On a conjecture of He concerning the spectral reconstruction of matrices

Wei Wang · Zongben Xu

Abstract This paper is concerned with a recent conjecture of He (Electron. J. Comb. 14(1), 2007) on the spectral reconstruction of matrices. A counterexample is provided by using Hadamard matrices. We also give some results to the above mentioned conjecture (with slight modifications) in the positive direction.

Keywords Reconstruction · Hadamard matrix

1 Introduction

The graph reconstruction conjecture, also known as Kelly-Ulam's conjecture, is one of the most notoriously difficult problems to solve in graph theory. Various methods have been attempted to tackle this conjecture, say, among others, the linear algebra method, originated from Tutte [7], has been proved to be a useful one. For example, Tutte [7] proved that, if the characteristic polynomial of the adjacency matrix of a graph is irreducible, then the reconstruction conjecture is true.

Motivated by the original reconstruction conjecture and the attempts to deal with it, it is natural to consider the following spectral version of the matrix reconstruction problem:

Fix $n \geq 3$ from now on. Let A be an n by n real symmetric matrix, let A_i denote the matrix obtained from A by deleting the i-th row and i-th column. Denote by $\phi(A) = det(xI - A)$ the characteristic polynomial of matrix A. Suppose that A and B are two real symmetric matrices such that

$$\phi(A) = \phi(B) \text{ and } \phi(A_i) = \phi(B_i) \text{ for each } i. \tag{1}$$

W. Wang (✉) · Z. Xu
Department of Mathematics, Xi'an Jiaotong University, Xi'an 710049, People's Republic of China
e-mail: wang_weiw@163.com

Then, what can be said about the relations between A and B under condition (1), analogously to the reconstruction conjecture?

The above problem has been investigated by several authors [1–3, 5, 9] in some different guises, as an attempt to deal with the reconstruction conjecture. In graph context, [1] (see also [2]) showed that under condition (1), if all of the eigenvectors of A are not orthogonal to the all-one vector, then the graphs with adjacency matrices A and B are isomorphic; while [5] indicated that there exist two non-isomorphic graphs whose adjacency matrices satisfy (1). In the matrix form, [8] showed that if A and B are integral symmetric matrices with $\phi(A)$ being irreducible over the rationals, then (1) implies $B = D^T A D$ for some diagonal matrix D with each entry equal to ± 1 (this slightly generalizes a result in [7]). However, this is no longer true even if $\phi(A)$ can be factored exactly into two distinct irreducible polynomials; see [9]. Thus, it seems difficult to give a correct formulation of the matrix reconstruction conjecture in the spectral form.

More recently, He [3] posed, among others, the following conjecture along this line of research:

Conjecture 1 *Let A be a real symmetric matrix. Then there exists a subgroup $G(A) \subset O(n)$ (the orthogonal group of order n) such that a real symmetric matrix B satisfies condition (1) iff $B = U^T A U$ for some $U \in G(A)$.*

Let's give a few explanations to Conjecture 1: (i) If A and B satisfy condition (1), then there certainly exist many orthogonal matrices U such that $B = U^T A U$. Conjecture 1 asserts that we can choose some U for each B appropriately, then these U form a group $G(A)$ under matrix multiplication; (ii) For each $U \in G(A)$, matrices A and $B =: U^T A U$ satisfy condition (1).

As mentioned previously, Conjecture 1 holds if A and B are integral symmetric matrices with $\phi(A)$ being irreducible. And accordingly, $G(A)$ can be chosen to be $\mathbf{Z}_2^n$, i.e., the group of diagonal orthogonal matrices.

However, in this paper, we show that Conjecture 1 is generally not true when $\phi(A)$ is completely factored over the rationals. A counterexample will be given by using Hadamard matrices of order 16.

On the other hand, attempts have also been made to give some results to Conjecture 1 (with a slightly different reformulation) on the positive side. Based on a recent work [9], we prove that a slight modification of Conjecture 1 holds under the condition that $\phi(A)$ can be factored exactly into two distinct irreducible polynomials. We have the following

Theorem 1.1 *Let A be an integral symmetric matrix. Suppose that $\phi(A)$ can be decomposed exactly into two distinct irreducible polynomials over the rationals. Then there exists a subgroup $G(A) \subset O(n)$ such that an integral symmetric matrix B satisfies condition (1) iff $B = (UD)^T A(UD)$ for some $U \in G(A)$ and some diagonal orthogonal matrix D.*

