



Fluctuation Moments Induced by Conjugation with Asymptotically Liberating Random Matrix Ensembles

Josue Vazquez-Becerra¹

Received: 25 August 2020 / Revised: 3 August 2022 / Accepted: 12 August 2022 /
Published online: 6 May 2023

© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2023

Abstract

Independent Haar-unitary random matrices and independent Haar-orthogonal random matrices are known to be asymptotically liberating ensembles, and they give rise to asymptotic free independence when used for conjugation of constant matrices. G. Anderson and B. Farrel showed that a certain family of discrete random unitary matrices can actually be used to the same end. In this paper, we investigate fluctuation moments and higher-order moments induced on constant matrices by conjugation with asymptotically liberating ensembles. We show for the first time that the fluctuation moments associated with second-order free independence can be obtained from conjugation with an ensemble consisting of signed permutation matrices and the discrete Fourier transform matrix. We also determine fluctuation moments induced by various related ensembles where we do not get known expressions but others related to traffic free independence.

Keywords Free probability · Random matrices · Fluctuation moments · Discrete Fourier transform matrix

Mathematics Subject Classification (2020) 46I54 · 60B20 · 15B52

1 Introduction

1.1 Background

Random matrices are matrix-valued random variables that were first investigated in mathematical statistics [29] and then in nuclear physics [28]. Over the years, its study

✉ Josue Vazquez-Becerra
13jdvb1@queensu.ca

¹ Department of Mathematics and Statistics, Queen's University, Jeffery Hall, Kingston, ON K7L 3N6, Canada

has evolved into a theory with applications to pure and applied sciences such as numerical analysis [6], analytic number theory [10], and wireless communications [24].

One of the main topics in random matrix theory is the study of limiting, or asymptotic, properties of random matrix ensembles. The term *random matrix ensemble* is used in the literature to refer to a sequence of random matrices $\{X_N\}_{N=1}^\infty$, or a sequence of families of random matrices $\{\{X_{N,i}\}_{i \in I}\}_{N=1}^\infty$, where the considered random matrices increase in size with respect to N . Their *limiting properties* are those arising from letting N go to infinity. Joint eigenvalue distributions, eigenvalues spacing, concentration inequalities, large deviation principles, maximal eigenvalues, and central limit theorems are some examples of limiting properties, for an introduction on these subjects one can consult [2].

Now, introduced by D. Voiculescu in his research on von Neumann algebras in [25], free probability theory has played a key role in the study of random matrices when multiple ensembles need to be considered. A main notion from free probability is that of *asymptotic free independence*.

Definition 1 Let I be a non-empty set. Suppose $\{X_{N,i}\}_{N=1}^\infty$ is a random matrix ensemble for each $i \in I$ where each $X_{N,i}$ is a N -by- N random matrix. We say that $\{X_{N,i}\}_{N=1}^\infty$ with $i \in I$ are **asymptotically freely independent** if the following two conditions hold:

(AF.1) for each index $i \in I$ and every integer $m \geq 1$ the limit

$$\lim_{N \rightarrow \infty} \mathbb{E} [\text{tr} (X_{N,i}^m)],$$

where $\text{tr} (\cdot)$ denotes the normalized trace $\frac{1}{N} \text{Tr} (\cdot)$, exists and

(AF.2) for all integers $m \geq 1$, all indexes $i_1, i_2, \dots, i_m \in I$ satisfying $i_1 \neq i_2, i_2 \neq i_3, \dots, i_{m-2} \neq i_{m-1}, i_{m-1} \neq i_m$, and $i_m \neq i_1$ and all polynomials p_1, p_2, \dots, p_m in the algebra $\mathbb{C}[x]$, we have

$$\lim_{N \rightarrow \infty} \mathbb{E} [\text{tr} (Y_{N,1} Y_{N,2} \cdots Y_{N,m})] = 0$$

where $Y_{N,k} = p_k (X_{N,i_k}) - \mathbb{E} [\text{tr} (p_k (X_{N,i_k}))] I_N$.

The first connection between free probability and random matrices was established by D. Voiculescu when he showed in [26] that independent Gaussian unitary ensembles converge to free semicircular random variables, a result which generalizes Wigner’s semicircular law and entails the asymptotic free independence of independent Gaussian unitary ensembles. The list of random matrix ensembles exhibiting asymptotic free independence has been extended since then, and it now includes: independent Wishart ensembles, independent Gaussian orthogonal ensembles, independent Haar-unitary distributed ensembles, independent Haar-orthogonal distributed ensembles, among others. The monograph [27] and the book [20] are standard introductions to free probability, and the recent monograph [18] is an excellent source presenting multiples directions in which the relation between free probability and random matrices has been extended.

