Some families of density matrices for which separability is easily tested

Samuel L. Braunstein,[1] Sibasish Ghosh,[1] Toufik Mansour,[2] Simone Severini,[1] and Richard C. Wilson[1]
[1]*University of York, Heslington, York YO10 5DD, United Kingdom*
[2]*University of Haifa, 31905 Haifa, Israel*
(Received 3 August 2005; revised manuscript received 8 November 2005; published 18 January 2006)

We reconsider density matrices of graphs as defined in quant-ph/0406165. The density matrix of a graph is the combinatorial Laplacian of the graph normalized to have unit trace. We describe a simple combinatorial condition (the "degree condition") to test the separability of density matrices of graphs. The condition is directly related to the Peres-Horodecki partial transposition condition. We prove that the degree condition is necessary for separability, and we conjecture that it is also sufficient. We prove special cases of the conjecture involving nearest-point graphs and perfect matchings. We observe that the degree condition appears to have a value beyond the density matrices of graphs. In fact, we point out that circulant density matrices and other matrices constructed from groups always satisfy the condition and indeed are separable with respect to any split. We isolate a number of problems and delineate further generalizations.

DOI: 10.1103/PhysRevA.73.012320 PACS number(s): 03.67.Mn

I. INTRODUCTION

Let us consider the set $\mathcal{S}$ of all density matrices ρ of a bipartite system with assigned Hilbert space $\mathbb{C}_A^p \otimes \mathbb{C}_B^q$. Let $\mathcal{M}(pq)$ be the linear space (over the complex field $\mathbb{C}$) of all $pq \times pq$ complex matrices equipped with the inner product $\langle A|B\rangle := \mathrm{Tr}(A^\dagger B)$ for any $A, B \in \mathcal{M}(pq)$. Let us consider the metric $D(A,B) := \langle (A-B)|(A-B)\rangle$ on $\mathcal{M}(pq)$, for any $A, B \in \mathcal{M}(pq)$. With respect to this metric, the set $\mathcal{S}$ forms a compact (which is also convex) subset of $\mathcal{M}(pq)$ generated by (p^2q^2-1) real parameters. Deciding whether a given element from this compact set $\mathcal{S}$ is separable or entangled (the *separability problem*) is known to be NP hard [18] (see also [1]). This problem is an instance of the weak membership problem as defined by Grötschel *et al.* [2] (see also [3]). Recently the separability problem has been considered and discussed in [1,4–6].

There are few cases where the separability problem is known to be efficiently solvable. The best known situation is $(p,q)=(2,3)$ or (3, 2). In this case, the positivity of ρ^{Γ_B} (the partial transposition of ρ with respect to the system B) is equivalent to the separability of ρ [7,8]. Also, the set of all density matrices "very near" (in the sense of some useful metric) to the maximally mixed state is known to be separable [9]. Other examples are given in [10].

For some discrete family of density matrices (that is, for which no continuity argument can be applied), no such efficient criterion is known to us. Here we consider the family of the *density matrices of graphs* as introduced in [11]. In the remainder of this section we introduce some terminology and state the results. There are two other sections in the paper: Section II contains the proofs. Section III is a list of further problems and generalizations.

Let $G=(V,E)$ be a simple graph on n labeled vertices—that is, $V=\{v_1,v_2,\ldots,v_n\}$ and $E \subseteq V^2 = \{\{v_i,v_j\}: v_i, v_j \in V \text{ and } i \neq j\}$. The *adjacency matrix* of G is an $n \times n$ matrix, denoted by $M(G)$, with lines indexed by the vertices of G and ijth entry defined as

$$[M(G)]_{i,j} = \begin{cases} 1, & \text{if } \{v_i,v_j\} \in E(G), \\ 0, & \text{if } \{v_i,v_j\} \notin E(G). \end{cases}$$

The *degree matrix* of G is an $n \times n$ matrix, denoted by $\Delta(G)$, with ijth entry defined as

$$[\Delta(G)]_{i,j} = \begin{cases} |\{v_j:\{v_i,v_j\} \in E\}|, & \text{if } i=j, \\ 0, & \text{if } i \neq j. \end{cases}$$

The *Laplacian* [12] of G is the symmetric positive semidefinite matrix

$$L(G) := \Delta(G) - M(G).$$

Other than this combinatorial Laplacian, there are several other types of Laplacians associated with graphs [13]. The matrix

$$\rho(G) := \frac{1}{2|E|} L(G)$$

is a density matrix. This is called the *density matrix of G* [11].

It should be noted here that the notion of density matrix $\rho(G)$ of a graph $G=(V(G),E(G))$, as defined above, is completely different from the notion of "graph states," introduced by Briegel and Raussendorf [14]. A graph state $|G\rangle$, corresponding to a (simple) graph $G=(V(G),E(G))$ is a common eigenstate (corresponding to the eigenvalue 1) of the $n=|V(G)|$ number of n-qubit operators $\sigma_{11}\otimes\sigma_{12}\otimes\cdots\otimes\sigma_{1n}$, $\sigma_{21}\otimes\sigma_{22}\otimes\cdots\otimes\sigma_{2n},\ldots,$ $\sigma_{n1}\otimes\sigma_{n2}\otimes\cdots\otimes\sigma_{nn}$, where (i) $\sigma_{ii}=\sigma_x$ for all $i \in \{1,2,\ldots,n\}$, (ii) for $j \neq i$, $\sigma_{ij}=\sigma_z$ if the vertices v_i and v_j of G are connected by an edge, and (iii) for $j \neq i$, $\sigma_{ij}=I$ if the vertices v_i and v_j of G are not connected by an edge. Thus, in this formalism, a two-level system is attached with each vertex of the graph and each edge of the graph represents an interaction (Ising type) between the two two-level subsystems attached to the two vertices of the edge.

Let G be a graph on $n=p\cdot q$ vertices $v_1, v_2, \ldots, v_n$. These vertices are represented here as ordered pairs in the following way: $v_1=(u_1,w_1)\equiv u_1w_1$, $v_2=(u_1,w_2)\equiv u_1w_2,\ldots$, $v_q=(u_1,w_q)\equiv u_1w_q$, $v_{q+1}=(u_2,w_1)\equiv u_2w_1$, $v_{q+2}=(u_2,w_2)\equiv u_2w_2,\ldots$, $v_{2q}=(u_2,w_q)\equiv u_2w_q,\ldots\ldots$, $v_{(p-1)q+1}=(u_p,w_1)\equiv u_pw_1$, $v_{(p-1)q+2}=(u_p,w_2)\equiv u_pw_2,\ldots$, $v_{pq}=(u_p,w_q)\equiv u_pw_q$. We associate to this graph G on n labeled vertices (described above) the orthonormal basis $\{|v_i\rangle : i=1,2,\ldots,n\}=\{|u_j\rangle\otimes|w_k\rangle : j=1,2,\ldots,p; k=1,2,\ldots,q\}$, where $\{|u_j\rangle : j=1,2,\ldots,p\}$ and $\{|w_k\rangle : k=1,2,\ldots,q\}$ are orthonormal bases of the Hilbert spaces $\mathcal{H}_A\cong\mathbb{C}^p$ and $\mathcal{H}_B\cong\mathbb{C}^q$, respectively. The *partial transpose* of a graph $G=(V,E)$ (with respect to $\mathcal{H}_B$), denoted by $G^{\Gamma_B}=(V,E')$, is the graph such that $\{u_iw_j,u_kw_l\}\in E'$ if and only if $\{u_iw_l,u_kw_j\}\in E$. We propose the following conjecture.

Conjecture 1. Let $\rho(G)$ be the density matrix of a graph on $n=pq$ vertices. Then $\rho(G)$ is separable in $\mathbb{C}_A^p\otimes\mathbb{C}_B^q$ if and only if $\Delta(G)=\Delta(G^{\Gamma_B})$.

A proof of this conjecture would give a simple method for testing the separability of density matrices of graphs, as we would only need to check whether the $n\times n$ diagonal matrices $\Delta(G)$ and $\Delta(G^{\Gamma_B})$ are equal. This fact is in some sense analogous to the fact that the separability of all two-mode Gaussian states (which form a continuous family) is equivalent to the Peres-Horodecki partial transposition criterion [15]. We prove one side of our conjecture.

Theorem 2. Let $\rho(G)$ be the density matrix of a graph on $n=pq$ vertices. If $\rho(G)$ is separable in $\mathbb{C}_A^p\otimes\mathbb{C}_B^q$, then $\Delta(G)=\Delta(G^{\Gamma_B})$.

We prove the other side of the conjecture for the following two families of graphs.

(i) Consider a rectangular lattice with pq points arranged in p rows and q columns, such that the distance between two neighboring points on the same row or in the same column is 1. A *nearest-point graph* is a graph whose vertices are identified with the points of the lattice and the edges have length 1 or $\sqrt{2}$.

(ii) A *perfect matching* is a graph $G=(V,E)$ such that for every v_i there is a unique vertex v_j such that $\{v_i,v_j\}\in E$.

Namely, we prove the following two theorems.

Theorem 3. Let G be a nearest point graph on $n=pq$ vertices. Then the density matrix $\rho(G)$ is separable in $\mathbb{C}_A^p\otimes\mathbb{C}_B^q$ iff $\Delta(G)=\Delta(G^{\Gamma_B})$.

Theorem 4. Let G be a perfect matching on $n=2k$ vertices. Then the density matrix $\rho(G)$ is separable in $\mathbb{C}_A^k\otimes\mathbb{C}_B^2$ iff $\Delta(G)=\Delta(G^{\Gamma_B})$.

See Fig. 1 as examples of perfect matching H, the partial transpose graph H^{Γ_B}, nearest-point graph G, and the partial-transpose graph G^{Γ_B}.