We prove the above theorem by finding the group $G(A)$, i.e., we actually find out all integral symmetric matrices B such that A and B satisfy condition (1). The

proof is based on an observation in [9]: Let Q $(\neq \pm I)$ be a rational orthogonal matrix that commutes with A (under the assumption of Theorem 1.1), then Q is essentially unique (up to a sign). Without loss of generality (permuting rows and columns of A simultaneously, if necessary) we can assume that $Q = \mathrm{diag}[Q_1, Q_2, \cdots, Q_k]$, where Q_i is a symmetric, rational orthogonal matrix, the underlying graph (in a precise sense, see Sect. 3) of which is connected, for each i. Let $G(A)$ be the set of all matrices obtained from Q by replacing some of $Q_i's$ with the identity matrices of the same order. It is not difficult to show that $G(A)$ forms a group under matrix multiplication, and matrices $(UD)^T A(UD)$ and A satisfy condition (1). We manage to prove that all integral symmetric matrices B satisfying condition (1) can be written as $B = (UD)^T A(UD)$ for some $U \in G(A)$ and some diagonal orthogonal matrix D.

Finally, we mention that the similar result does not hold for Conjecture 1 without the modification made in Theorem 1.1. This gives another counterexample to Conjecture 1; see remarks in Sect. 4. Yet we do not know whether the method in the paper to construct a counterexample to Conjecture 1 is still valid to provide a counterexample to Theorem 1.1 without the assumption on $\phi(A)$.

The rest of the paper is organized as follows: In Sect. 2, we give a counterexample to Conjecture 1. In Sect. 3, we present the proof of Theorem 1.1. Some remarks are given in Sect. 4.

2 A counterexample to Conjecture 1

In this section, we give a counterexample to Conjecture 1 by using Hadamard matrices. An n by n matrix H is a *Hadamard matrix* if each entry of H is ± 1 and $H^T H = nI_n$. Two Hadamard matrices H_1 and H_2 are said to be *inequivalent* if H_1 can not be obtained from H_2 by permuting rows, permuting columns, and multiplying rows or columns by -1.

It is known (see e.g. [6]) that there exist exactly five classes of inequivalent Hadamard matrices of order 16. We will need the following two inequivalent Hadamard matrices H_1 and H_2 (which are the fifth and the first Hadamard matrices given in [6], respectively) in the sequel.

$$H_1 = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\
1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\
1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\
1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\
1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\
1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \\
1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\
1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 \\
1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 \\
1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\
1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 \\
1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 \\
1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 \\
1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1
\end{bmatrix},$$

$$H_2 = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\
1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\
1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\
1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\
1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\
1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\
1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\
1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & 1 & -1 \\
1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 \\
1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 \\
1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 \\
1 & -1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 \\
1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 \\
1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & 1 & -1
\end{bmatrix}.$$

To construct a counterexample to Conjecture 1, we need the following lemma which gives a characterization of matrices with the same $\phi(A)$ and $\phi(A_i)$.

Lemma 2.1 [4] *Let A and B be two real symmetric matrices such that $\phi(A) = \phi(B)$. Suppose all the eigenvalues of A (and hence B) are simple. Then for a fixed i, $\phi(A_i) = \phi(B_i)$ iff $(e_i^T \tilde{\xi}_k)^2 = (e_i^T \tilde{\eta}_k)^2$ $(k = 1, \cdots, n)$, where $\tilde{\xi}_k$ and $\tilde{\eta}_k$ $(k = 1, \cdots, n)$ are the normalized eigenvectors of A and B respectively, and e_i is the i-th standard unit vector of $\mathbf{R}^n$.*

Lemma 2.2 *Let $A = P\Lambda P^T$ and $B = Q\Lambda Q^T$, where $\Lambda = \mathrm{diag}(\lambda_1, \lambda_2, \cdots, \lambda_n)$ is a diagonal matrix with λ_i being distinct, and P and Q are orthogonal matrices respectively. If there is an orthogonal matrix U such that $B = U^T AU$, then $U = PDQ^T$ for some diagonal orthogonal matrix D.*

Proof Clearly the i-th column ξ_i of P and the i-th column η_i of Q are the eigenvectors of A and B associated with λ_i, respectively. By $B = U^T AU$ we get $AU = UB$. Thus $AU\eta_i = UB\eta_i = \lambda_i U\eta_i$. It follows that $U\eta_i$ is an eigenvector of A associated with λ_i. Note that λ_i is a simple eigenvalue of A, we get $U\eta_i = \pm\xi_i$. Hence $UQ = PD$ for some diagonal orthogonal matrix D, and the lemma follows. $\square$

Now, let $\tilde{H}_1 = H_1/4$ and $\tilde{H}_2 = H_2/4$. Then $\tilde{H}_1$ and $\tilde{H}_2$ are orthogonal matrices. Let

$$A = \tilde{H}_1 \Delta \tilde{H}_1^T, \ B = \tilde{H}_2 \Delta \tilde{H}_2^T, \tag{2}$$

where $\Delta = \mathrm{diag}(\lambda_1, \lambda_2, \cdots, \lambda_n)$ is a diagonal matrix with $\lambda_1, \lambda_2, \cdots, \lambda_n$ being distinct integers. Clearly we have $\phi(A) = \phi(B)$. By Lemma 2.1, we have $\phi(A_i) = \phi(B_i)$ for $i = 1, 2, \cdots, 16$.

