rfloor$.

Proof. Let $t = \lceil \frac{n}{2} \rceil = \mathrm{rank}_2(\tilde{W}_Q)$. It suffices to show that the first t columns of $\tilde{W}_Q$ are linearly independent over $\mathbb{F}_2$. For contradiction, suppose $e, \frac{Qe}{2}, \ldots, \frac{Q^{t-1}e}{2}$ are linearly dependent, i.e., there exist $c_0, c_1, \ldots, c_{t-1} \in \mathbb{F}_2$, not all zero, such that $c_0 e + c_1 \frac{Qe}{2} + \cdots + c_{t-1} \frac{Q^{t-1}e}{2} = 0$. Let m be the maximum index among $0, 1, \ldots, t-1$ with $c_m \ne 0$. Then we have $0 < m \le t-1$ and

$$\frac{Q^m e}{2} = -c_m^{-1} c_0 e - c_m^{-1} c_1 \frac{Qe}{2} - \cdots - c_m^{-1} c_{m-1} \frac{Q^{m-1} e}{2} \text{ over } \mathbb{F}_2, \tag{6}$$

i.e., $\frac{Q^m e}{2} \in \mathrm{span}\{e, \frac{Qe}{2}, \ldots, \frac{Q^{m-1}e}{2}\}$. It follows from Eq. (6) that

$$\frac{Q^m e}{2} = -c_m^{-1} c_0 e - c_m^{-1} c_1 \frac{Qe}{2} - \cdots - c_m^{-1} c_{m-1} \frac{Q^{m-1} e}{2} + 2\beta \text{ over } \mathbb{Z}, \tag{7}$$

for some integral vector β. Left-multiplying Q on both sides of Eq. (7) gives that

$$\frac{Q^{m+1} e}{2} = -2 c_m^{-1} c_0 \frac{Qe}{2} - c_m^{-1} c_1 \frac{Q^2 e}{2} - \cdots - c_m^{-1} c_{m-1} \frac{Q^m e}{2} + 2Q\beta,$$

i.e.,

$$\frac{Q^{m+1} e}{2} = -c_m^{-1} c_1 \frac{Q^2 e}{2} - \cdots - c_m^{-1} c_{m-1} \frac{Q^m e}{2} \text{ over } \mathbb{F}_2. \tag{8}$$

It follows that $\frac{Q^{m+1}e}{2} \in \mathrm{span}\{e, \frac{Qe}{2}, \ldots, \frac{Q^{m-1}e}{2}\}$. Similarly, we have

$$\frac{Q^{m+s} e}{2} \in \mathrm{span}\{e, \frac{Qe}{2}, \ldots, \frac{Q^{m-1} e}{2}\},$$

for any $s \ge 0$. Thus we have $\mathrm{rank}_2(\tilde{W}_Q) \le m \le t-1$; a contradiction. This completes the proof. □

Let $\tilde{W}_{Q,1}=[e,\frac{Q^2e}{2},\ldots,\frac{Q^{2n-2}e}{2}]$. Similarly, $\hat{W}_{Q,1}$ is defined as follows:

$$\hat{W}_{Q,1}=\begin{cases}[e,\dfrac{Q^2e}{2},\ldots,\dfrac{Q^{n-2}e}{2}], & \text{if } n \text{ is even;}\\ [\dfrac{Q^2e}{2},\dfrac{Q^4e}{2},\ldots,\dfrac{Q^{n-1}e}{2}], & \text{if } n \text{ is odd.}\end{cases}$$

Lemma 3.8. *Let $G\in\mathscr{F}_{Q,n}$. We have* $\operatorname{rank}_2(\frac{\tilde{W}_Q^T(G)\hat{W}_{Q,1}(G)}{2})=\lfloor\frac{n}{2}\rfloor$.

Proof. If n is even, by Lemma 3.5, it follows $\det(\frac{\tilde{W}_Q^T\tilde{W}_Q}{2})=(2^{\lfloor\frac{n}{2}\rfloor}b)^2/2^n=b^2$. Therefore, the column vectors of matrix $\frac{\tilde{W}_Q^T\tilde{W}_Q}{2}$ are linearly independent over $\mathbb{F}_2$. It follows that $\operatorname{rank}_2(\frac{\tilde{W}_Q^T(G)\hat{W}_{Q,1}(G)}{2})$ equals the number of columns of $\hat{W}_{Q,1}$, which is $\frac{n}{2}=\lfloor\frac{n}{2}\rfloor$.