Another result due to D. Voiculescu in [26], and subsequently generalized by other authors, states that conjugation by independent Haar-unitary distributed random matrices gives rise to asymptotic free independence. More concretely, assume $D_{N,i}$ is a self-adjoint N -by- N deterministic matrix for each index $i \in I$ and each integer $N \geq 1$ and suppose that

$$\sup_{N \in \mathbb{N}} \|D_{N,i}\| < \infty \quad \text{and} \quad \lim_{N \rightarrow \infty} \text{tr}(D_{N,i}^m) \text{ exists} \tag{1.1}$$

for all $i \in I$ and $m \geq 1$; the random matrix ensembles $\{D_{N,i}\}_{N=1}^\infty$ with $i \in I$ might or might not be asymptotically freely independent; however, if $\{U_{N,i}\}_{i \in I}$ is a family of independent N -by- N Haar-unitary distributed random matrices for each $N \geq 1$, then $\{U_{N,i} D_{N,i} U_{N,i}^*\}_{N=1}^\infty$ with $i \in I$ are asymptotically freely independent. The same conclusion holds if each $U_{N,i}$ is Haar-orthogonal distributed, see [13].

Aiming to enclose all of those unitary random matrix ensembles that give rise to asymptotic free independence when used for conjugation, B. Farrell and G. Anderson introduced in [1] the notion of *asymptotically liberating random matrix ensembles*.

Definition 2 Suppose $U_{N,i}$ is an N -by- N unitary random matrix for each index $i \in I$ and each integer $N \geq 1$. The unitary random matrix ensemble $\{\{U_{N,i}\}_{i \in I}\}_{N=1}^\infty$ is **asymptotically liberating** if for all indexes $i_1, i_2, \dots, i_m \in I$ with $i_1 \neq i_2, i_2 \neq i_3, \dots, i_{m-1} \neq i_m$, and $i_m \neq i_1$ there exists a constant $C > 0$ depending only on the indexes i_1, i_2, \dots, i_m such that

$$\begin{aligned} & \left| \mathbb{E} \left[\text{Tr} \left(U_{N,i_1} A_{N,1} U_{N,i_1}^* U_{N,i_2} A_{N,2} U_{N,i_2}^* \cdots U_{N,i_m} A_{N,m} U_{N,i_m}^* \right) \right] \right| \\ & \leq C \|A_{N,1}\| \|A_{N,2}\| \cdots \|A_{N,m}\| \end{aligned}$$

for all integers $N \geq 1$ and all matrices $A_{N,1}, A_{N,2}, \dots, A_{N,m} \in \text{Mat}_N(\mathbb{C})$ each of trace zero.

It follows immediately from the above definition that asymptotically liberating ensembles gives rise to asymptotic free independence when used for conjugation. Indeed, suppose $\{\{U_{N,i}\}_{i \in I}\}_{N=1}^\infty$ is an asymptotically liberating ensemble and assume $\{D_{N,i}\}_{N=1}^\infty$ with $i \in I$ satisfy (1.1). Letting $X_{N,i} = U_{N,i} D_{N,i} U_{N,i}^*$, we have (1.1) implies (AF.1) from Definition 1; moreover, if each $Y_{N,k}$ is as in (AF.2) from Definition 1, then

$$Y_{N,1} Y_{N,2} \cdots Y_{N,m} = (U_{N,i_1} A_{N,1} U_{N,i_1}^*) (U_{N,i_2} A_{N,2} U_{N,i_2}^*) \cdots (U_{N,i_m} A_{N,m} U_{N,i_m}^*)$$

where $A_{N,k}$ denotes the matrix of trace zero $p_k(D_{N,i_k}) - \text{tr}(p_k(D_{N,i_k}))I_N$, but (1.1) also implies that $\sup_N \|A_{N,k}\| < \infty$, and hence, (AF.2) holds. As it was intended, independent Haar-unitary random matrix ensembles and independent Haar-orthogonal random matrix ensembles are among those unitary random matrix ensembles shown to be asymptotically liberating, see Theorem 2.8 in [1] or Lemma 3.