Assume that Conjecture 1 is true, then there exists a real orthogonal matrix U and a group $G(A) \subset O(16)$ such that $U \in G(A)$ and $B = U^T AU$. By Lemma 2.2, we can write $U = \tilde{H}_1 D \tilde{H}_2^T$ for some diagonal orthogonal matrix D. Note that U is an element of the group $G(A)$, it follows that $U^{-1} = U^T \in G(A)$. Conjecture 1 says

that matrix

$$C =: (U^T)^T A U^T = (\tilde{H}_1 D \tilde{H}_2{}^T \tilde{H}_1) \Delta (\tilde{H}_1 D \tilde{H}_2{}^T \tilde{H}_1)^T$$

satisfies that $\phi(A) = \phi(C)$ and $\phi(A_i) = \phi(C_i)$ for $i = 1, 2, \cdots, 16$.

Using Lemma 2.1 again, we obtain that $V =: 4\tilde{H}_1 D \tilde{H}_2{}^T \tilde{H}_1$ is a Hadamard matrix of order 16. However, next, we will show through some simple calculations that V is not a Hadamard matrix for each diagonal orthogonal matrix D, which gives a contradiction to Conjecture 1.

First, it can be computed that $\tilde{H}_2{}^T \tilde{H}_1 = \begin{bmatrix} I_6 & O \\ O & X \end{bmatrix}$, where I_6 is the identity matrix of order 6 and

$$X = \frac{1}{4} \begin{bmatrix}
2 & 2 & 0 & 1 & 1 & 0 & -2 & 1 & -1 & 0 \\
2 & 2 & 0 & -1 & -1 & 0 & 2 & -1 & 1 & 0 \\
0 & 0 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 2 & -2 & 0 & 0 & 2 & 2 & 0 \\
0 & 0 & 0 & 2 & 0 & 2 & 0 & -2 & 0 & 2 \\
0 & 0 & 0 & 0 & 2 & -2 & 0 & 0 & 2 & 2 \\
0 & 0 & 0 & 2 & 2 & 0 & 2 & 0 & 0 & -2 \\
0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & -2 & 2 \\
2 & -2 & 0 & -1 & 1 & 2 & 0 & 1 & 1 & 0 \\
-2 & 2 & 0 & -1 & 1 & 2 & 0 & 1 & 1 & 0
\end{bmatrix}.$$

Now let the corresponding matrix partition of D and $\tilde{H}_1$ be as follows:

$$D = \begin{bmatrix} D_1 & O \\ O & D_2 \end{bmatrix}, \quad \tilde{H}_1 = \begin{bmatrix} W_1 & W_2 \\ W_2 & W_4 \end{bmatrix},$$

where D_1 and D_2 are diagonal orthogonal matrices of order 6 and 10 respectively, W_1 is a square matrix of order 6 and

$$W_4 = \frac{1}{4} \begin{bmatrix}
1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \\
1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\
1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\
1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 \\
-1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 \\
-1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\
-1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 \\
-1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 \\
1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 \\
1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1
\end{bmatrix}.$$

Then the right-bottom 10×10 sub-matrix Y of V equals $4W_4 D_2 X$. The first column of Y equals

$$W_4 D_2 [2, 2, 0, 0, 0, 0, 0, 0, 2, -2]^T = W_4 [2\varepsilon_1, 2\varepsilon_2, 0, 0, 0, 0, 0, 0, 2\varepsilon_3, 2\varepsilon_4]^T,$$

where $\varepsilon_i = \pm 1, i = 1, 2, 3, 4$. It can be verified for each choice of $\varepsilon_i = \pm 1$, the first column of Y cannot be a vector with each entry being equal to ± 1. That is, V can

not be a Hadamard matrix for each diagonal orthogonal matrix D, as claimed. Thus matrices A and B in (1) give a counterexample to Conjecture 1.