If n is odd, by Lemma 3.5, it follows $\det(\frac{\tilde{W}_Q^T\tilde{W}_Q}{2})=b^2$. Therefore, the column vectors of matrix $\frac{\tilde{W}_Q^T\tilde{W}_Q}{2}$ are linearly independent over $\mathbb{F}_2$. Thus, $\operatorname{rank}_2(\frac{\tilde{W}_Q^T(G)\hat{W}_{Q,1}(G)}{2})$ equals the number of columns of $\hat{W}_{Q,1}$, which is $\frac{n-1}{2}=\lfloor\frac{n}{2}\rfloor$. □

Now we are ready to present the proof of Theorem 3.3:

Proof. We only prove the case that n is even, the case that n is odd can be proved in a similar way.

Suppose on the contrary that ℓ is even. It follows from Lemma 3.2 that there exists a vector $v\not\equiv 0\pmod 2$ such that $v^TQ^k(G)v\equiv 0\pmod 4$, $\tilde{W}_Q^T(G)v\equiv 0\pmod 2$. According to Lemma 3.7 and Eq. (4), it follows that v can be written as the linear combination of the column vectors of $\hat{W}_Q$, i.e. $v=\hat{W}_Qu+2\beta$, where u and β are integral vectors and $u\not\equiv 0\pmod 2$. It follows that

$$\begin{aligned}v^TQ^kv&=(\hat{W}_Qu+2\beta)^TQ^k(\hat{W}_Qu+2\beta)\\&=u^T\hat{W}_Q^TQ^k\hat{W}_Qu+4u^T\hat{W}_Q^TQ^k\beta+4\beta^TQ^k\beta\\&\equiv u^T\hat{W}_Q^TQ^k\hat{W}_Qu\\&\equiv 0\pmod 4.\end{aligned}$$

Note that

$$\hat{W}_Q^TQ^k\hat{W}_Q=\begin{bmatrix}e^TQ^ke & \dfrac{e^TQ^{1+k}e}{2} & \cdots & \dfrac{e^TQ^{n/2-1+k}e}{2}\\ \dfrac{e^TQ^{1+k}e}{2} & \dfrac{e^TQ^{2+k}e}{4} & \cdots & \dfrac{e^TQ^{n/2+k}e}{4}\\ \vdots & \vdots & \ddots & \vdots\\ \dfrac{e^TQ^{n/2-1+k}e}{2} & \dfrac{e^TQ^{n/2+k}e}{4} & \cdots & \dfrac{e^TQ^{n-2+k}e}{4}\end{bmatrix}\equiv 0\pmod 2.$$

Let $M=\hat{W}_Q^TQ^k\hat{W}_Q$, $u=(u_1,u_2,\ldots,u_l)^T$ $(l=n/2)$. Then it follows that

$$\begin{aligned}u^T\hat{W}_Q^TQ^k\hat{W}_Qu&=\sum_{1\le i,j\le l}M_{ij}u_iu_j\\&=\sum_{1\le i\le l}M_{ii}u_i^2+2\sum_{1\le i<j\le l}M_{ij}u_iu_j\\&\equiv(e^TQ^ke)u_1+\frac{e^TQ^{2+k}e}{4}u_2+\cdots+\frac{e^TQ^{n-2+k}e}{4}u_l\\&=[e^TQ^ke,\frac{e^TQ^{2+k}e}{4},\ldots,\frac{e^TQ^{n-2+k}e}{4}]u\\&\equiv 0\pmod 4),\end{aligned}$$

for $k=0,1,\ldots,n-1$, or equivalently,

$$[\frac{e^TQ^ke}{2},\frac{e^TQ^{2+k}e}{8},\ldots,\frac{e^TQ^{n-2+k}e}{8}]u\equiv 0\,(\mathrm{mod}\ 2,)$$

for $k=0,1,\ldots,n-1$, where we have used Lemma 2.5.