The *degree condition* expressed in the conjecture appears to have value beyond density matrices of graphs. In general, given a density matrix ρ in $\mathbb{C}_A^p\otimes\mathbb{C}_B^q$, let $\Delta(\rho)$ be the matrix defined as follows:

$$[\Delta(\rho)]_{i,j}=\begin{cases}\displaystyle\sum_{k=1}^{pq}\rho_{ik}, & \text{if } i=j,\\ 0, & \text{if } i\neq j.\end{cases}$$

In a *circulant matrix* each row is a cyclic shift of the row above to the right. This means that a circulant matrix is then defined by its first row. Let G be a finite group of order n, and let σ be the regular permutation representation of G. Then σ is an homomorphism from G to the set of permutation matrices of dimension n. The *Fourier transform* (evaluated at σ) of a complex-valued function f on G is defined as the matrix $\hat{f}=\Sigma f(g)\sigma(g)$ [16]. According to this definition, a complex circulant matrix M of dimension n has the form $M=\Sigma_{g\in\mathbb{Z}_n}f(g)\sigma(g)$. We prove the following result.

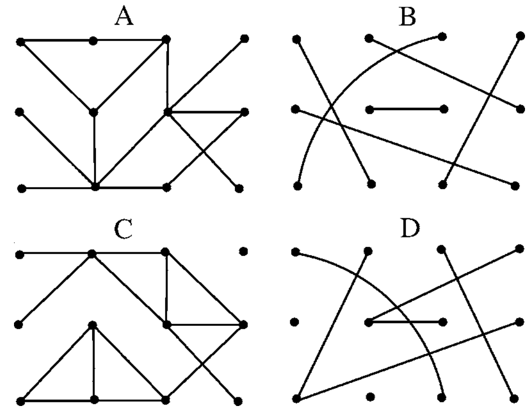

FIG. 1. (A) A nearest-point graph G, (B) a perfect matching H, (C) the partial-transpose graph G^{Γ_B}, and (D): the partial-transpose graph H^{Γ_B}.

Theorem 5. Let ρ be a circulant density matrix of dimension $n=pq$. Then $\Delta(\rho)=\Delta(\rho^{\Gamma_B})$ and ρ is separable in $\mathbb{C}_A^p\otimes\mathbb{C}_B^q$. Let $\rho=\Sigma_{g\in\mathbb{Z}_2^n}f(g)\sigma(g)$ be a density matrix of dimension 2^n. Then $\Delta(\rho)=\Delta(\rho^{\Gamma_B})$ and ρ is separable in $\mathbb{C}_A^{2^k}\otimes\mathbb{C}_B^{2^l}$, where $k+l=n$.

II. PROOFS

A. Proof of theorem 2

Let $L(G)$ be the Laplacian of a graph $G=(V,E)$ on n vertices $v_1,\ldots,v_n$. Let D be any $n\times n$ real diagonal matrix in the orthonormal basis $\{|v_1\rangle,\ldots,|v_n\rangle\}$ such that $D\neq 0$ and $\mathrm{tr}(D)=0$. It follows that there is at least one negative entry in the diagonal of D. Let this entry be $D_{i,i}=b_i$. Let $|\psi_0\rangle=\Sigma_{j=1}^n|v_j\rangle$ and $|\phi\rangle=\Sigma_{j=1}^n\chi_j|v_j\rangle$, where

$$\chi_j=\begin{cases}0, & \text{if } j\neq i,\\ k & \text{if } j=1,\end{cases}$$

Let $|\chi\rangle=|\psi_0\rangle+|\phi\rangle=\Sigma_{j=1}^n(1+\chi_j)|v_j\rangle$. Then,

$$\begin{aligned}\langle\chi|(L(G)+D)|\chi\rangle &= \langle\chi|L(G)|\chi\rangle+\langle\chi|D|\chi\rangle\\ &= \langle\psi_0|L(G)|\psi_0\rangle+\langle\psi_0|L(G)|\phi\rangle+\langle\phi|L(G)\\ &\quad\times|\psi_0\rangle+\langle\phi|L(G)|\phi\rangle+\langle\psi_0|D|\psi_0\rangle\\ &\quad+\langle\psi_0|D|\phi\rangle+\langle\phi|D|\psi_0\rangle+\langle\phi|D|\phi\rangle.\end{aligned}$$

The state $|\psi_0\rangle$ is an eigenvector (unnormalized) of $L(G)$, corresponding to the eigenvalue 0: $L(G)|\psi_0\rangle=0$. Also $\langle\psi_0|D|\psi_0\rangle=\mathrm{tr}(D)=0$. Then,

$$\langle\chi|(L(G)+D)|\chi\rangle = \langle\psi_0|L(G)|\phi\rangle + \langle\phi|L(G)|\phi\rangle + \langle\psi_0|D|\phi\rangle + \langle\phi|D|\psi_0\rangle + \langle\phi|D|\phi\rangle.$$

Now $\langle\psi_0|L(G)|\phi\rangle = \langle\phi|L(G)^T|\psi_0\rangle = \langle\phi|L(G)|\psi_0\rangle = 0$. In fact, $L(G)=L(G)^T$. Let $[L(G)]_{j,l}$ be the jlth entry of $L(G)$ with respect to the basis $\{|v_1\rangle,\ldots,|v_n\rangle\}$. Let $d_i = |\{v_j : \{v_i,v_j\}\in E\}|$. We have

$$\langle\phi|L(G)|\phi\rangle = k^2(L(G))_{i,i} = k^2 d_i,$$

$$\langle\phi|D|\phi\rangle = b_i k^2,$$

$$\langle\psi_0|D|\phi\rangle = b_i k,$$

$$\langle\phi|D|\psi_0\rangle = b_i k.$$

Thus,

$$\langle\chi|(L(G)+D)|\chi\rangle = k^2(d_i+b_i) + 2b_i k, \quad \text{with } d_i \geqslant 0 \text{ and } b_i < 0.$$

So we can then always choose a positive k, small enough, such that

$$2b_i k + k^2(d_i+b_i) < 0.$$

It follows that

$$L(G) + D \ngeq 0.$$

For any graph G on $n=pq$ vertices,

$$v_1 = (u_1,w_1), v_2 = (u_1,w_2), \ldots, v_q = (u_1,w_q), v_{q+1} = (u_2,w_1), v_{q+2} = (u_2,w_2), \ldots, v_{2q} = (u_2,w_q), \ldots, v_{pq} = (u_p,w_q),$$

consider now the degree condition $\Delta(G)=\Delta(G^{\Gamma_B})$. Now,

$$(L(G))^{\Gamma_B} = [\Delta(G) - \Delta(G^{\Gamma_B})] + L(G^{\Gamma_B}).$$

Let

$$D = \Delta(G) - \Delta(G^{\Gamma_B}).$$

Then D is an $n\times n$ real diagonal matrix with respect to the orthonormal basis

$$|v_1\rangle = |u_1\rangle\otimes|w_1\rangle, \ldots, |v_{pq}\rangle = |u_p\rangle\otimes|w_q\rangle.$$

Also,

$$\mathrm{tr}(D) = \mathrm{tr}[\Delta(G)] - \mathrm{tr}[\Delta(G^{\Gamma_B})] = 0.$$

As G^{Γ_B} is a graph on n vertices $v_1, v_2, \ldots, v_n$, as here $D = \Delta(G) - \Delta(G^{\Gamma_B})$ is a diagonal matrix with respect to the orthonormal basis $\{|v_1\rangle,|v_2\rangle,\ldots,|v_n\rangle\}$, and as here $\mathrm{tr}(D)=0$, therefore, by the above-mentioned reasoning, $D + L(G^{\Gamma_B}) \ngeq 0$ if $D\neq 0$. Now if $\rho(G)$ is separable then we must have $L(G)^{\Gamma_B}$ $(=D+L(G^{\Gamma_B})) \geqslant 0$ [8]. Therefore separability of $L(G)$ implies that $D=\Delta(G)-\Delta(G^{\Gamma_B})=0$.

B. Proof of theorem 3

Let G be a nearest-point graph on $n=pq$ vertices and m edges. We associate to G the orthonormal basis $\{|v_i\rangle : i=1,2,\ldots,n\} = \{|u_j\rangle\otimes|w_k\rangle : j=1,2,\ldots,p; k=1,2,\ldots,q\}$, where $\{|u_j\rangle : j=1,2,\ldots,p\}$ is an orthonormal basis of $\mathbb{C}_A^p$ and $\{|w_k\rangle : k=1,2,\ldots,q\}$ is an orthonormal basis of $\mathbb{C}_B^q$. Let $j,j' \in\{1,2,\ldots,p\}$ and $k,k'\in\{1,2,\ldots,q\}$. Let $\lambda_{jk,j'k'}\in\{0,1\}$ be defined as follows:

$$\lambda_{jk,j'k'} = \begin{cases} 1, & \text{if } \{u_jw_k, u_{j'}w_{k'}\}\in E,\\ 0, & \text{if } \{u_jw_k, u_{j'}w_{k'}\}\notin E. \end{cases} \tag{2.1}$$