Let's give a remark. In an attempt to construct a counterexample to Theorem 1.1 without the assumption on $\phi(A)$, using a similar method above, we have to show that there exist two diagonal orthogonal matrices D_1 and D_2 such that $4\tilde{H}_1 D_1 \tilde{H}_2^T D_2 \tilde{H}_1$ is a Hadamard matrix. But it needs heavy computational efforts to verify.

3 Proof of Theorem 1.1

In this section, we present the proof of Theorem 1.1. We shall assume in the sequel that $\phi(A)$ can be decomposed as follows:

$$\phi(A) = \chi_1(x)\chi_2(x), \tag{3}$$

where $\chi_1(x)$ and $\chi_2(x)$ are two distinct irreducible polynomials.

The following lemma is a key to the proof of Theorem 1.1.

Lemma 3.1 [9] *Suppose that $\phi(A)$ satisfies* (3). *If there exist rational orthogonal matrices Q which are distinct from $\pm I_n$ such that $Q^T A Q = A$, then Q is unique up to a sign.*

The underlying graph of an n by n real symmetric matrix M is a simple graph on n vertices in which there is an edge between vertices i and j iff the (i, j)-th element of M is not equal to zero.

Lemma 3.2 *Let*
$$\begin{bmatrix} Q_1 & & & \\ & Q_2 & & \\ & & \ddots & \\ & & & Q_l \end{bmatrix} = P^T \begin{bmatrix} Q_1' & & & \\ & Q_2' & & \\ & & \ddots & \\ & & & Q_m' \end{bmatrix} P, \text{ where } Q_1, Q_2, \cdots, Q_l$$
(resp. $Q_1', Q_2', \cdots, Q_m'$) are symmetric matrices whose underlying graphs are connected, and P is a permutation matrix. Then we have $l = m$, and $P = \mathrm{diag}[P_1, P_2, \cdots, P_l]\hat{P}$, where P_k is a permutation matrix of the same order as Q_k' for each k, and $\hat{P}$ is a permutation matrix that permutes the diagonal blocks $Q_{i_k} = P_k^T Q_k' P_k$ ($k = 1, 2, \cdots, l$) into $Q_1, Q_2, \cdots, Q_l$. (By abuse use of language, we do not distinguish a permutation matrix and the corresponding permutation.)

Proof Denote by Γ_k (resp. Γ_k') the underlying graph of Q_k (resp. Q_k'). Then the disjoint unions $\Gamma = \bigcup_{k=1}^{l} \Gamma_k$ and $\Gamma' = \bigcup_{k=1}^{m} \Gamma_k'$ are isomorphic. It follows that the number of their connected components are equal, i.e., $l = m$.

Let the subgraph Γ_k' of Γ' be indexed as $I(\Gamma_1') = \{1, 2, \cdots, n_1\}$, $I(\Gamma_2') = \{n_1 + 1, n_1 + 2, \cdots, n_1 + n_2\}, \cdots, I(\Gamma_l') = \{n_{l-1} + 1, n_{l-1} + 2, \cdots, n_{l-1} + n_l\}$. Let Γ_k be indexed as $I(\Gamma_1) = \{1, 2, \cdots, m_1\}$, $I(\Gamma_2) = \{m_1 + 1, m_1 + 2, \cdots, m_1 + m_2\}, \cdots$, $I(\Gamma_l) = \{m_{l-1} + 1, m_{l-1} + 2, \cdots, m_{l-1} + m_l\}$.

Note that Γ can be obtained from Γ' by reindexing using permutation P. We claim that for each k there must exist some i_k such that P permutes $I(\Gamma_k')$ into $I(\Gamma_{i_k})$.

Suppose that an element, say $n_{k-1} + n_k$, of $I(\Gamma'_k)$ is permuted into $I(\Gamma_{i_k})$, we prove that each element in $I(\Gamma'_k)$ is permuted into $I(\Gamma_{i_k})$. For contradiction, assume that each element in subset V_1 $(\neq \phi)$ of $I(\Gamma'_k)$ is permuted into $I(\Gamma_{i_k})$, while the elements in the subset $V_2 := I(\Gamma'_k) - V_1$ $(\neq \phi)$ are not permuted into $I(\Gamma_{i_k})$. Since Γ'_k is connected, there is an edge $e = uv$ with $u \in V_1$ and $v \in V_2$. Thus, the (u, v) entry of the adjacency matrix $A(\Gamma)$ of Γ equals 1. Note that $u \in I(\Gamma_{i_k})$ and $v \notin I(\Gamma_{i_k})$, it follows that $A(\Gamma)_{uv} = 0$. Thus, we get a contradiction.