A key feature of asymptotic free independence is that it provides us with universal rules to compute limiting mixed moments out of individual ones. A *limiting mixed moment* of the ensembles $\{X_{N,i}\}_{N=1}^\infty$ with $i \in I$ is a limit of the form

$$\lim_{N \rightarrow \infty} \mathbb{E} [\text{tr} (X_{N,i_1} X_{N,i_2} \cdots X_{N,i_m})] \tag{1.2}$$

where at least two of the indexes $i_1, i_2, \dots, i_m \in I$ are distinct and none of them depend on N . For instance, if $\{X_{N,i}\}_{N=1}^\infty$ with $i \in I$ are asymptotically free independent and $i_1, i_2 \in I$ are distinct, one can show that

$$\begin{aligned} \lim_{N \rightarrow \infty} \mathbb{E} \left[\text{tr} \left(X_{N,i_1}^1 X_{N,i_2}^4 X_{N,i_1}^7 X_{N,i_2}^2 \right) \right] &= \alpha_8^{(i_1)} \alpha_4^{(i_2)} \alpha_2^{(i_2)} + \alpha_6^{(i_2)} \alpha_1^{(i_1)} \alpha_7^{(i_1)} \\ &\quad - \alpha_1^{(i_1)} \alpha_4^{(i_2)} \alpha_7^{(i_1)} \alpha_2^{(i_2)} \end{aligned}$$

where $\alpha_m^{(i)}$ denotes $\lim_{N \rightarrow \infty} \mathbb{E}[\text{tr}(X_{N,i}^m)]$ and is called the *m-th limiting individual moment* of $\{X_{N,i}\}_{N=1}^\infty$. The relation above, and any other derived from asymptotic free independence to compute mixed moments, is called *universal* since it does not depend on any particular choice of i_1 and i_2 and it only requires $\{X_{N,i_1}\}_{N=1}^\infty$ and $\{X_{N,i_2}\}_{N=1}^\infty$ to be asymptotically freely independent.

At this point, one might wonder if there are universal rules for computing limiting mixed moments of higher order out of individual ones. A *limiting moment of n-th order* of the ensembles $\{X_{N,i}\}_{N=1}^\infty$ with $i \in I$ is defined to be a limit of the form

$$\lim_{N \rightarrow \infty} N^{n-2} c_n [\text{Tr}(\tilde{X}_{N,1}), \text{Tr}(\tilde{X}_{N,2}), \dots, \text{Tr}(\tilde{X}_{N,n})] \tag{1.3}$$

where $c_n[\cdot, \dots, \cdot]$ denotes the *n-th classical cumulant* and each $\tilde{X}_{N,k}$ is of the form

$$\tilde{X}_{N,k} = X_{N,i_1^{(k)}} X_{N,i_2^{(k)}} \cdots X_{N,i_{m_k}^{(k)}}$$

for some integer $m_k \geq 1$ and some indexes $i_1^{(k)}, i_2^{(k)}, \dots, i_{m_k}^{(k)} \in I$ not depending on N . The choice of the normalization factor N^{n-2} appearing in (1.3) is due to what has been observed for the behavior of (1.3) when each $X_{N,i}$ is a Gaussian unitary ensemble. Since the limiting moment (1.3) is just a generalization of (1.2), we call it *mixed* if at least two of the indexes $i_1^{(1)}, \dots, i_{m_1}^{(1)}, i_1^{(2)}, \dots, i_{m_2}^{(2)}, \dots, i_1^{(n)}, \dots, i_{m_n}^{(n)}$ are distinct, and *individual*, otherwise.

The most studied moments of higher order are moments of second order, also known as *fluctuation moments*. A fluctuation moment of the ensembles $\{X_{N,i}\}_{N=1}^\infty$ with $i \in I$ is then a limit of the form

$$\lim_{N \rightarrow \infty} \text{Cov}[\text{Tr}(X_{N,i_1} X_{N,i_2} \cdots X_{N,i_{m_1}}), \text{Tr}(X_{N,i_{m_1+1}} X_{N,i_{m_1+2}} \cdots X_{N,i_{m_1+m_2}})] \tag{1.4}$$

for some integers $m_1, m_2 \geq 1$ and indexes $i_1, i_2, \dots, i_{m_1}, i_{m_1+1}, i_{m_1+2}, \dots, i_{m_1+m_2} \in I$. A common practice in free probability theory to determine combinatorially (1.3), or (1.4), is that of calculating limiting moments of products of cyclically alternating and

centered random matrices, as in (AF.2) from Definition 1. For fluctuation moments, this means one must consider limits of the form

$$\lim_{N \rightarrow \infty} \text{Cov} [\text{Tr}(Y_{N,1}Y_{N,2} \cdots Y_{N,m_1}), \text{Tr}(Z_{N,1}Z_{N,2} \cdots Z_{N,m_2})]$$

where $Y_{N,k}$ and $Z_{N,l}$ are given by

$$\begin{aligned} Y_{N,k} &= p_k (X_{N,i_k}) - \mathbb{E} [\text{tr} (p_k (X_{N,i_k}))] I_N \quad \text{and} \\ Z_{N,l} &= q_l (X_{N,j_l}) - \mathbb{E} [\text{tr} (q_l (X_{N,j_l}))] I_N \end{aligned} \tag{1.5}$$