Define

$$M_1 := \begin{bmatrix} \frac{e^Te}{2} & \frac{e^TQ^2e}{8} & \frac{e^TQ^4e}{8} & \cdots & \frac{e^TQ^{n-2}e}{8} \\ 0 & \frac{e^TQ^3e}{8} & \frac{e^TQ^5e}{8} & \cdots & \frac{e^TQ^{n-1}e}{8} \\ 0 & \frac{e^TQ^4e}{8} & \frac{e^TQ^4e}{8} & \cdots & \frac{e^TQ^ne}{8} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \frac{e^TQ^{n+1}e}{8} & \frac{e^TQ^{n+3}e}{8} & \cdots & \frac{e^TQ^{2n-3}e}{8} \end{bmatrix}$$
$$\equiv \begin{bmatrix} \frac{e^Te}{2} & \frac{e^TQ^2e}{8} & \frac{e^TQ^4e}{8} & \cdots & \frac{e^TQ^{n-2}e}{8} \\ \frac{e^TQe}{2} & \frac{e^TQ^3e}{8} & \frac{e^TQ^5e}{8} & \cdots & \frac{e^TQ^{n-1}e}{8} \\ \frac{e^TQ^2e}{2} & \frac{e^TQ^4e}{8} & \frac{e^TQ^6e}{8} & \cdots & \frac{e^TQ^ne}{8} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \frac{e^TQ^{n-1}e}{2} & \frac{e^TQ^{n+1}e}{8} & \frac{e^TQ^{n+3}e}{8} & \cdots & \frac{e^TQ^{2n-3}e}{8} \end{bmatrix} \pmod 2.$$

Then we have $M_1u \equiv 0 \pmod 2$. Moreover,

$$M_2 := \begin{bmatrix} \frac{e^Te}{2} & 0 & 0 & \cdots & 0 \\ \frac{e^TQe}{4} & \frac{e^TQ^3e}{8} & \frac{e^TQ^5e}{8} & \cdots & \frac{e^TQ^{n-1}e}{8} \\ 0 & \frac{e^TQ^4e}{8} & \frac{e^TQ^6e}{8} & \cdots & \frac{e^TQ^ne}{8} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \frac{e^TQ^{n+1}e}{8} & \frac{e^TQ^{n+3}e}{8} & \cdots & \frac{e^TQ^{2n-3}e}{8} \end{bmatrix}$$
$$\equiv \begin{bmatrix} \frac{e^Te}{2} & \frac{e^TQ^2e}{4} & \frac{e^TQ^4e}{4} & \cdots & \frac{e^TQ^{n-2}e}{4} \\ \frac{e^TQe}{4} & \frac{e^TQ^3e}{8} & \frac{e^TQ^5e}{8} & \cdots & \frac{e^TQ^{n-1}e}{8} \\ \frac{e^TQ^2e}{4} & \frac{e^TQ^4e}{8} & \frac{e^TQ^6e}{8} & \cdots & \frac{e^TQ^ne}{8} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \frac{e^TQ^{n-1}e}{4} & \frac{e^TQ^{n+1}e}{8} & \frac{e^TQ^{n+3}e}{8} & \cdots & \frac{e^TQ^{2n-3}e}{8} \end{bmatrix}$$
$$= \frac{1}{2} \begin{bmatrix} e^T \\ \frac{e^TQ}{2} \\ \vdots \\ \frac{e^TQ^{n-1}}{2} \end{bmatrix} [e, \frac{Q^2e}{2}, \dots, \frac{Q^{n-2}e}{2}]$$
$$= \frac{\tilde{W}_Q^T \hat{W}_{Q,1}}{2} \pmod 2,$$

where $\hat{W}_{Q,1} = [e, \frac{Q^2e}{2}, \dots, \frac{Q^{n-2}e}{2}]$ and we have used the fact that $e^TQe \equiv 0 \pmod 4$ and $e^TQ^ke \equiv 0 \pmod 8$ for $k \geq 2$.