Since Γ' can also be obtained from Γ by reindexing using permutation P^{-1}. It can be shown in a similar way that for each j, there must exist some i_j such that P^{-1} permutes $I(\Gamma_j)$ into $I(\Gamma'_{i_j})$. Thus, for each k, the image of $I(\Gamma_k)$ under permutation P equals exactly to some $I(\Gamma_{i_k})$, for each k. Denote by P_k the permutation of $\{1, 2, \cdots, n_k\}$ into itself with $P_k(s - n_{k-1}) = P(s) - m_{i_k-1}$, where $s \in I(\Gamma'_k)$ and $P(s)$ is the image of s under permutation P. Then we have $P_k^T Q'_k P_k = Q_{i_k}$. Let $\hat{P}$ be a permutation that permutes $Q_{i_1}, Q_{i_2}, \cdots, Q_{i_l}$ into $Q_1, Q_2, \cdots, Q_l$. Then $P = \mathrm{diag}[P_1, P_2, \cdots, P_l]\hat{P}$, and the lemma follows.   □

The following theorem is a slightly revised version of a theorem in [9], which is proved for adjacency matrices of graphs and the proof can be carried out without difficulty to integral symmetric matrices.

Theorem 3.3 (cf. [9]) *Let A be an integral symmetric matrix. Suppose that $\phi(A)$ satisfies* (3). *Then there exists an integral symmetric matrix B such that condition* (1) *holds iff there exist two symmetric, rational orthogonal matrices Q_1 and Q_2 such that B can be written as follows*:

$$B = (DP^T \begin{bmatrix} Q_1 & O \\ O & I_1 \end{bmatrix} P) A (P^T \begin{bmatrix} Q_1 & O \\ O & I_1 \end{bmatrix} PD)$$

$$= (DP^T \begin{bmatrix} I_2 & O \\ O & Q_2 \end{bmatrix} P)A(P^T \begin{bmatrix} I_2 & O \\ O & Q_2 \end{bmatrix} PD), \tag{4}$$

where I_1 and I_2 are identity matrices, and P is some permutation matrix and D is a diagonal orthogonal matrix.

Proof (a sketch) By a theorem in [9], there exists a matrix B such that condition (1) holds iff there exist two symmetric, rational orthogonal matrices Q_1 and Q_2 such that PBP^T can be written as follows (permuting rows and columns of A and B simultaneously, if necessary):

$$PBP^T = (\Lambda \begin{bmatrix} Q_1 & O \\ O & \Lambda_1 \end{bmatrix})(PAP^T)(\begin{bmatrix} Q_1 & O \\ O & \Lambda_1 \end{bmatrix} \Lambda)$$

$$= (\Lambda \begin{bmatrix} \Lambda_2 & O \\ O & Q_2 \end{bmatrix})(PAP^T)(\begin{bmatrix} \Lambda_2 & O \\ O & Q_2 \end{bmatrix} \Lambda), \tag{5}$$

where Λ_1 and Λ_2 are diagonal orthogonal matrices, P is some permutation matrix and Λ is some diagonal orthogonal matrix.

Let $D = P^T \Lambda P$. Then (4) follows immediately from (5).   □

Proof of Theorem 1.1 We prove the theorem by actually finding the group $G(A)$.

First suppose that for any integral symmetric matrix B with A and B satisfying condition (1), B can be written as $B = DAD$ for some diagonal orthogonal matrix D, then $G(A)$ can be chosen to be the trivial group with an identity matrix. Theorem 1.1 trivially holds. Next we will assume that there exists an integral symmetric matrix B such that A and B satisfy condition (1), while A and B are not similar through any diagonal orthogonal matrix.

It is easy to see that Theorem 1.1 holds for matrices A and B iff it holds for PAP^T and PBP^T with P being a permutation matrix. By Theorem 3.3, it suffices to assume that there exist symmetric, orthogonal matrices Q_1 and Q_2 such that

$$
\begin{aligned}
B &= (D \begin{bmatrix} Q_1 & O \\ O & I_1 \end{bmatrix}) A (\begin{bmatrix} Q_1 & O \\ O & I_1 \end{bmatrix} D) \\
&= (D \begin{bmatrix} I_2 & O \\ O & Q_2 \end{bmatrix}) A (\begin{bmatrix} I_2 & O \\ O & Q_2 \end{bmatrix} D).
\end{aligned}
\tag{6}
$$

Clearly Q_1 and Q_2 are not $\pm$identity matrices, for otherwise A and B would be similar through a diagonal orthogonal matrix. Without loss of generality we can assume that $Q_1 = \text{diag}[\hat{Q}_1, \hat{Q}_2 \cdots, \hat{Q}_k]$ and $Q_2 = \text{diag}[\hat{Q}_{k+1}, \hat{Q}_{k+2}, \cdots, \hat{Q}_l]$, where the underlying graph of each $\hat{Q}_i$ is connected.