Thus, for the above-mentioned nearest-point graph G, $\lambda_{jk,j'k'}$ can have nonzero values only in the following cases: either (i) $j'=j$ and $k'=k+1$, (ii) $j'=j+1$ and $k'=k$, (iii) $j'=j+1$ and $k'=k+1$, or (iv) a combination of some or all three cases (i)–(iii). Let $\rho(G)$ and $\rho(G^{\Gamma_B})$ be the density matrices corresponding to the graphs G and G^{Γ_B}, respectively. Thus,

$$\rho(G) = \frac{1}{2m}[\Delta(G) - M(G)],$$

$$\rho(G^{\Gamma_B}) = \frac{1}{2m}[\Delta(G^{\Gamma_B}) - M(G^{\Gamma_B})].$$

Let G_1 be the subgraph of G whose edges are all the entangled edges of G. An edge $\{ij,kl\}$ is *entangled* if $i\neq k$ and $j\neq l$. Also let G_1' be the subgraph of G^{Γ_B} corresponding to all the "entangled edges" of G^{Γ_B}. Obviously $G_1' = (G_1)^{\Gamma_B}$. Using the above-mentioned notations, we have

$$\rho(G_1) = \frac{1}{m}\sum_{j=2}^{p}\left(\lambda_{(j-1)1,j2}P\left[\frac{1}{\sqrt{2}}(|u_{(j-1)}w_1\rangle - |u_jw_2\rangle)\right]\right) + \frac{1}{m}\sum_{j=2}^{p}\sum_{k=3}^{q}\left(\lambda_{(j-1)(k-1),j(k-2)}P\left[\frac{1}{\sqrt{2}}(|u_{j-1}w_{k-1}\rangle - |u_jw_{k-2}\rangle)\right] + \lambda_{(j-1)(k-1),jk}P\left[\frac{1}{\sqrt{2}}(|u_{j-1}w_{k-1}\rangle - |u_jw_k\rangle)\right]\right) + \frac{1}{m}\sum_{j=2}^{p}\left(\lambda_{(j-1)q,j(q-1)}P\left[\frac{1}{\sqrt{2}}(|u_{j-1}w_q\rangle - |u_jw_{q-1}\rangle)\right]\right), \tag{2.2}$$

where, for any normalized pure state $|\psi\rangle$, $P[|\psi\rangle]$ denotes the one-dimensional projector onto the vector $|\psi\rangle$. Also we have

$$\rho(G_1') = \frac{1}{m}\sum_{j=2}^{p}\left(\lambda_{(j-1)1,j2}P\left[\frac{1}{\sqrt{2}}(|u_{(j-1)}w_2\rangle - |u_jw_1\rangle)\right]\right) + \frac{1}{m}\sum_{j=2}^{p}\sum_{k=3}^{q}\left(\lambda_{(j-1)(k-1),j(k-2)}P\left[\frac{1}{\sqrt{2}}(|u_{j-1}w_{k-2}\rangle - |u_jw_{k-1}\rangle)\right]\right.$$
$$\left. + \lambda_{(j-1)(k-1),jk}P\left[\frac{1}{\sqrt{2}}(|u_{j-1}w_k\rangle - |u_jw_{k-1}\rangle)\right]\right) + \frac{1}{m}\sum_{j=2}^{p}\left(\lambda_{(j-1)q,j(q-1)}P\left[\frac{1}{\sqrt{2}}(|u_{j-1}w_{q-1}\rangle - |u_jw_q\rangle)\right]\right). \tag{2.3}$$

One can check that

$$\Delta(G_1) = \frac{1}{2m}\left(\lambda_{11,22}P[|u_1w_1\rangle] + \sum_{k=3}^{q}(\lambda_{1(k-1),2(k-2)} + \lambda_{1(k-1),2k})P[|u_1w_{k-1}\rangle] + \lambda_{1q,2(q-1)}P[|u_1w_q\rangle]\right) + \frac{1}{2m}\sum_{j=3}^{p}(\lambda_{(j-2)2,(j-1)1}$$
$$+ \lambda_{(j-1)1,j2})P[|u_{j-1}w_1\rangle] + \frac{1}{2m}\sum_{j=3}^{p}\sum_{k=3}^{q}(\lambda_{(j-2)(k-2),(j-1)(k-1)} + \lambda_{(j-2)k,(j-1)(k-1)} + \lambda_{(j-1)(k-1),j(k-2)} + \lambda_{(j-1)(k-1),jk})P[|u_{j-1}w_{k-1}\rangle]$$
$$+ \frac{1}{2m}\sum_{j=3}^{p}(\lambda_{(j-2)(q-1),(j-1)q} + \lambda_{(j-1)q,j(q-1)})P[|u_{j-1}w_q\rangle] + \frac{1}{2m}\lambda_{(p-1)2,p1}P[|u_pw_1\rangle] + \frac{1}{2m}\sum_{k=3}^{q}(\lambda_{(p-1)(k-2),p(k-1)}$$
$$+ \lambda_{(p-1)k,p(k-1)})P[|u_pw_{k-1}\rangle] + \frac{1}{2m}\lambda_{(p-1)(q-1),pq}P[|u_pw_q\rangle] \tag{2.4}$$

and

$$\Delta(G_1') = \frac{1}{2m}\left(\lambda_{12,21}P[|u_1w_1\rangle] + \sum_{k=3}^{q}(\lambda_{1(k-2),2(k-1)} + \lambda_{1k,2(k-1)})P[|u_1w_{k-1}\rangle] + \lambda_{1(q-1),2q}P[|u_1w_q\rangle]\right) + \frac{1}{2m}\sum_{j=3}^{p}(\lambda_{(j-2)1,(j-1)2}$$
$$+ \lambda_{(j-1)2,j1})P[|u_{j-1}w_1\rangle] + \frac{1}{2m}\sum_{j=3}^{p}\sum_{k=3}^{q}(\lambda_{(j-2)(k-1),(j-1)(k-2)} + \lambda_{(j-2)(k-1),(j-1)k} + \lambda_{(j-1)(k-2),j(k-1)} + \lambda_{(j-1)k,j(k-1)})P[|u_{j-1}w_{k-1}\rangle]$$
$$+ \frac{1}{2m}\sum_{j=3}^{p}(\lambda_{(j-2)q,(j-1)(q-1)} + \lambda_{(j-1)(q-1),jq})P[|u_{j-1}w_q\rangle] + \frac{1}{2m}\lambda_{(p-1)1,p2}P[|u_pw_1\rangle] + \frac{1}{2m}\sum_{k=3}^{q}(\lambda_{(p-1)(k-1),p(k-2)}$$
$$+ \lambda_{(p-1)(k-1),pk})P[|u_pw_{k-1}\rangle] + \frac{1}{2m}\lambda_{(p-1)q,p(q-1)}P[|u_pw_q\rangle]. \tag{2.5}$$

Let G_2 and G_2', respectively, be the subgraphs of G and G^{Γ_B}, each containing all the edges of the forms $\{u_iw_j, u_iw_{j'}\}$ (where $j\neq j'$) as well as $\{u_iw_j, u_{i'}w_j\}$ (where $i\neq i'$). Then it is obvious that $\Delta(G_2)=\Delta(G_2')$, due to the fact that G_2 and G_2' represent the same graph. So $\Delta(G)=\Delta(G^{\Gamma_B})$ if and only if $\Delta(G_1)=\Delta(G_1')$. Using Eqs. (2.4) and (2.5), we see that the equality of $\Delta(G_1)$ and $\Delta(G_1')$ implies that

$$\lambda_{11,22} = \lambda_{12,21},$$

$$\lambda_{1(k-1),2(k-2)} + \lambda_{1(k-1),2k} = \lambda_{1(k-2),2(k-1)} + \lambda_{1k,2(k-1)}, \quad \text{for } k=3,4,\ldots,q,$$

$$\lambda_{1q,2(q-1)} = \lambda_{1(q-1),2q}, \tag{2.6}$$

for each $j\in\{3,44,\ldots,p\}$,

$$\lambda_{(j-2)2,(j-1)1} + \lambda_{(j-1)1,j2} = \lambda_{(j-2)1,(j-1)2} + \lambda_{(j-1)2,j1},$$

$$\lambda_{(j-2)(k-2),(j-1)(k-1)} + \lambda_{(j-2)k,(j-1)(k-1)} + \lambda_{(j-1)(k-1),j(k-2)} + \lambda_{(j-1)(k-1),jk} = \lambda_{(j-2)(k-1),(j-1)(k-2)} + \lambda_{(j-2)(k-1),(j-1)k} + \lambda_{(j-1)(k-2),j(k-1)} + \lambda_{(j-1)k,j(k-1)} \quad \text{for } k=3,4,\ldots,q,$$

$$\lambda_{(j-2)(q-1),(j-1)q} + \lambda_{(j-1)q,j(q-1)} = \lambda_{(j-2)q,(j-1)(q-1)} + \lambda_{(j-1)(q-1),jq}, \tag{2.7}$$

$$\lambda_{(p-1)1,p2} = \lambda_{(p-1)2,p1},$$

$$\lambda_{(p-1)(k-2),p(k-1)} + \lambda_{(p-1)k,p(k-1)} = \lambda_{(p-1)(k-1),p(k-2)} + \lambda_{(p-1)(k-1),pk}, \quad \text{for } k=3,4,\ldots,q,$$

$$\lambda_{(p-1)(q-1),pq} = \lambda_{(p-1)q,p(q-1)}. \tag{2.8}$$

The solution of Eqs. (2.6)–(2.8) is of the form

$$\lambda_{ij,i'j'} = \lambda_{ij',i'j}, \quad \text{for all } i,i' \in \{1,2,\ldots,p\}$$
$$\text{and all } j,j' \in \{1,2,\ldots,q\}, \qquad (2.9)$$

and wherever $\lambda_{ij,i'j'}$ and $\lambda_{ij',i'j}$ are defined. Equation (2.9) shows that whenever there is an entangled edge $\{u_iw_j, u_{i'}w_{j'}\}$ in G (so we must have $i \neq i'$ and $j \neq j'$), there must be the entangled edge $\{u_iw_{j'}, u_{i'}w_j\}$ in G. The two entangled edges $\{u_iw_j, u_{i'}w_{j'}\}$ and $\{u_iw_{j'}, u_{i'}w_j\}$ in G together give rise to the following contribution (which is again a density matrix) in the density matrix $\rho(G)$, with the multiplicative factor $2/m$:

$$\rho(i,i';j,j') = \frac{1}{2}\left(P\left[\frac{1}{\sqrt{2}}(|u_iw_j\rangle - |u_{i'}w_{j'}\rangle)\right] + P\left[\frac{1}{\sqrt{2}}(|u_iw_{j'}\rangle - |u_{i'}w_j\rangle)\right]\right). \qquad (2.10)$$

Let us write

$$\frac{1}{\sqrt{2}}(|u_i\rangle \pm |u_{i'}\rangle) = |V(i,i';\pm)\rangle, \quad \frac{1}{\sqrt{2}}(|w_j\rangle \pm |w_{j'}\rangle)|X(j,j';\pm)\rangle. \qquad (2.11)$$

Using Eq. (2.11), it is easy to see from Eq. (2.10) that

$$\rho(i,i';j,j') = \frac{1}{2}P[|V(i,i';+)X(j,j';-)\rangle] + \frac{1}{2}P[|V(i,i';-)X(j,j';+)\rangle], \qquad (2.12)$$

which is a separable state in $\mathbb{C}_A^p \otimes \mathbb{C}_B^q$. This shows that, under the constraint $\Delta(G_1)=\Delta(G_1')$, $\rho(G_1)$ is nothing but an equal mixture of separable states of the form $\rho(i,i';j,j')$, and so $\rho(G_1)$ must be separable, which, in turn, shows that $\rho(G)$ has to be separable. This shows that a nearest-point graph G is separable in $\mathbb{C}_A^p \otimes \mathbb{C}_B^q$ if and only if $\Delta(G)=\Delta(G^{\Gamma_B})$.