According to Lemma 3.7, $\text{rank}_2(M_2) = \text{rank}_2(\frac{\tilde{W}_Q^T \hat{W}_{Q,1}}{2}) = \frac{n}{2}$, i.e., M_2 has full column rank over $\mathbb{F}_2$. Comparing M_1 and M_2, we distinguish the following two cases:

Case 1. If $n = e^T e \not\equiv 0 \pmod 4$, then we have $\text{rank}_2(M_1) = \text{rank}_2(M_2) = \frac{n}{2}$, i.e., M_1 has full column rank over $\mathbb{F}_2$. It follows from $M_1 u \equiv 0 \pmod 2$ that $u \equiv 0 \pmod 2$; a contradiction.

Case 2. If $n = e^T e \equiv 0 \pmod 4$, then we have $\text{rank}_2(M_1) = \text{rank}_2(M_2) - 1 = \frac{n}{2} - 1$. It follows that the solution space of the linear systems of equations $M_1 u \equiv 0 \pmod 2$ has dimension one, i.e., it is spanned by $u \equiv (1, 0, 0, \dots, 0)^T \pmod 2$. Hence $v \equiv \hat{W}_Q u \equiv e \pmod 2$. However, by Lemma 3.6, we have $\ell \mid 2b$. Moreover, by Theorem 3.1, we have $\ell \mid 2$, i.e., $\ell = 2$ since ℓ is assumed to be even. It follows that the (0,1)-vector $v \equiv e \pmod 2$ has exactly four "1". This happens only when $n = 4$. However, it is easy to check by enumerating all graphs with four vertices that none of them belongs to $\mathcal{F}_{Q,n}$. We got a contradiction again.

Combining Cases 1 and 2, the theorem follows. This completes the proof. □

Finally, we present the proof of Theorem 1.2.

Proof. Let $G \in \mathcal{F}_{Q,n}$. Let $U \in \Gamma(G)$ with level ℓ. By Theorem 3.1, we get $p \nmid \ell$ for any odd prime p. By Theorem 3.3, we get that $2 \nmid \ell$. Therefore, the only possibility left is that $\ell = 1$, and hence G is DGQS according to Theorem 2.2. This completes the proof. □

4. Some numerical results

In this section, we shall present some numerical results to demonstrate how often a randomly generated graph satisfies the condition of Theorem 1.2.

First we give a specific example below as an illustration of Theorem 1.2.

Example. Let the adjacency matrix of graph G be given as follows:

$$A = \begin{pmatrix}
0&1&0&0&0&0&1&0&1&0&0&0&0&1\\
1&0&1&0&0&1&0&1&1&1&0&1&1&0\\
0&1&0&0&0&1&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&0&0&0&1&1&0&1&0\\
0&0&0&0&0&1&0&1&1&1&0&0&0&1\\
0&1&1&0&1&0&0&1&1&0&0&1&1&0\\
1&0&0&0&0&0&0&1&1&0&1&0&0&1\\
0&1&0&0&1&1&1&0&1&1&1&1&1&0\\
1&1&0&0&1&1&1&1&0&0&1&0&0&0\\
0&1&0&1&1&0&0&1&0&0&0&0&1&0\\
0&0&0&1&0&0&1&1&1&0&0&1&1&0\\
0&1&1&0&0&1&0&1&0&0&1&0&1&1\\
0&1&0&1&0&1&0&1&0&1&1&1&0&0\\
1&0&0&0&1&0&1&0&0&0&0&1&0&0
\end{pmatrix}_{14\times 14}.$$

It can be computed easily using Mathematica 8.0 that

$$\det W_Q(G) = 2^{20} \times 3853 \times 279659 \times 60587890527299.$$

Thus, G is DGQS.

We have also conducted a series of numerical experiments to estimate the fraction of graphs satisfying Theorem 1.2. Our method works as follows. For a fixed n ($1 \le n \le 20$), we randomly generate 10,000 graphs of order n in which every edge was selected independently with probability $\frac{1}{2}$, then count the number of the generated graphs satisfying Theorem 1.2. Table 1 records the results of one of such experiments.

It can be observed from Table 1 that there are many graphs that are DGQS. In particular, for $6 \le n \le 20$, the estimated fraction of DGQS graphs is around 21% for odd n; it is around 7% for $n \equiv 0 \pmod 4$, and is round 14% for $n \equiv 2 \pmod 4$.