Let $I \subset \{1, 2, \cdots, l\}$, define $G(A)$ to be the set of all symmetric, rational orthogonal matrices obtained from $Q =: \text{diag}[\hat{Q}_1, \hat{Q}_2, \cdots, \hat{Q}_k, \hat{Q}_{k+1}, \cdots, \hat{Q}_l]$ by replacing $\hat{Q}_i$ with an identity matrix of the same order, for $i \in I$ and all subsets I. It is easy to verify that $G(A)$ form a group under matrix multiplication. We claim that $G(A)$ satisfies conditions of Theorem 1.1.

Let $U \in G(A)$ with index set I (i.e., U is generated from Q by replacing $\hat{Q}_i$ with an identity matrix, for $i \in I$). Let $U_1 \in G(A)$ with index set $I^c = \{1, 2, \cdots, \} - I$. Note that $UU_1^T = Q$, we get $M =: U^T AU = U_1^T AU_1$. Clearly we have $\phi(M) = \phi(A)$. By the first equality of the above equation we get $M_i = U_i^T A_i U_i$ for $i \in I$, and hence $\phi(M_i) = \phi(A_i)$ for $i \in I$. Similarly, it follows from the second equality that $\phi(M_j) = \phi(A_j)$ for $j \in I^c$. Thus A and M satisfy (1).

Now let C be any integral symmetric matrix such that A and C satisfy condition (1), whereas A and C are not similar through any diagonal orthogonal matrix (the opposite case is trivial). It remains to show that there exists some $U \in G(A)$ and some diagonal orthogonal matrix D such that $C = (UD)^T A(UD)$ holds.

According to Theorem 3.3, there exist symmetric, rational orthogonal matrices Q_1' and Q_2' (which are not $\pm I$) such that

$$
\begin{aligned}
C &= (D'P'^T \begin{bmatrix} Q_1' & O \\ O & I_1' \end{bmatrix} P') A (P'^T \begin{bmatrix} Q_1' & O \\ O & I_1' \end{bmatrix} P'D') \\
&= (D'P'^T \begin{bmatrix} I_2' & O \\ O & Q_2' \end{bmatrix} P') A (P'^T \begin{bmatrix} I_2' & O \\ O & Q_2' \end{bmatrix} P'D'),
\end{aligned}
\tag{7}
$$

where P' is some permutation matrix, and D' is a diagonal orthogonal matrix. From the second equalities in (6) and (7) we get

$$A\left(\begin{bmatrix} Q_1 & O \\ O & Q_2 \end{bmatrix}\right) = \left(\begin{bmatrix} Q_1 & O \\ O & Q_2 \end{bmatrix}\right)A, \tag{8}$$

$$A\left(P'^T \begin{bmatrix} Q'_1 & O \\ O & Q'_2 \end{bmatrix} P'\right) = \left(P'^T \begin{bmatrix} Q'_1 & O \\ O & Q'_2 \end{bmatrix} P'\right)A. \tag{9}$$

That is, both matrices $\begin{bmatrix} Q_1 & O \\ O & Q_2 \end{bmatrix}$ and $P'^T \begin{bmatrix} Q'_1 & O \\ O & Q'_2 \end{bmatrix} P'$ commute with A.

By Lemma 3.1, we obtain that $\begin{bmatrix} Q_1 & O \\ O & Q_2 \end{bmatrix} = \pm P'^T \begin{bmatrix} Q'_1 & O \\ O & Q'_2 \end{bmatrix} P'$. First assume that

$$\begin{bmatrix} Q_1 & O \\ O & Q_2 \end{bmatrix} = P'^T \begin{bmatrix} Q'_1 & O \\ O & Q'_2 \end{bmatrix} P'. \tag{10}$$

Choose some permutation matrices P_1 and P_2 such that

$$P_1^T Q'_1 P_1 = \text{diag}[\bar{Q}_1, \bar{Q}_2, \cdots, \bar{Q}_r], \text{ and } P_2^T Q'_2 P_2 = \text{diag}[\bar{Q}_{r+1}, \cdots, \bar{Q}_s],$$

where the underlying graph of each $\bar{Q}_i$ is connected.