for all polynomials $p_1, p_2, \dots, p_{m_1}, q_1, q_2, \dots, q_{m_2} \in \mathbb{C}[x]$ and all indexes $i_1, i_2, \dots, i_{m_1}, j_1, j_2, \dots, j_{m_2} \in I$ satisfying the condition

$$i_1 \neq i_2, i_2 \neq i_3, \dots, i_{m_1-1} \neq i_{m_1}, i_{m_1} \neq i_1, j_1 \neq j_2, j_2 \neq j_3, \dots, j_{m_2-1} \neq j_{m_2}, j_{m_2} \neq j_1. \tag{1.6}$$

Analyzing the fluctuation moments of complex Gaussian and complex Wishart random matrix ensembles, J. Mingo and R. Speicher found a relation between individual and mixed moments of first and second order and introduced in [16] the notion of *asymptotic free independence of second order*.

Definition 3 We say that the random matrix ensembles $\{X_{N,i}\}_{N=1}^\infty$ with $i \in I$ are **asymptotically freely independent of second order** if they are asymptotically freely independent and the following three conditions are satisfied:

(ASOF.1) for each index $i \in I$ and all integers $m, n \geq 1$ the limit

$$\lim_{N \rightarrow \infty} \text{Cov} [\text{Tr}(X_{N,i}^m), \text{Tr}(X_{N,i}^n)]$$

exists,

(ASOF.2) for all integers $m_1, m_2 \geq 1$, all indexes $i_1, i_2, \dots, i_{m_1}, j_1, j_2, \dots, j_{m_2} \in I$ satisfying (1.6), and all polynomials $p_1, p_2, \dots, p_{m_1}, q_1, q_2, \dots, q_{m_2}$ in the algebra $\mathbb{C}[x]$, if we take

$$Y_N = Y_{N,1}Y_{N,2} \cdots Y_{N,m_1} \quad \text{and} \quad Z_N = Z_{N,1}Z_{N,2} \cdots Z_{N,m_2}$$

with $Y_{N,k}$ and $Z_{N,l}$ given by (1.5) for $1 \leq k \leq m_1$ and $1 \leq l \leq m_2$, we have

$$\lim_{N \rightarrow \infty} \text{Cov} [\text{Tr}(Y_N), \text{Tr}(Z_N)] = \delta_{m_1,m_2} \lim_{N \rightarrow \infty} \sum_{l=1}^{m_1} \prod_{k=1}^{m_2} \mathbb{E} [\text{tr} (Y_{N,k}Z_{N,l-k})] \tag{1.7}$$

where $l - k$ is taken modulo m_2 , and

(ASOF.3) for every integer $n \geq 3$, all polynomials p_1, p_2, \dots, p_n in the algebra of non-commutative polynomials $\mathbb{C}\langle x_i \mid i \in I \rangle$, letting $Y_{N,k} = p_k(\{X_{N,i}\}_{i \in I})$, we have

$$\lim_{N \rightarrow \infty} c_n [\text{Tr}(Y_{N,1}), \text{Tr}(Y_{N,2}), \dots, \text{Tr}(Y_{N,n})] = 0$$

Similar to asymptotic free independence, asymptotic free independence of second order provides us with universal rules, via the conditions (ASOF.1) and (ASOF.2) above, to calculate limiting mixed fluctuation moments out of individual ones. Moreover, independent Gaussian unitary ensembles are asymptotically freely independent of second order and conjugation by independent Haar-unitary random matrix ensembles leads to asymptotic free independence of second order, see [16] and [15], respectively.

However, in contrast to moments of first order, fluctuation moments induced by Haar-unitary random matrix ensembles and those induced by Haar-orthogonal random matrix ensembles differ. Investigating fluctuation moments of independent Gaussian orthogonal ensembles, E. Redelmeier proved in [21] that if each $\{X_{N,i}\}_{i \in I}$ forms a family of independent Gaussian orthogonal ensembles for every $N \geq 1$, then the ensembles $\{X_{N,i}\}_{N=1}^\infty$ with $i \in I$ satisfy (ASOF.1) and (ASOF.3) from Definition 3 but (ASOF.2) has to be replaced by the following:

(ASOF.2') for all integers $m_1, m_2 \geq 1$, all indexes $i_1, i_2, \dots, i_{m_1}, j_1, j_2, \dots, j_{m_2} \in I$ satisfying (1.6), and all polynomials $p_1, p_2, \dots, p_{m_1}, q_1, q_2, \dots, q_{m_2}$ in the algebra $\mathbb{C}[x]$, if we take

$$Y_N = Y_{N,1}Y_{N,2} \cdots Y_{N,m_1} \quad \text{and} \quad Z_N = Z_{N,1}Z_{N,2} \cdots Z_{N,m_2}$$

with $Y_{N,k}$ and $Z_{N,l}$ given by (1.5) for $1 \leq k \leq m_1$ and $1 \leq l \leq m_2$, we then have

$$\begin{aligned} \lim_{N \rightarrow \infty} \text{Cov} [\text{Tr}(Y_N), \text{Tr}(Z_N)] &= \delta_{m_1, m_2} \lim_{N \rightarrow \infty} \sum_{l=1}^{m_1} \left(\prod_{k=1}^{m_2} \mathbb{E}[\text{tr}(Y_{N,k}Z_{N,l-k})] \right. \\ &\quad \left. + \prod_{k=1}^{m_2} \mathbb{E}[\text{tr}(Y_{N,k}Z_{N,l+k}^T)] \right) \end{aligned} \tag{1.8}$$

where $l - k$ and $l + k$ are taken modulo m_2 .

Asymptotically freely independent ensembles satisfying (ASOF.1), (ASOF.2'), and (ASOF.3) are called *asymptotically freely independent of second order in the real sense*. Generalizing the findings of E. Redelmeier in [21], it was shown by J. Mingo and M. Popa in [13] that independent orthogonally invariant ensembles are asymptotically freely independent of second order in the real sense, and therefore, the fluctuation moments induced by Haar-orthogonal ensembles are not described by (1.7) but (1.8) instead.

1.2 Objectives and Main Results

The aim of this paper is to investigate the behavior of the fluctuation moments, and higher-order moments, resulting from conjugation by asymptotically liberating ensembles. Since independent Haar-unitary and independent Haar-orthogonal are both asymptotically liberating but the fluctuation moments each of them induces are distinct, we already know that the induced fluctuation moments depend on the specific liberating ensemble used for conjugation. However, it might well be the case that the relations in (1.7) and (1.8) cover all possible behaviors for fluctuation moments induced by liberating ensembles; our first result shows that this is actually not the case, adding even more evidence that fluctuation moments are more intricate than its first-order counterpart.

It is illustrative and good for comparison to restate what the relations in (1.7) and in (1.8) yield when Haar-unitary ensembles and Haar-orthogonal ensembles are used of conjugation. So, let us assume $X_{N,1} = U_{N,1} D_{N,1} U_{N,1}^*$ and $X_{N,2} = U_{N,2} D_{N,2} U_{N,2}^*$ for each integer $N \geq 1$ where each sequence $\{D_{N,i}\}_{N=1}^\infty$ satisfies (1.1) and $\{U_{N,1}, U_{N,2}\}_{N=1}^\infty$ is an asymptotically liberating ensemble. Note that if the random matrices Y_N and Z_N are as in (ASOF.2) from Definition 3, then we can write

$$Y_N = (U_{N,i_1} A_{N,1} U_{N,i_1}^*) (U_{N,i_2} A_{N,2} U_{N,i_2}^*) \cdots (U_{N,i_{2m_1}} A_{N,2m_1} U_{N,i_{2m_1}}^*) \tag{1.9}$$

and

$$Z_N = (U_{N,j_1} B_{N,1} U_{N,j_1}^*) (U_{N,j_2} B_{N,2} U_{N,j_2}^*) \cdots (U_{N,j_{2m_2}} B_{N,2m_2} U_{N,j_{2m_2}}^*) \tag{1.10}$$

where $A_{N,k}$ and $B_{N,l}$ are deterministic matrices of trace zero given by

$$A_{N,k} = p_k (D_{N,i_k}) - \text{tr} (p_k (D_{N,i_k})) I_N \quad \text{and} \quad B_{N,l} = q_l (D_{N,j_l}) - \text{tr} (q_l (D_{N,j_l})) I_N \tag{1.11}$$

for $1 \leq k \leq 2m_1$ and $1 \leq l \leq 2m_2$. For simplicity, and without loss of generality, let us assume $i_1 = j_1$. Now, if $U_{N,1}$ and $U_{N,2}$ are independent Haar-unitary ensembles, it follows from (AF.2) in Definition 1 and the relation in (1.7) that the covariance $\text{Cov} [\text{Tr}(Y_N), \text{Tr}(Z_N)]$ converges to

$$\lim_{N \rightarrow \infty} \delta_{m_1, m_2} \sum_{l=1}^{m_1} \prod_{k=1}^{2m_2} \text{tr} (A_{N,k} B_{N,2l-k}) \tag{1.12}$$