C. Perfect matchings

1. Proof of theorem 4

Definition (degree condition). For any graph G on $n=pq$ vertices $v_1 \equiv (u_1,w_1)$, $v_2 \equiv (u_1,w_2), \ldots$, $v_q \equiv (u_1,w_q)$, $v_{(q+1)} \equiv (u_2,w_1)$, $v_{(q+2)} \equiv (u_2,w_2), \ldots$, $v_{2q} \equiv (u_2,w_q), \ldots$, $v_{(p-1)q+1} \equiv (u_p,w_1)$, $v_{(p-1)q+2} \equiv (u_p,w_2), \ldots$, $v_{pq} \equiv (u_p,w_q)$, the equation $\Delta(G)=\Delta(G^{\Gamma_B})$ is called as the degree condition, where G^{Γ_B} is the graph with $V(G^{\Gamma_B})=V(G)$ and $\{(u_i,w_j),(u_{i'},w_{j'})\} \in E(G^{\Gamma_B})$ if and only if $\{(u_i,w_{j'}),(u_{i'},w_j)\} \in E(G)$.

We consider here only those graphs G on $n=pq$ vertices, where n is even and $E(G)$ consists of edges of the forms $\{(i_k,j_k),(i_k',j_k')\}$, where (i) k runs from 1 up to $n/2$, (ii) $(i_k,j_k) \neq (i_k',j_k')$ for all k, (iii) $(i_k,j_k) \neq (i_l,j_l)$ whenever $k \neq l$, (iv) $(i_k,j_k) \neq (i_l',j_l')$ whenever $k \neq l$, and (v) $(i_k',j_k') \neq (i_l',j_l')$ whenever $k \neq l$. Thus G is nothing but a perfect matching on $n=pq$ vertices. In addition to above-mentioned conditions, if we have $i_k \neq i_k'$ and $j_k \neq j_k'$ for each $k \in \{1,2,\ldots,n/2\}$, then G is called as a *perfect entangling matching*. We denote the set of all such perfect entangling matchings on the same set of $n=pq$ vertices as $\mathcal{P}_{p\cdot q}$. The density matrix $\rho(G)$ of the graph G is given by

$$\rho(G) = \frac{2}{n}\sum_{k=1}^{n/2} P\left[\frac{1}{\sqrt{2}}(|i_kj_k\rangle - |i_k'j_k'\rangle)\right].$$

Let $G \in \mathcal{P}_{p\cdot q}$. Let G^{Γ_B} be the graph with vertex set as $V(G)$ and $\{(i_k,j_k'),(i_k',j_k)\} \in E(G^{\Gamma_B})$ if and only if $\{(i_k,j_k),(i_k',j_k')\} \in E(G)$. Let $\mathcal{P}_{p\cdot q}^S = \{G \in \mathcal{P}_{p\cdot q} : G^{\Gamma_B} \in \mathcal{P}_{p\cdot q}\}$. It can be easily shown that for any perfect matching G on $n=p\cdot q$ vertices, $G \in \mathcal{P}_{p\cdot q}^S$ if and only if $\Delta(G)=\Delta(G^{\Gamma_B})$. Following are the two examples of "canonical" perfect entangling matchings.

(1) Crisscross: A crisscross $\mathcal{C}$ is given by

$$\mathcal{C} = (V(\mathcal{C}) = \{(i_1,1),(i_1,2),(i_2,1),(i_2,2)\}, E(\mathcal{C}) = \{\{(i_1,1),(i_2,2)\},\{(i_2,1),(i_1,2)\}\})$$

(where $i_1 \neq i_2$).

(2) Tally mark: A tally mark $\mathcal{T}$ is given by $\mathcal{T} = (V(\mathcal{T}), E(\mathcal{T}))$ where $V(\mathcal{T}) = \{(i_k,1) : k = 1,2,\ldots,r'\} \cup \{(i_k,2) : k=1,2,\ldots,r'\}$ and

$$E(\mathcal{T}) = \{\{(i_1,1),(i_2,2)\},\{(i_2,1),(i_3,2)\},\ldots,\{(i_{(r'-1)},1),(i_{r'},2)\}, \{(i_{r'},1),(i_1,2)\}\}$$

(where $1 \leq i_1 < i_2 < \ldots < i_{r'} \leq p'$ and $r' \leq p'$).

We are now ready to give a proof of theorem 4.

Proof of theorem 4. Let G be a perfect matching on $n=2p$ vertices $v_1 \equiv (1,1)$, $v_2 \equiv (1,2)$, $v_3 \equiv (2,1)$, $v_4 \equiv (2,2), \ldots$, $v_{(2p-1)} \equiv (p,1)$, $v_{2p} \equiv (p,2)$.

Let us first assume that $\rho(G)$ is separable in $\mathbb{C}_A^p \otimes \mathbb{C}_B^2$. Then, by theorem 2, we have $\Delta(G)=\Delta(G^{\Gamma_B})$.

Next we assume that $\Delta(G)=\Delta(G^{\Gamma_B})$. Let us denote the subgraph of G, consisting of all its unentangled edges, as G_1 and the subgraph of G, consisting of all its entangled edges, as G_2. As G is a perfect matching, therefore G is the disjoint union of G_1 and G_2: $G=G_1 \uplus G_2$. Thus $V(G)$ is the set wise disjoint union of $V(G_1)$ and $V(G_2)$, while $E(G)$ is the set wise disjoint union of $E(G_1)$ and $E(G_2)$. Let us take $E(G_2) = \{\{(i_k,1),(j_k,2)\} : k=1,2,\ldots,q\}$, where q is a non-negative integer with $q \leq p$, $1 \leq i_1 < i_2 < \cdots < i_q \leq p$, $1 \leq j_1, j_2, \ldots, j_q \leq p$, $i_k \neq j_k$ whenever $k=1,2,\ldots,q$, and $j_k \neq j_l$ whenever $k \neq l$. Thus we see that $V(G_2)$ is the (disjoint) union of $\{(i_k,1) : k=1,2,\ldots,q\}$ and $\{(j_k,2) : k=1,2,\ldots,q\}$.

Let us denote the subgraph of G^{Γ_B}, consisting of all its unentangled edges, as G_3, while the subgraph of G^{Γ_B}, consisting of all its entangled edges, is denoted here by G_4. Here $G_1^{\Gamma_B}=G_1=G_3$. This is true for any general graph G on $n=p'\cdot q'$ vertices. Again, for any perfect matching G on $n=p'\cdot q'$ vertices $v_1' \equiv (u_1,w_1)$, $v_2' \equiv (u_1,w_2), \ldots$, $v_{q'}' \equiv (u_1,w_{q'})$, $v_{(q'+1)}' \equiv (u_2,w_1)$, $v_{(q'+2)}' \equiv (u_2,w_2), \ldots$, $v_{2q'}' \equiv (u_2,w_{q'}), \ldots, \ldots$, $v_{((p'-1)q'+1)}' \equiv (u_{p'},w_1)$, $v_{((p'-1)q'+2)}' \equiv (u_{p'},w_2), \ldots$, $v_{p'q'}' \equiv (u_{p'},w_{q'})$, the degree condition $\Delta(G) = \Delta(G^{\Gamma_B})$ implies that (and is implied by) G^{Γ_B} is a perfect matching on the above-mentioned $n=p'\cdot q'$ vertices. So we must have $G^{\Gamma_B}=G_3 \uplus G_4$, and hence, $V(G_4)=V(G_2)$ (this is true for arbitrary values of p' and q' provided $n=p'\cdot q'$ is even). Thus we see that both G_2 and G_4 are perfect entangling matchings on the *same* subset of vertices of G (this is also true for arbitrary values of p' and q' provided n

$=p'\cdot q'$). It then follows that the two subsets $\{i_k:k=1,2,\ldots,q\}$ and $\{j_k:k=1,2,\ldots,q\}$ of $\{1,2,\ldots,p\}$ must be same. This is so because if some $j_k\notin\{i_k:k=1,2,\ldots,q\}$, then vertex $(j_k,1)$ of the (entangled) edge $\{(i_k,2),(j_k,1)\}$ in G_4 will belong to $V(G_1)$ [and hence, to $V(G_3)$]—a contradiction. Therefore, G_2 (and, hence, G_4) is a perfect entangling matching on the set of $2q$ vertices (i,j), where $i\in\{i_1,i_2,\ldots,i_q\}$ and $j\in\{1,2\}$. Note that this fact is true not only for $n=2p$ but for any general $n=p'\cdot q'$, provided n is even [and so, for any $G\in\mathcal{P}_{p'\cdot q'}$, $G\in\mathcal{P}^S_{p'\cdot q'}$ if and only if $\Delta(G)=\Delta(G^{\Gamma_B})$].