It follows from (10) that matrices $\text{diag}[\hat{Q}_1, \hat{Q}_2 \cdots, \hat{Q}_k, \hat{Q}_{k+1}, \hat{Q}_{k+2}, \cdots, \hat{Q}_l]$ and $\text{diag}[\bar{Q}_1, \bar{Q}_2, \cdots, \bar{Q}_r, \bar{Q}_{r+1}, \cdots, \bar{Q}_s]$ are similar through permutation matrix $\text{diag}[P_1^T, P_2^T]P'$. By Lemma 3.2, we get that $l = s$ and

$$\text{diag}[P_1^T, P_2^T]P' = \text{diag}[\hat{P}_1, \hat{P}_2, \cdots, \hat{P}_l]\hat{P},$$

where $\hat{P}_i$ is a permutation matrix of the same order as $\bar{Q}_i$ and $\hat{P}$ is a permutation matrix such that $\text{diag}[\hat{Q}_1, \hat{Q}_2 \cdots, \hat{Q}_l] = \hat{P}^T \text{diag}[\hat{Q}_{i_1}, \hat{Q}_{i_2}, \cdots, \hat{Q}_{i_l}]\hat{P}$, where $\hat{Q}_{i_1}, \hat{Q}_{i_2}, \cdots, \hat{Q}_{i_l}$ are permutations of $\hat{Q}_1, \hat{Q}_2 \cdots, \hat{Q}_l$, and $\hat{Q}_{i_j} = \hat{P}_j^T \bar{Q}_j \hat{P}_j$ for each $j = 1, 2, \cdots, l$. Thus $P' = \text{diag}[P_1, P_2]\text{diag}[\hat{P}_1, \hat{P}_2, \cdots, \hat{P}_l]\hat{P}$.

Therefore, $P'^T \begin{bmatrix} Q'_1 & O \\ O & I'_1 \end{bmatrix} P'$ equals

$$\hat{P}^T \begin{bmatrix} \hat{P}_1^T & & \\ & \ddots & \\ & & \hat{P}_l^T \end{bmatrix} \begin{bmatrix} P_1^T & O \\ O & P_2^T \end{bmatrix} \begin{bmatrix} Q'_1 & O \\ O & I'_1 \end{bmatrix} \begin{bmatrix} P_1 & O \\ O & P_2 \end{bmatrix} \begin{bmatrix} \hat{P}_1 & & \\ & \ddots & \\ & & \hat{P}_l \end{bmatrix} \hat{P}$$

$$= \hat{P}^T \begin{bmatrix} \hat{P}_1^T & & \\ & \ddots & \\ & & \hat{P}_l^T \end{bmatrix} \begin{bmatrix} \bar{Q}_1 & & & \\ & \ddots & & \\ & & \bar{Q}_r & \\ & & & I'_1 \end{bmatrix} \begin{bmatrix} \hat{P}_1 & & \\ & \ddots & \\ & & \hat{P}_l \end{bmatrix} \hat{P}$$

$$= \hat{P}^T \begin{bmatrix} \hat{Q}_{i_1} & & & \\ & \ddots & & \\ & & \hat{Q}_{i_r} & \\ & & & I'_1 \end{bmatrix} \hat{P} \in G(A). \tag{11}$$

It follows from (7) and (11) that $C = (UD')^T A(UD')$, where $U = P'^T \begin{bmatrix} Q'_1 & O \\ O & I'_1 \end{bmatrix} P' \in G(A)$, as claimed.

It remains to consider the case $\begin{bmatrix} Q_1 & O \\ O & Q_2 \end{bmatrix} = -P'^T \begin{bmatrix} Q'_1 & O \\ O & Q'_2 \end{bmatrix} P'$, from which we get $\begin{bmatrix} -Q_1 & O \\ O & -Q_2 \end{bmatrix} = P'^T \begin{bmatrix} Q'_1 & O \\ O & Q'_2 \end{bmatrix} P'$. Using the same arguments as above, a similar result can also be obtained. This completes the proof. □

4 Some remarks

We end the paper by giving a few remarks.

1. If the underlying graphs of Q_1 and Q_2 (which are not diagonal matrices) are connected, then $G(A)$ can be simply chosen to be $\{I_n, U_1, U_2, U_1U_2\}$, where $U_1 = \begin{bmatrix} Q_1 & O \\ O & I_1 \end{bmatrix}$ and $U_2 = \begin{bmatrix} I_2 & O \\ O & Q_2 \end{bmatrix}$. Under such a situation, there is essentially a unique (up to similarity through a diagonal orthogonal matrix) integral symmetric matrix

$$B = U_1^T A U_1 = U_2^T A U_2 \tag{12}$$

such that (1) holds (except for the trivial case that $B = DAD$ for some diagonal orthogonal matrix D).