as N goes to infinity. On the other hand, if $U_{N,1}$ and $U_{N,2}$ are independent Haar-orthogonal ensembles, then (AF.2) and (1.8) imply that $\text{Cov} [\text{Tr}(Y_N), \text{Tr}(Z_N)]$ converges to

$$\lim_{N \rightarrow \infty} \delta_{m_1, m_2} \sum_{l=1}^{m_1} \left(\prod_{k=1}^{2m_2} \text{tr} (A_{N,k} B_{N,2l-k}) + \prod_{k=1}^{2m_2} \text{tr} (A_{N,k} B_{N,2l+k}^T) \right) \tag{1.13}$$

Table 1 The rules for $\text{Cov}[\text{Tr}(Y_N), \text{Tr}(Z_N)]$ with Y_N and Z_N as in (1.9) and (1.10), respectively, and $U_{N,1}$ and $U_{N,2}$ independent and uniformly distributed on the classical compact groups

| Conjugation type | Value of $\text{Cov}[\text{Tr}(Y_N), \text{Tr}(Z_N)]$ |
|---|--|
| $U_{N,1}$ and $U_{N,2}$ independent Haar-unitary | $\sum_{l=1}^m \prod_{k=1}^{2m} \text{tr}(A_{N,k} B_{N,2l-k})$ |
| $U_{N,1}$ and $U_{N,2}$ independent Haar-orthogonal | $\sum_{l=1}^m \prod_{k=1}^{2m} \text{tr}(A_{N,k} B_{N,2l-k}) + \sum_{l=1}^m \prod_{k=1}^{2m} \text{tr}(A_{N,k} B_{N,2l+k}^T)$ |
| $U_{N,1}$ and $U_{N,2}$ independent Haar-symplectic | $\frac{1}{4} \sum_{l=1}^m \prod_{k=1}^{2m} \text{tr}(A_{N,k} B_{N,2l-k}) + \frac{1}{4} \sum_{l=1}^{m-1} \prod_{k=1}^{2m} \text{tr}(A_{N,k} B_{N,2l+k}^T) - \frac{1}{2} \prod_{k=1}^{2m} \text{tr}(A_{N,k} B_{N,2m+k}^T)$ |

For simplicity, we only display the case $m_1 = m_2$

as N goes to infinity. Note that (1.1) alone guarantees the existence of each of the limits above if each matrix $D_{N,i}$ equals its transpose, regardless of what $U_{N,1}$ and $U_{N,2}$ are.

Another ensemble shown to be asymptotically liberating, see Corollary 3.2 in [1], and a main focus in this paper, is the unitary random matrix ensemble $\{W_N, H_N W_N / \sqrt{N}, X_N H_N W_N / \sqrt{N}\}$ where W_N is a random N -by- N signed permutation matrix, X_N is a random N -by- N signature matrix independent from W_N , and H_N is the N -by- N discrete Fourier transform matrix. Our first result shows that if we take pairs of distinct unitary matrices $U_{N,1}$ and $U_{N,2}$ from $\{W_N, H_N W_N / \sqrt{N}, X_N H_N W_N / \sqrt{N}\}$ and use them for conjugation, then the resulting fluctuation moments vary with each pair and differ from those in (1.12) and in (1.13).

Theorem 1 Let $D_{N,1}$ and $D_{N,2}$ be N -by- N self-adjoint matrices for each integer $N \geq 1$ so that each $\{D_{N,i}\}_{N=1}^\infty$ satisfies (1.1).

Suppose $X_{N,1} = U_{N,1} D_{N,2} U_{N,1}^*$ and $X_{N,2} = U_{N,2} D_{N,2} U_{N,2}^*$ where $U_{N,1}$ and $U_{N,2}$ are distinct matrices from $\{W_N, H_N W_N / \sqrt{N}, X_N H_N W_N / \sqrt{N}\}$.