Now, it is known that (see lemma 4.4 in [11]) any perfect entangling matching G' on $n=2p'$ vertices $v_1'\equiv(1,1)$, $v_2'\equiv(1,2)$, $v_3'\equiv(2,1)$, $v_4'\equiv(2,2),\ldots$, $v'_{(2p'-1)}\equiv(p',1)$, $v'_{2p'}\equiv(p',2)$ can be transformed in to a "canonical" perfect entangling matching G_0 on the same set of vertices by applying a suitable permutation on the first label of the vertices $v_1',v_2',\ldots,v_{2p'}$, where, by "canonical" perfect entangling matching, we mean either (i) a crisscross, (ii) a tally mark, or (iii) a disjoint union of some tally marks and/or some crisscrosses (this kind of result is still lacking for a general $G\in\mathcal{P}^S_{p'\cdot q'}$ and we do not know what should be the canonical form of such a G). As $\rho(G_0)$ is known to be separable in $\mathbb{C}^{p'}_A\otimes\mathbb{C}^2_B$ (according to lemma 4.5 in [11] together with the fact that the density matrix of a crisscross is always separable), therefore $\rho(G')$ is separable in $\mathbb{C}^{p'}_A\otimes\mathbb{C}^2_B$.

Thus, it follows that $\rho(G_2)$ is separable in $\mathbb{C}^q_A\otimes\mathbb{C}^2_B$ (and hence, in $\mathbb{C}^p_A\otimes\mathbb{C}^2_B$, as the orthonormal basis $\{|i_k\rangle:k=1,2,\ldots,q\}$ of $\mathbb{C}^q_A$ is contained inside the orthonormal basis $\{|l\rangle:l=1,2,\ldots,p\}$ of $\mathbb{C}^p_A$). Also $\rho(G_1)$ is separable in $\mathbb{C}^p_A\otimes\mathbb{C}^2_B$, as G_1 consists of only unentangled edges of G. Now $\rho(G)=(1/p)[(p-q)\rho(G_1)+q\rho(G_2)]$. Hence $\rho(G)$ is separable in $\mathbb{C}^p_A\otimes\mathbb{C}^2_B$. □

During the proof of theorem 4, we have proved the following result.

Corollary 1. Let G be a perfect matching on $n=p\cdot q$ vertices $v_1=(u_1,w_1)$, $v_2=(u_1,w_2),\ldots$, $v_n=(u_p,w_q)$ for which $\Delta(G)=\Delta(G^{\Gamma_B})$. Then G is a disjoint union of N, the number of perfect matchings G_1, $G_2,\ldots$, G_N, where (i) $V(G_i)=\{(u_{ij},w_{ik}):j=1,2,\ldots,p_i;k=1,2,\ldots,q_i\}$, (ii) $\cup_{i=1}^N\{u_{ij}|j=1,2,\ldots,p_i\}=\{u_1,u_2,\ldots,u_p\}$ and $\cup_{i=1}^N\{w_{ik}|k=1,2,\ldots,q_i\}=\{w_1,w_2,\ldots,w_q\}$, (iii) for any two different $i,i'\in\{1,2,\ldots,N\}$, either $\{u_{ij}|j=1,2,\ldots,p_i\}\cap\{u_{i'j}|j=1,2,\ldots,p_{i'}\}=\phi$ or $\{w_{ik}|k=1,2,\ldots,q_i\}\cap\{w_{i'k}|k=1,2,\ldots,q_{i'}\}=\phi$ or both, and (iv) for each $i\in\{1,2,\ldots,N\}$, either G_i consists of only entangled edges or only unentangled edges, but not both.

Thus we see that, for any perfect matching G, when the degree condition is satisfied, it is enough to study the separability of the density matrices of its pairwise disjoint entangled subgraphs (i.e., subgraphs each of whose edge is entangled), each of which is a perfect entangling matching on its own right (i.e., it is a perfect entangling matching on a set S of vertices taken from $V(G)$ such that all the elements of S can be labeled by two labels). See Fig. 2 for an illustration.

A speciality of the case $n=p2$ is also reflected in the following lemma.

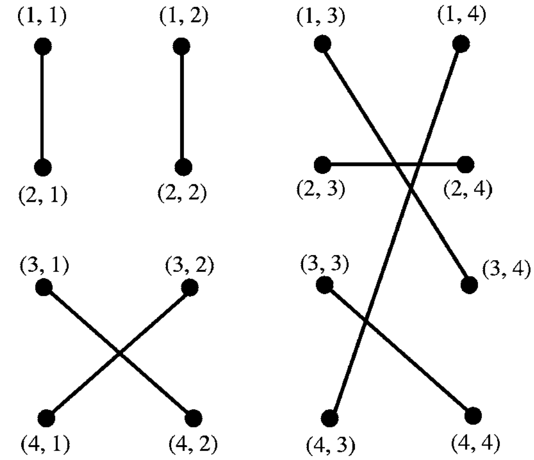

FIG. 2. A perfect matching G on 16 vertices (1,1),(1,2),…,(4,4), for which the degree condition is satisfied. G is the disjoint union of of the following four perfect matchings: (i) The unentangled graph: $G_1=(V(G_1),E(G_1))$ with $V(G_1)=\{(1,1),(1,2),(2,1),(2,2)\}$ and $E(G_1)=\{\{(1,1),(2,1)\},\{(1,2),(2,2)\}\}$. (ii) The crisscross: $G_2=(V(G_2),E(G_2))$ with $V(G_2)=\{(3,1),(3,2),(4,1),(4,2)\}$ and $E(G_2)=\{\{(3,1),(4,2)\},\{(3,2),(4,1)\}\}$. (iii) The perfect entangling matching: $G_3=(V(G_3),E(G_3))$ with $V(G_3)=\{(1,3),(1,4),(3,3),(3,4),(4,3),(4,4)\}$ and $E(G_3)=\{\{(1,3),(3,4)\},\{(1,4),(4,3)\},\{(3,3),(4,4)\}\}$. (iv) The unentangled graph: $G_4=(V(G_4),E(G_4))$ with $V(G_4)=\{(2,3),(2,4)\}$ and $E(G_4)=\{(2,3),(2,4)\}$.

Lemma 1. $\mathcal{P}_{2p}=\mathcal{P}^S_{2p}$.

Proof. By definition, $\mathcal{P}^S_{2p}\subseteqq\mathcal{P}_{2p}$. Let $G\in\mathcal{P}_{2p}$, where $V(G)=\{(k,1):k=1,2,\ldots,p\}\cup\{(k,2):k=1,2,\ldots,p\}$ and $E(G)=\{\{(k,1),(i_k,2)\}:k=1,2,\ldots,p\}$ where (i) for each $k\in\{1,2,\ldots,p\}$, i_k is a particular element in $\{1,2,\ldots,p\}\backslash\{k\}$ and (ii) $i_k\neq i_l$ whenever $k\neq l$. Thus we see that G^{Γ_B} is a graph on $2p$ vertices such that $V(G^{\Gamma_B})=V(G)$ and $E(G^{\Gamma_B})=\{\{(k,2),(i_k,1)\}:\{(k,1),(i_k,2)\}\in E(G)$ for all $k=1,2,\ldots,p\}$ with the properties that (i) for each $k\in\{1,2,\ldots,p\}$, i_k is a particular element in $\{1,2,\ldots,p\}\backslash\{k\}$, (ii) $i_k\neq i_l$ whenever $k\neq l$. So G^{Γ_B} must be a perfect entangling matching with vertex set as $V(G)$. Therefore, $\mathcal{P}_{2p}\subseteqq\mathcal{P}^S_{2p}$. □

The result in lemma 1 cannot, in general, be extended for the case of $\mathcal{P}_{p\cdot q}$ if $q>2$ (see, for example, Figs. 2 and 3 in [11]).

2. Properties of general perfect entangling matchings

If $\rho(H)$ is separable in $\mathbb{C}^p_A\otimes\mathbb{C}^q_B$, where H is the subgraph of a perfect entangling matching G on $p\cdot q$ vertices such that H consists of all the entangled edges in G, then $\rho(G)$ will be automatically separable in $\mathbb{C}^p_A\otimes\mathbb{C}^q_B$. So the relevant question is, what can we say about separability of $\rho(G)$ whenever $G\in\mathcal{P}^S_{p\cdot q}$, with $q>2$? Note that it is irrelevant to consider separability of $\rho(G)$ for an arbitrary $G\in\mathcal{P}_{p\cdot q}$, as $\rho(G)$ is inseparable if $G\in\mathcal{P}_{p\cdot q}\backslash\mathcal{P}^S_{p\cdot q}$ (because, in that case, the degree condition is not satisfied). As we have mentioned during the proof of theorem 4, we still do not have a canonical set of perfect entangling matchings on $n=p\cdot q$ vertices, to one (or a disjoint mixture of some) of which any element of $\mathcal{P}_{p\cdot q}$ can be transformed via local permutation(s) on one or both the labels the vertices. Moreover, even if we have that canonical set, we still do not have any proof of separability of the corresponding density matrices. But for a particular class of perfect entangling matchings G on $n=p(2r)$ vertices, for each of which the degree condition is satisfied, one can show that $\rho(G)$ is separable in $\mathbb{C}_A^p\otimes\mathbb{C}_B^{2r}$:

Let $G\in\mathcal{P}_{p(2r)}$, where $G=\uplus_{k=1}^r G_{j_kl_k}$, with $V(G_{j_kl_k})=\{(a,j_k):a=1,2,\ldots,p\}\cup\{(a,l_k):a=1,2,\ldots,p\}$ and $E(G_{j_kl_k})=\{\{(a,j_k),(i_a^{(k)},l_k)\}:a=1,2,\ldots,p\}$ such that for each $k\in\{1,2,\ldots,r\}$, (i) $i_a^{(k)}\in\{1,2,\ldots,p\}\backslash\{a\}$ for each $a\in\{1,2,\ldots,p\}$ and (ii) $j_k,l_k\in\{1,2,\ldots,2r\}$ with the properties that $j_k\neq l_k$, $j_k\neq j_{k'}$ (if $k\neq k'$), $l_k\neq l_{k'}$ (if $k\neq k'$). Thus we see that for each $k\in\{1,2,\ldots,r\}$, $G_{j_kl_k}$ is a perfect entangling matching on $2p$ vertices $(1,j_k)$, $(1,l_k)$, $(2,j_k)$, $(2,l_k),\ldots$, (p,j_k), (p,l_k) and with p edges $\{(1,j_k),(i_1^{(k)},l_k)\}$, $\{(2,j_k),(i_2^{(k)},l_k)\},\ldots,\{(p,j_k),(i_p^{(k)},l_k)\}$. So, by lemma 4.4 of [11], $G_{j_kl_k}$ can be transformed into a canonical perfect entangling matching on same set $V(G_{j_kl_k})$ of vertices. And so $\rho(G_{j_kl_k})$ is separable in $\mathbb{C}_A^p\otimes\mathbb{C}_B^2$ [and so, by theorem 2, $\Delta(G_{j_kl_k})=\Delta(G_{j_kl_k}^{\Gamma_B})$]. Therefore, $\rho(G)$ $[=\oplus_{k=1}^r\rho(G_{j_kl_k})]$ is separable in $\mathbb{C}_A^p\otimes\mathbb{C}_B^{(2r)}$ and $\Delta(G)=\oplus_{k=1}^r\Delta(G_{j_kl_k})=\oplus_{k=1}^r\Delta(G_{j_kl_k}^{\Gamma_B})=\Delta(G^{\Gamma_B})$.

The set of all elements in $\mathcal{P}_{p(2r)}^S$, each of which is a disjoint union of exactly r number of elements of $\mathcal{P}_{2p}$, is denoted here by $\mathcal{E}_{p(2r)}$. Let $G\in\mathcal{E}_{p(2r)}$. Then, as described above, G is a disjoint union of r elements $G_{j_1l_1}$, $G_{j_2l_2},\ldots$, $G_{j_rl_r}$ of $\mathcal{P}_{2p}^S$. Note that each element $G_{j_kl_k}$ of $\mathcal{P}_{2p}^S$ is a disjoint union of N_k number of elements $G_{1j_kl_k}(L_{1k})$ $(\in\mathcal{P}_{L_{1k}}^2)$, $G_{2j_kl_k}(L_{2k})$ $(\in\mathcal{P}_{L_{2k}}^2),\ldots$, $G_{N_kj_kl_k}(L_{N_kk})$ $(\in\mathcal{P}_{L_{N_kk}}^2)$ such that *no* further splitting of any $G(L_{ik})$ (as a disjoint union of perfect entangling matchings) is possible (see Fig. 3 for an illustration). For each $i\in\{1,2,\ldots,N_k\}$, we must have $V(G_{ij_kl_k}(L_{ik}))=\{(a_m^{(ik)},j_k):m=1,2,\ldots,L_{ik}\}\cup\{(a_m^{(ik)},l_k):m=1,2,\ldots,L_{ik}\}$, where $\{a_m^{(ik)}:m=1,2,\ldots,L_{ik}\}\cap\{a_m^{(i'k)}:m=1,2,\ldots,L_{i'k}\}=\varnothing$ if $i\neq i'$ and $\cup_{i=1}^{N_k}\{a_m^{(ik)}:m=1,2,\ldots,L_{ik}\}=\{1,2,\ldots,p\}$. Now by using lemma 4.4 of [11], we have

$$\rho(G_{i'j_kl_k}(L_{i'k}))=\frac{1}{L_{i'k}}\sum_{l=0}^{L_{i'k}-1}P\left[\frac{1}{\sqrt{L_{i'k}}}\sum_{m=1}^{L_{i'k}}\exp\left(\frac{2\pi i(m-1)l}{L_{i'k}}\right)\times U_{i'k}|a_m^{(i'k)}\rangle\right]\otimes P\left\{\frac{1}{\sqrt{2}}\left[|j_k\rangle-\exp\left(-\frac{2\pi il}{L_{i'k}}\right)\times|l_k\rangle\right]\right\},\tag{2.13}$$

where $U_{i'k}$ is the permutation matrix corresponding to a permutation on the labels $a_1^{(i'k)},a_2^{(i'k)},\ldots,a_{L_{i'k}}^{(i'k)}$ for $i'\in\{1,2,\ldots,N_k\}$ and $k=1,2,\ldots,r$. So we have

$$\rho(G_{j_kl_k})=\frac{1}{N_k}\sum_{i'=1}^{N_k}\rho(G_{i'j_kl_k}(L_{i'k}))$$

and, finally,

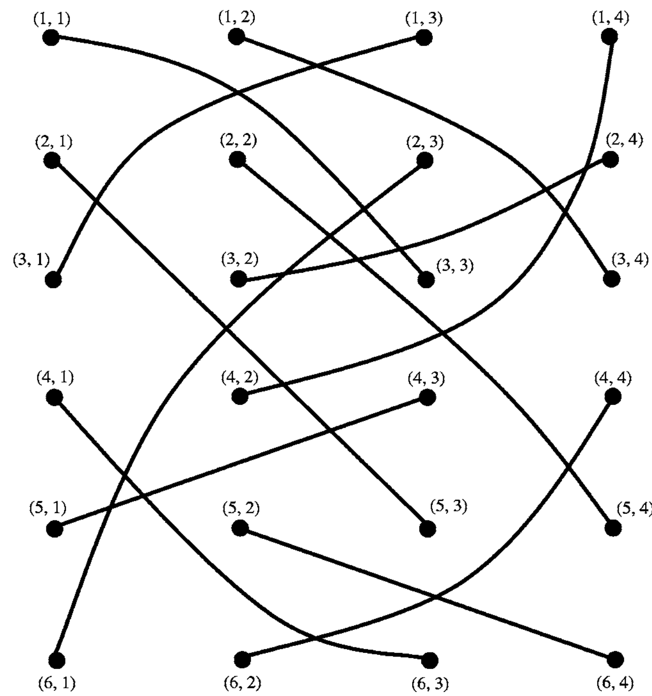

FIG. 3. A perfect entangling matching $G\in\mathcal{P}_{6.(2.2)}^S$ on the 24 vertices (1,1), (1,2), …, (6,4). G is a disjoint union of two perfect entangling matchings G_{13} and G_{24} in $\mathcal{P}_{6.2}$, where $V(G_{13})=\{(i,1)|i=1,2,\ldots,6\}\cup\{(i,3)|i=1,2,\ldots,6\}$ and $V(G_{24})=\{(i,2)|i=1,2,\ldots,6\}\cup\{(i,4)|i=1,2,\ldots,6\}$. Thus $G\in\mathcal{E}_{6.(2.2)}$. G_{13} itself is a disjoint union of the crisscross $G_{113}(2)$ [with $V(G_{113}(2))=\{(1,1),(3,1)\}\cup\{(1,3),(3,3)\}$ and $E(G(2))=\{\{(1,1),(3,3)\},\{(3,1),(1,3)\}\}$] and the perfect entangling matching $G_{213}(4)$ [with $V(G_{213}(4))=\{(2,1),(4,1),(5,1),(6,1)\}\cup\{(2,3),(4,3),(5,3),(6,3)\}$ and $E(G_{213}(4))=\{\{(2,1),(5,3)\},\{(4,1),(6,3)\},\{(5,1),(4,3)\},\{(6,1),(2,3)\}\}$]. $G_{213}(4)$ can be transformed (via the local permutation $4\leftrightarrow5$ on the first label) to a tally mark. And G_{24} is a perfect entangling matching on the vertices (1,2), (2,2), …, (6,2), (1,4), (2,4), …, (6,4) which can be transformed (via first applying the local permutation $2\leftrightarrow3$, $4\leftrightarrow5$ and then applying the local permutation $5\leftrightarrow6$, both on the first label) to a tally mark.

$$\rho(G)=\frac{1}{r}\sum_{k=1}^{r}\rho(G_{j_kl_k}).\tag{2.14}$$

Note that the range of $\rho(G)$ (where $G\in\mathcal{E}_{p(2r)}$) will always contain at least pr number of pairwise orthogonal product states: namely, the states

$$\frac{1}{\sqrt{L_{i'k}}}\sum_{m=1}^{L_{i'k}}\exp\left(\frac{2\pi i(m-1)l}{L_{i'k}}\right)U_{i'k}|a_m^{(i'k)}\rangle\otimes\frac{1}{\sqrt{2}}\left[|j_k\rangle-\exp\left(-\frac{2\pi il}{L_{i'k}}\right)|l_k\rangle\right],$$

where $\sum_{i'=1}^{N_k}L_{i'k}=p$ and $k=1,2,\ldots,r$. The range of $\rho(G)$ can also contain some other (possibly infinite in number) product states if either (i) $L_{ik}=L_{i'k}$ for different i, i' in $\{1,2,\ldots,N_k\}$ or (ii) $\{a_1^{(ik)},a_2^{(ik)},\ldots,a_{L_{ik}}^{(ik)}\}=\{a_1^{(ik')},a_2^{(ik')},\ldots,a_{L_{ik'}}^{(ik')}\}$ for different $k,k'\in\{1,2,\ldots,r\}$ (but for same i). All the above-mentioned pr number of pairwise orthogonal product states are reliably distinguishable by using local operations and classical communication (LOCC).