5. Conclusions

In this paper, we have given a simple arithmetic condition for a large family of graphs to be DGQS in terms of whether the determinant of its Q-walk matrix divided by $2^{\lfloor \frac{3n-2}{2} \rfloor}$ is odd and square-free. It would be an interesting future work to study the asymptotic density of graphs in $\mathcal{F}_{Q,n}$ satisfying this property, e.g., we would like to know whether the family of graphs $\mathcal{F}_{Q,n}$ has positive density, as $n \to \infty$.

Table 1
Estimated fraction of DGQS Graphs.

n	Fraction	n	Fraction
1	0	11	0.2109
2	0	12	0.0747
3	0	13	0.2137
4	0	14	0.1455
5	0	15	0.2081
6	0.0862	16	0.0736
7	0.1904	17	0.2064
8	0.0738	18	0.1408
9	0.2009	19	0.2214
10	0.1457	20	0.0730

Acknowledgements

The authors would like to thank the reviewers for their careful reading of the manuscript of the paper and for their detailed comments and suggestions which significantly improved the presentation of the paper.

References

[1] L. Babai, Graph isomorphism in quasipolynomial time, 2015. arXiv:1512.03547.
[2] H. Cohen, A Course in Computational Algebraic NumberTheory, in: Graduate Texts in Math., Springer-Verlag, Berlin, 1993.
[3] D.M. Cvetković, P. Rowlinson, S.K. Simić, An Introduction to the Theory of Graph Spectra, Cambridge University Press, Cambridge, 2010.
[4] D.M. Cvetković, S.K. Simić, Towards a spectral theory of graphs based on the signless Laplacian I, Publ. Inst. Math. (Beograd) 85 (99) (2009) 19–33.
[5] D.M. Cvetković, S.K. Simić, Towards a spectral theory of graphs based on the signless Laplacian II, Linear Algebra Appl. 432 (2010) 2257–2272.
[6] D.M. Cvetković, S.K. Simić, Towards a spectral theory of graphs based on the signless Laplacian III, Appl. Anal. Discrete Math. 4 (2010) 156–166.
[7] E.R. van Dam, W.H. Haemers, Which graphs are determined by their spectrum? Linear Algebra Appl. 373 (2003) 241–272.
[8] E.R. van Dam, W.H. Haemers, Developments on spectral characterizations of graphs, Discrete Math. 309 (2009) 576–586.
[9] Hs.H. Günthard, H. Primas, Zusammenhang von Graphentheorie und MO-Theorie von Molekeln mit Systemen konjugierter Bindungen, Helv. Chim. Acta 39 (1956) 1645–1653.
[10] M. Fisher, On hearing the shape of a drum, J. Combin. Theory 1 (1966) 105–125.
[11] M. Kac, Can one hear the shape of a drum? Amer. Math. Monthly 73 (1966) 1–23.
[12] X. Ma, Q. Huang, Signless Laplacian spectral characterization of 4-rose graphs, Linear and Multilinear Algebra 64 (2016) 2474–2485.
[13] G.R. Omidi, On a signless Laplacian spectral characterization of T-shape trees, Linear Algebra Appl. 431 (2009) 1607–1615.
[14] A. Schrijver, The Theory of Linear and Integer Programming, John Wiley & Sons, 1998.
[15] W. Wang, Generalized spectral characterization revisited, Electron. J. Combin. 20 (4) (2013) ♯ P4.
[16] W. Wang, A simple arithmetic criterion for graphs being determined by their generalized spectra, J. Combin. Theory, Ser. B 122 (2017) 438–451.
[17] W. Wang, C.X. Xu, An excluding algorithm for testing whether a family of graphs are determined by their generalized spectra, Linear Algebra Appl. 418 (2006) 62–74.
[18] 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.
[19] Y. Zhang, X. Liu, B. Zhang, X. Yong, The lollipop graph is determined by its Q-spectrum, Discrete Math. 309 (2009) 3364–3369.

Please cite this article in press as: L. Qiu, et al., A new arithmetic criterion for graphs being determined by their generalized Q-spectrum, Discrete Mathematics (2018), https://doi.org/10.1016/j.disc.2018.08.008.