If Y_N and Z_N are given by $Y_N = Y_{N,1} Y_{N,2} \cdots Y_{N,2m_1}$ and $Z_N = Z_{N,1} Z_{N,2} \cdots Z_{N,2m_2}$ where $Y_{N,k}$ and $Z_{N,l}$ are defined as in (1.5) for some polynomials $p_1, p_2, \dots, p_{2m_1}, q_1, q_2, \dots, q_{2m_2} \in \mathbb{C}[x]$ and some indexes $i_1, i_2, \dots, i_{2m_1}, j_1, j_2, \dots, j_{2m_2} \in \{1, 2\}$ satisfying (1.6) and $i_1 = j_1$, then the following holds:

(1) $U_{N,1} = W_N$ and $U_{N,2} = H_N W_N / \sqrt{N}$ implies

$$\begin{aligned} &\text{Cov}[\text{Tr}(Y_N), \text{Tr}(Z_N)] \\ &= \delta_{m_1, m_2} \sum_{l=1}^{m_1} \left(\prod_{k=1}^{2m_1} \text{tr}(A_{N,k} B_{N,2l-k}) + \prod_{k=1}^{2m_1} \text{tr}(A_{N,k} B_{N,2l+k-1}^T) \right) \\ &\quad + O\left(N^{-\frac{1}{2}}\right) \end{aligned}$$

(2) $U_{N,1} = W_N$ and $U_{N,2} = X_N H_N W_N / \sqrt{N}$ implies

$$\text{Cov}[\text{Tr}(Y_N), \text{Tr}(Z_N)]$$

$$\begin{aligned}
 &= \delta_{m_1, m_2} \sum_{l=1}^{m_1} \left(\prod_{k=1}^{2m_1} \text{tr} (A_{N, k} B_{N, 2l-k}) + \prod_{k=1}^{2m_1} \text{tr} (A_{N, k} \circ B_{N, 2l+k-1}) \right) \\
 &\quad + O \left(N^{-\frac{1}{2}} \right)
 \end{aligned}$$

(3) $U_{N,1} = H_N W_N / \sqrt{N}$ and $U_{N,2} = X_N H_N W_N / \sqrt{N}$ implies

$$\begin{aligned}
 \text{Cov} [\text{Tr}(Y_N), \text{Tr}(Z_N)] &= \sum_{l_1=1}^{2m_1} \sum_{l_2=1}^{2m_2} \prod_{k_1=1}^{m_1} \text{tr} (A_{N, l_1+k_1-1} A_{N, l_1-k_1}) \cdot \\
 &\quad \prod_{k_2=1}^{m_2} \text{tr} (B_{N, l_2+k_2-1} B_{N, l_2-k_2}) \\
 &\quad + \delta_{m_1, m_2} \sum_{l=1}^{2m_1} \left(\prod_{k=1}^{2m_1} \text{tr} (A_{N, k} B_{N, l-k}) \right) + O \left(N^{-\frac{1}{2}} \right)
 \end{aligned}$$

with $A_{N,k}$ and $B_{N,l}$ defined as in (1.11), $2l - k$, $2l + k - 1$, $l_1 + k_1 - 1$, $l_1 - k_1$, and $l - k$ interpreted modulo $2m_1$, and $l_2 + k_2 - 1$ and $l_2 + k_2$ interpreted modulo $2m_2$.

The discovery of second-order behaviors deviating from second-order free independence, and second-order free independence in the real sense, is not new. From a more algebraic setting, the authors of [8] and [9] analyze fluctuation moments of matrices with entries from a possibly non-commutative unital algebra and obtain different relations from those mentioned above. Additionally, the fluctuation moments of symplectically invariant random matrices have been fully determined in [22]. In particular, the relations (1.12) and (1.13) must be replaced by

$$\begin{aligned}
 \lim_{N \rightarrow \infty} \frac{\delta_{m_1, m_2}}{4} &\left(\sum_{l=1}^{m_1} \prod_{k=1}^{2m_2} \text{tr} (A_{N, k} B_{N, 2l-k}) + \sum_{l=1}^{m_1-1} \prod_{k=1}^{2m_2} \text{tr} (A_{N, k} B_{N, 2l+k}^T) \right. \\
 &\quad \left. - 2 \prod_{k=1}^{2m_2} \text{tr} (A_{N, k} B_{N, 2m_1+k}^T) \right)
 \end{aligned}$$

when considering conjugation by independent Haar-symplectic random matrix ensembles. We recap in Table 1 the fluctuation moments induced by conjugation with matrices uniformly distributed on classical compact groups and in Table 2 the fluctuation moments induced by conjugation with the matrices considered in this paper.

Notice (1.1) alone is not enough to guarantee the existence of limiting second-order behaviors in Theorem 1, in contrast to (1.12) and (1.13). For instance, if we want to take the limit as N goes to infinity in (3) from Theorem 1, we need $\{D_{N,1}\}_{N=1}^\infty$ and $\{D_{N,2}\}_{N=1}^\infty$ to have a joint limiting distribution, i.e., we need that the limit $\lim_{N \rightarrow \infty} \text{tr} (D_{N, i_1} D_{N, i_2} \cdots D_{N, i_m})$ exists for all integers $m \geq 1$ and all indexes $i_1, i_2, \dots, i_m \in \{1, 2\}$. This shows we cannot expect a classification for universal products of second order, in the spirit of [19] or [23], encompassing all of the second-order behaviors exhibited by random matrices.