We mention that this is not always the case, namely, there are numerical examples showing that the number of connected components of the underlying graphs of Q_1 and Q_2 can be larger than 1, even if $\phi(A)$ can be decomposed exactly into two distinct, irreducible polynomials.

2. Conjecture 1 does not hold without the modification of replacing U with UD for some diagonal orthogonal matrix D. Let A be an integral symmetric matrix and $Q = \text{diag}[Q_1, Q_2]$ a symmetric, rational orthogonal matrix that commutes with A. Assume further that the underlying graphs of Q_1 and Q_2 are connected (such an A with the above property does exist; see [9]).

Let B be defined as (12). Note that A and B satisfy (1). If Conjecture 1 is true, then there exists $U \in G(A)$ such that $B = U^T AU$. It is easy to see $U = \pm U_1$ or $\pm U_2$. Moreover, let D be any diagonal orthogonal matrix. Then $C =: DAD$ and A satisfy condition (1). Let $C = U^T AU$, $U \in G(A)$, then $U = \pm D$ or $\pm QD$. Since $G(A)$ is a group, we have $DU \in G(A)$, where $U = \pm U_1$ or $\pm U_2$. Thus $(DU)^T A(DU)$ and A satisfy (1).

By the previous discussions, we distinguish two cases: either $(DU)^T A(DU) = D'AD'$ or $(DU)^T A(DU) = D'BD' = D'U_1^T AU_1 D'$, where D' is some diagonal orthogonal matrix. In the former case, it follows from Lemma 3.1 that $DUD' = \pm I$ or $\pm Q$; it is impossible. For the latter, we obtain that $DUD'U_1 = \pm I$ or $\pm Q$. That is, $DU = \pm U_1 D'$ or $DU = \pm U_2 D'$. Therefore, we have $DU_1 = \pm U_1 D'$ or $DU_2 = \pm U_2 D'$. Let $D = \text{diag}[D_1, D_2]$ and $D' = \text{diag}[D'_1, D'_2]$. It follows that $D_1 Q_1 = Q_1 D'_1$ or $D_2 Q_2 = Q_2 D'_2$, where D_1 (resp. D_2) is *any* diagonal orthogonal matrix of the same order as Q_1 (resp. Q_2), and D'_1 (resp. D'_2) is *some* diagonal orthogonal matrix of the same order as Q_1 (resp. Q_2).

At this point, it is not difficult to construct another counterexample to Conjecture 1. In [9], an example of a 16×16 (0,1)-symmetric matrix A is given that commutes

with $Q = \text{diag}[Q_1, Q_2]$, where $Q_1 = Q_2 = \frac{1}{4}J - I$, and J and I are the all-one matrix and the identity matrix of order 8, respectively. If Conjecture 1 is true, then for any diagonal orthogonal matrix D of order 8, there exists some diagonal orthogonal matrix D' of order 8, such that $D(\frac{1}{4}J - I) = (\frac{1}{4}J - I)D'$. Comparing the diagonal entries of both sides gives $D = D'$. Thus we have $DJ = JD$ holds for any D, which gives a contradiction if we let $D = \text{diag}[-1, 1, \cdots, 1]$.

3. It seems that the truthfulness of Theorem 1.1 is closely related to the factorization properties of the characteristic polynomial $\phi(A)$ of matrix A. It would be interesting to give some further results in this direction of research.

References

1. Godsil, C.D., McKay, B.D.: Spectral conditions for the reconstructibility of a graph. J. Comb. Theory, Ser. B **30**(3), 285–289 (1981)
2. He, H.: Reconstruction and higher dimensional geometry. J. Comb. Theory, Ser. B **97**(3), 421–429 (2007)
3. He, H.: Eigenvectors and reconstruction. Electron. J. Comb. **14**(1) (2007)
4. Herndon, W.C., Ellzey, M.L. Jr.: Isospectral graphs and molecules. Tetrahedron **31**, 99–107 (1975)
5. Schwenk, A.J.: Spectral reconstruction problem. Ann. N.Y. Acada. Sci. **328**, 183–189 (1979)
6. Sloane, N.J.A.: A Library of Hadamard Matrices, available at the website: http://www.research.att.com/~njas/hadamard/
7. Tutte, W.T.: All the king's horses (A guide to reconstruction). In: Graph Theory and Related Topics, pp. 15–33. Academic Press, San Diego (1979)
8. Wang, W.: A uniqueness theorem on matrices and reconstruction, J. Combin. Theory, Ser. B (to appear)
9. Wang, W., Xu, C.X.: Some results on the spectral reconstruction problem. Linear Algebra Appl. **427**, 151–158 (2007)