Is there any $\mathcal{P}^S_{p(2r)}$ such that $G \notin \mathcal{E}_{p(2r)}$? Yes, there are such perfect entangling matchings: for $p=3$, $r=2$, there is (up to local permutations on the labels of right-hand and/or left-hand sides) *one* such G which contains neither any crisscross nor tally mark (see Fig. 4). The higher the values of p and/or r, the higher will be the number of such different G's (not containing crisscrosses or tally marks). From now on, we shall only consider those perfect entangling matchings, none of which contains a crisscross or tally mark. Let $H \in \mathcal{P}^S_{p(2r)} \backslash \mathcal{E}_{p(2r)}$. Is $\rho(H)$ a separable state in $\mathbb{C}^p_A \otimes \mathbb{C}^{2r}_B$? In order to answer this question, we need to see whether there is any product state (of $\mathbb{C}^p_A \otimes \mathbb{C}^{2r}_B$) within the range ($\mathcal{R}_H$, say) of $\rho(H)$. Also we consider here the density matrix $\rho(H_+) = (1/pr)[I-\rho(H)]$, where I is the $2pr \times 2pr$ identity matrix. Let $\mathcal{R}_{H_+}$ be the range of $\rho(H_+)$. We have the following conjecture.

Conjecture 2. Let $H \in \mathcal{P}^S_{p(2r)} \backslash \mathcal{E}_{p(2r)}$ such that H neither contains any crisscross nor any tally mark. Then the range $\mathcal{R}_H$ of $\rho(H)$ [the range $\mathcal{R}_{H_+}$ of $\rho(H_+)$] contains exactly pr number of product states $|\psi_1\rangle \otimes |\phi_1\rangle$, $|\psi_2\rangle \otimes |\phi_2\rangle, \ldots, |\psi_{pr}\rangle \otimes |\phi_{pr}\rangle$ of $\mathbb{C}^p_A \otimes \mathbb{C}^{2r}_B$. Moreover, (i) all these product states are pairwise orthogonal, (ii) all the states $|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_{pr}\rangle$ are different but one can always have at least one class of exactly p of them all of which are pairwise orthogonal, (iii) all the states $|\phi_1\rangle, |\phi_2\rangle, \ldots, |\phi_{pr}\rangle$ are different but one can always have at least one class of exactly $2r$ of them all of which are pairwise orthogonal, and (iv) all the states $|\psi_1\rangle \otimes |\phi_1\rangle$, $|\psi_2\rangle \otimes |\phi_2\rangle, \ldots, |\psi_{pr}\rangle \otimes |\phi_{pr}\rangle$ are reliably distinguishable by LOCC.

The validity of conjecture 2 would directly show that for any $H \in \mathcal{P}^S_{p(2r)} \backslash \mathcal{E}_{p(2r)}$, which neither contains any crisscross nor any tally mark, $\rho(H) = (1/pr)\Sigma_{j=1}^{pr} P[|\psi_j\rangle \otimes |\phi_j\rangle]$, and hence, $\rho(H)$ is separable in $\mathbb{C}^p_A \otimes C^{2r}_B$. If an $H \in \mathcal{P}^S_{p(2r)} \backslash \mathcal{E}_{p(2r)}$ contains some crisscrosses and/or tally marks, the remaining part of H (eliminating out all these crisscrosses, tally marks) will be again an element of $\mathcal{P}^S_{p'(2r')} \backslash \mathcal{E}_{p'(2r')}$, for some $p' \leqslant p$ and $r' \leqslant r$, such that this new graph does not contain any crisscross or tally mark. As crisscrosses or tally marks always form separable density matrices, therefore we see that for any $H \in \mathcal{P}^S_{p(2r)}$, $\rho(H)$ is separable in $\mathbb{C}^p_A \otimes \mathbb{C}^{2r}_B$, provided the above-mentioned conjecture is true. Note that the validity of conjecture 1 automatically implies that for any $G \in \mathcal{P}_{p(2r)}$, $\rho(G)$ is separable if $G \in \mathcal{P}^S_{p(2r)} \backslash \mathcal{E}_{p(2r)}$. However, the statement in conjecture 2 is much stronger than just saying that $\rho(G)$ is separable if $G \in \mathcal{P}^S_{p(2r)} \backslash \mathcal{E}_{p(2r)}$.

D. Proof of theorem 5

Let ρ be a circulant density matrix of dimension $n = p \cdot q$. As we already mentioned in the Introduction, we can write $\rho = \Sigma_{g \in \mathbb{Z}_n} f(g)\sigma(g)$ where f is a complex-valued function. Obviously, there will be some constraints imposed by the fact that ρ is positive semidefinite and Hermitian. It is well known that ρ is diagonalized by the Fourier transform $\mathcal{F}(\mathbb{Z}_n)$ over $\mathbb{Z}_n$ [17]: $[\mathcal{F}(\mathbb{Z}_n)]_{j,k} = \exp(2\pi ijk/n)$. The eigenvectors of ρ are then the columns of $(\mathcal{F}(\mathbb{Z}_n))^\dagger$. We prove the theorem in two steps: (1) we prove that if $|\lambda\rangle$ is an eigenvector of ρ, then $|\lambda\rangle = |a\rangle \otimes |b\rangle$, where $|a\rangle \in \mathbb{C}^p_A$ and $|b\rangle \in \mathbb{C}^q_B$, for any p and q such that $n = pq$. (2) Then, for any chosen p and q, we prove that $\Delta(\rho) = \Delta(\rho^{\Gamma_B})$, where the partial transpose is taken with respect to the standard orthonormal basis $\{|ij\rangle : i = 1, \ldots, q; j = 1, \ldots, p\}$ of $\mathbb{C}^p_A \otimes \mathbb{C}^q_B$.

(1) Let A be an $n \times n$ matrix which is diagonalized by a unitary matrix U. We take $n = pq$. So $UAU^\dagger = D$, where $D = \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$, with respect to the standard orthonormal basis $\{|\psi_1\rangle, \ldots, |\psi_n\rangle\}$. Thus $A(U^\dagger|\psi_i\rangle) = \lambda_i(U^\dagger|\psi_i\rangle)$ for $i = 1, 2, \ldots, n$, and $UAU^\dagger = \Sigma_{i=1}^n \lambda_i |\psi_i\rangle\langle\psi_i|$. Thus $U^\dagger|\psi_i\rangle$ is an eigenvector of A corresponding to the eigenvalue λ_i. Also, $\langle\psi_i|UU^\dagger|\psi_j\rangle = \langle\psi_i|\psi_j\rangle = \delta_{ij}$. Let U be any $n \times n$ unitary matrix with its (j,k)th entry as u_{jk} with respect to the orthonormal basis $\{|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_n\rangle\}$. Then $U^\dagger = (\omega_{jk})_{j,k=1}^n$ where $\omega_{jk} = u^*_{kj}$ for all j,k. Now $U^\dagger|\psi_i\rangle = \Sigma_{j=1}^n \omega_{ji}|\psi_j\rangle = \Sigma_{j=1}^n u^*_{ij}|\psi_j\rangle$, which is the ith column of $U^\dagger$. Assuming that ρ is a circulant matrix, with respect to $\{|\psi_1\rangle, \ldots, |\psi_n\rangle\}$, we have

$$U = \frac{1}{\sqrt{n}} \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{n-1} \\ 1 & \omega^2 & \omega^4 & \cdots & \omega^{2(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{n-1} & \omega^{2(n-1)} & \cdots & \omega^{(n-1)(n-1)} \end{bmatrix}.$$

The unitary matrix U is the Fourier transform over $\mathbb{Z}_n$ [17]. We can see that

$$\begin{aligned} \rho &= \sum_{j=1}^n \lambda_j P[U^\dagger|\psi_j\rangle] \\ &= \sum_{j=1}^n \lambda_j P\left[\frac{1}{\sqrt{n}} \sum_{l=0}^{n-1} \exp\left(-\frac{2\pi i(j-1)l}{n}\right)|\psi_{l+1}\rangle\right] \\ &= \sum_{j=1}^n \lambda_j P\left[\frac{1}{\sqrt{n}} \sum_{a=0}^{p-1} \sum_{b=0}^{q-1} \exp\left(-\frac{2\pi i(j-1)(aq+b)}{n}\right)|a,b\rangle\right] \\ &= \sum_{j=1}^n \lambda_j P\left[\frac{1}{\sqrt{p}} \sum_{a=0}^{p-1} \exp\left(-\frac{2\pi i(j-1)a}{p}\right)|a\rangle \right. \\ &\quad \left. \otimes \frac{1}{\sqrt{q}} \sum_{b=0}^{q-1} \exp\left(-\frac{2\pi i(j-1)b}{pq}\right)|b\rangle\right]. \end{aligned}$$

It follows that ρ is a separable density matrix provided that $\lambda_j \geqslant 0$ for $j = 1, \ldots, n$.

(2) The general form a circulant density matrix is

$$\rho = \begin{bmatrix} a_1 & a_2 & \cdots & a_n \\ a_n & a_1 & \cdots & a_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_2 & a_3 & \cdots & a_1 \end{bmatrix}.$$

Since the matrix is symmetric, we have

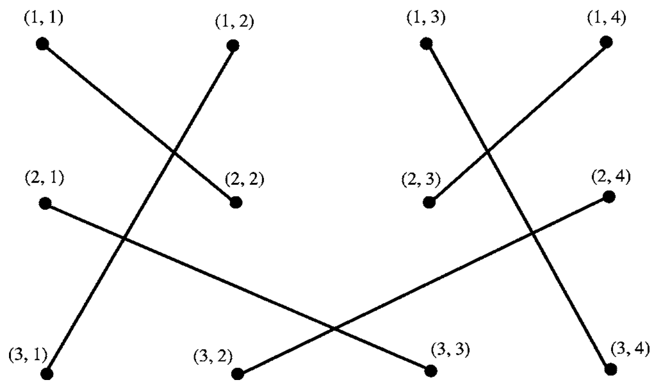

FIG. 4. G is the representative perfect entangling matching on 12 vertices (1,1), (1,2), … (3,4) such that $G \in \mathcal{P}^{S}_{3(2\times2)} \backslash \mathcal{E}_{3(2\times2)}$.

$$a_1 = a_1^*,\ a_2 = a_n^*,\ a_3 = a_{n-1}^*, \ldots,\ a_l = a_{n-l+2}^*. \quad (2.15)$$

Consider ρ as a block matrix with p^2 blocks, each block being a $q\times q$ matrix:

$$\rho = \begin{bmatrix} A_{1,1} & A_{1,2} & \cdots & A_{1,p} \\ A_{2,1} & A_{2,2} & \cdots & A_{2,p} \\ \vdots & \vdots & \ddots & \vdots \\ A_{p,1} & A_{p,2} & \cdots & A_{p,p} \end{bmatrix}.$$

Consider the block $A_{1,m+1}$. Then $[A_{1,m+1}]_{1,1}=a_{mq+1}$. Let $l=mq+1$. Then,

$$A_{1,m+1} = \begin{bmatrix} a_l & a_{l+1} & \cdots & a_{l+q-1} \\ a_{l-1} & a_l & \cdots & a_{l+q-2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{l-q+1} & & \cdots & \end{bmatrix}.$$

Now, consider the block $A_{1,p-m+1}$. Then $[A_{1,p-m+1}]_{1,1}=a_{n-l+2}=a_{n+1-mq}$. Then,

$$A_{1,n-m+1} = \begin{bmatrix} a_{n-l+2} & a_{n-l+3} & \cdots & a_{n-l+q+1} \\ a_{n-l+1} & a_{n-l+2} & \cdots & a_{n-l+q} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-l-q+3} & & \cdots & \end{bmatrix}$$

Applying the condition expressed in Eq. (2.15), one can verify that

$$A_{1,m+1} = A^{\dagger}_{1,n-m+1}.$$

This argument extends to all blocks of the ith block row of ρ. For example, the first block row of ρ is then of the form

$$A_{1,1}(=A^{\dagger}_{1,1})\ A_{1,2}\ A_{1,3}\ \cdots\ A_{1,p/2+1}\ A^{\dagger}_{1,p/2+1}\ \cdots\ A^{\dagger}_{1,3}\ A^{\dagger}_{1,2}$$

if p is even and

$$A_{1,1}(=A^{\dagger}_{1,1})\ A_{1,2}\ A_{1,3}\ \cdots\ A_{1,(p+1)/2}(=A^{\dagger}_{1,(p+1)/2})\ \cdots\ A^{\dagger}_{1,3}\ A^{\dagger}_{1,2}$$

if p is odd. It is then clear that $\Delta(\rho)=\Delta(\rho^{\Gamma_B})$; that is, the the row sums of ρ are invariant under the partial transpose. It should be noted here that each element of $\Delta(\rho)$ [as well as of $\Delta(\rho^{\Gamma_B})$] is real due to Eq. (2.15).

The same reasoning applies to the second part of the theorem. The only difference is that $\rho=\sum_{g\in\mathbb{Z}_2^n} f(g)\sigma(g)$ is diagonalized by the Hadamard matrices of Sylvester type, $H^n = H^{n-1}\otimes H$, where H is the 2×2 Hadamard matrix [16].

III. OPEN PROBLEMS

In this paper we have studied the separability of a class of states associated with the combinatorial Laplacians of graphs. The graphs for these states compactly encode information about their bipartite entanglement. We have shown that invariance of the degree matrices under partial transposition gives, in many cases, significant information about the separability of the states. Now the Peres-Horodecki partial transposition condition (known as the PPT *criterion*) is only a necessary condition (in general) for separability of any bipartite density matrices [7,8]. In fact, all the *practical* separability conditions, available so far, are either necessary or sufficient for general bipartite density matrices (see, for example, [10]). The degree condition, described in this paper, is of course weaker than the PPT criterion, as not all bipartite density matrices (not even the separable ones) can be described as density matrices generated from graphs. Nevertheless the validity of conjecture 1 (together with theorem 2) would imply that the degree condition is *both* necessary as well as sufficient for some particular classes of bipartite density matrices *irrespective* of the dimension of the system. In the quest for resolving the separability problem with the help of practical necessarily sufficient conditions (i.e., conditions, each of which is both necessary as well as sufficient), one possible way would be to find out the set of all possible independent but practical necessarily sufficient conditions each of which decides the separability problem of a *maximal* set of bipartite density matrices in such a way that the collection of these later sets would comprise the entire set of bipartite density matrices. The present work is one step forward in that direction. The following points are open for further investigation.

A. Partial transposition as a local permutation

It is not difficult to see that for any graph on $n=p\cdot q$ vertices $v_1=u_1w_1,\ldots,v_{pq}=u_pw_q$, if $\Delta(G)=\Delta(G^{\Gamma_B})$, then there is a permutation matrix P on the labels $w_1,\ldots,w_q$ such that

$$\Delta(G^{\Gamma_B}) = (I\otimes P)\Delta(G)(I\otimes P^{-1}),$$

$$M(G^{\Gamma_B}) = (I\otimes P)M(G)(I\otimes P^{-1}).$$

This says that if the degree condition is satisfied, then the operation of partial transposition is nothing but a local permutation. Note that this is, in general, false for the case of any given bipartite separable density matrix. The relation between separability of density matrices of graphs and isomorphism remains to be studied.

B. Structure of bipartite Hilbert spaces

The validity of of conjecture 6 can be traced back to basic problems in the structure of any bipartite Hilbert space.

Given a subspace $\mathcal{S}$ of dimension d of $\mathcal{H}$, what are the necessary and sufficient conditions under which at least one of the following situations hold good?

(i) $\mathcal{S}$ contains at least one linearly independent product state.

(ii) $\mathcal{S}$ contains only d' linearly independent product states, where $d' < d$.

(iii) $\mathcal{S}$ contains more than d product states (in which case they must be linearly dependent).

(iv) $\mathcal{S}$ contains contains exactly d linearly independent product states and these are pairwise orthogonal.

(v) $\mathcal{S}$ contains only d', where $d' \leqslant d$, pairwise orthogonal product states that one can extend to a full orthogonal product basis of $\mathcal{H}$, etc.

C. Multiparty entanglement

As a generalization of our result to density matrices of graphs having multiple labels on their vertices, we expect that if G is a graph on $n = p_1 p_2 \cdots p_m$ vertices,

$$v_i = u_{1u_1^{(1)}} u_{2s_i^{(2)}} \cdots u_{ms_i^{(m)}}, \quad \text{where } s_i^{(j)} \in \{1, \ldots, p_j\}$$
$$\text{for } j = 1, \ldots, m \text{ and } i = 1, \ldots, n,$$

then $\rho(G)$ is a separable density matrix in $\mathbb{C}^{p_1 p_2 \cdots p_{j-1} p_{j+1} \cdots p_m}_{A_1 \cdots A_{j-1} A_{j+1} \cdots A_m} \otimes \mathbb{C}^{p_j}_{A_j}$ if and only if $\Delta(G) = \Delta(G^{\Gamma_{A_j}})$. Moreover, we expect that $\rho(G)$ is a completely separable density matrix in $\mathbb{C}^{p_1}_{A_1} \otimes \mathbb{C}^{p_2}_{A_2} \otimes \cdots \otimes \mathbb{C}^{p_m}_{A_m}$ if and only if $\Delta(G) = \Delta(G^{\Gamma_{A_j}})$ for $j = 1, \ldots, m$ [18].

ACKNOWLEDGMENTS

S.G., S.S., and R.C.W. acknowledge the support received from the EPSRC. Part of of this work has been carried out while S.S. was at The Caesarea Rothschild Institute, Israel.

[1] A. Doherty, P. Parrilo, and F. Spedalieri, Phys. Rev. Lett. **88**, 187904 (2002).
[2] M. Grötschel, L. Lovász, and A. Schrijver, *Geometric Algorithms and Combinatorial Optimization* (Springer-Verlag, Berlin, 1988).
[3] P. Gritzmann and V. Klee, NATO ASI Ser., Ser. C **440**, 373 (1994).
[4] J. Eisert, P. Hyllus, O. Gühne, and M. Curty, Phys. Rev. A **70**, 062317 (2004).
[5] F. Hulpke and D. Bruß, e-print quant-ph/0407179.
[6] L. M. Ioannou, B. C. Travaglione, D. C. Cheung, and A. K. Ekert, e-print quant-ph/0403041.
[7] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A **223**, 1 (1996).
[8] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).
[9] S. L. Braunstein, C. M. Caves, R. Jozsa, N. Linden, S. Popescu, and R. Schack, Phys. Rev. Lett. **83**, 1054 (1999).
[10] D. Bruß, J. I. Cirac, P. Horodecki, F. Hulpke, B. Kraus, M. Lewenstein, and A. Sanpera, J. Mod. Opt. **49**, 1399 (2002).
[11] S. L. Braunstein, S. Ghosh, and S. Severini, Ann. Comb. (to be published), e-print quant-ph/0406165.
[12] C. Godsil and G. Royle, *Algebraic Graph Theory, Graduate Texts in Mathematics*, Vol. 207 (Springer-Verlag, New York, 2001).
[13] F. R. K. Chung, in *Spectral Graph Theory, Volume 92 of CBMS Regional Conference Series in Mathematics*, (American Mathematical Society, Providence, RI, 1997).
[14] H. J. Briegel and R. Raussendorf, Phys. Rev. Lett. **86**, 910 (2001).
[15] R. Simon, Phys. Rev. Lett. **84**, 2726 (2000).
[16] A. Terras, *Fourier Analysis on Finite Groups and Applications, London Mathematical Society Student Texts*, Vol. 43 (Cambridge University Press, Cambridge, England, 1999).
[17] P. J. Davis, *Circulant Matrices* (Wiley-Interscience, New York, 1979).
[18] L. Gurvits in, Proceedings of the 35th ACM Symposium on Theory of Computing, edited by ACM Press (New York, 2003).