Table 2 The rules for $\text{Cov}[\text{Tr}(Y_N), \text{Tr}(Z_N)]$ with Y_N and Z_N as in (1.9) and (1.10), respectively, when $U_{N,1}$ and $U_{N,2}$ are as in the left column

| Conjugation type | Value of $\text{Cov}[\text{Tr}(Y_N), \text{Tr}(Z_N)]$ |
|---|--|
| W_N and $\frac{H_N W_N}{\sqrt{N}}$ | $\sum_{l=1}^m \prod_{k=1}^{2m} \text{tr}(A_{N,k} B_{N,2l-k}) + \sum_{l=1}^m \prod_{k=1}^{2m} \text{tr}(A_{N,k} B_{N,2l+k-1}^T)$ |
| W_N and $\frac{X_N H_N W_N}{\sqrt{N}}$ | $\sum_{l=1}^m \prod_{k=1}^{2m} \text{tr}(A_{N,k} B_{N,2l-k}) + \sum_{l=1}^m \prod_{k=1}^{2m} \text{tr}(A_{N,k} \circ B_{N,2l+k-1})$ |
| $\frac{H_N W_N}{\sqrt{N}}$ and $\frac{X_N H_N W_N}{\sqrt{N}}$ | $\sum_{l=1}^{2m} \prod_{k=1}^{2m} \text{tr}(A_{N,k} B_{N,l-k}) + \sum_{l_1, l_2=1}^{2m} \prod_{k=1}^m \text{tr}(A_{N, l_1+k-1} A_{N, l_1-k}) \cdot \text{tr}(B_{N, l_2+k-1} B_{N, l_2-k})$ |
| $W_{N,1}$ and $\frac{H_N W_{N,2}}{\sqrt{N}}$ | $\sum_{l=1}^m \prod_{k=1}^{2m} \text{tr}(A_{N,k} B_{N,2l-k})$ |

The first three rules in this table are distinct from the rules in Table 1. We only display the case $m_1 = m_2$ for simplicity.

It would be desirable to have a master theorem encompassing all three cases in Theorem 1. However, in our analysis of fluctuation moments, we arrive to combinatorics that seem already too intricate when we consider each case separately. On this regard, although we make no explicit use of the theory of traffic free independence of C. Male, see [11], it is likely that our results will find a nice expression in terms of traffic algebras. Tools from traffic algebras have been already used in [12] to describe joint fluctuation moments of Wigner random matrices and deterministic matrices and their lack of second-order independence. Finally, it is pointed out in [7] that traffic algebras are closely related to \mathcal{A} -tracial algebras, with both notions generalizing classical and free independence. We hope to describe the results in this paper in terms of traffic or \mathcal{A} -tracial algebras in a future work.

Despite the fact that no pair of distinct unitary matrices $U_{N,1}$ and $U_{N,2}$ from the ensemble $\{W_N, H_N W_N/\sqrt{N}, X_N H_N W_N/\sqrt{N}\}_{N=1}^\infty$ leads to asymptotic free independence of second order when used for conjugation, it turns out not much more is needed to achieve this end, at least, partially. More concretely, if $U_{N,1} = W_{N,1}$ and $U_{N,2} = H_N W_{N,2}/\sqrt{N}$ where $W_{N,1}$ and $W_{N,2}$ are independent N -by- N uniformly distributed signed permutation matrices, then the fluctuation moments induced by $\{U_{N,1}, U_{N,2}\}_{N=1}^\infty$ are the same as if $U_{N,1}$ and $U_{N,2}$ were independent Haar-unitary, i.e., the induced fluctuation moments are described by (1.12). Thus, we can think of $\{W_{N,1}, H_N W_{N,2}/\sqrt{N}\}_{N=1}^\infty$ as an *asymptotically liberating ensemble of second order*.

Theorem 2 Let $D_{N,1}$ and $D_{N,2}$ be N -by- N self-adjoint matrices for each integer $N \geq 1$ so that each $\{D_{N,i}\}_{N=1}^\infty$ satisfies (1.1). Suppose $X_{N,1} = U_{N,1} D_{N,2} U_{N,1}^*$ and $X_{N,2} = U_{N,2} D_{N,2} U_{N,2}^*$ where $U_{N,1} = W_{N,1}$ and $U_{N,2} = H_N W_{N,2}/\sqrt{N}$. Then, $\{X_{N,1}\}_{N=1}^\infty$ and $\{X_{N,2}\}_{N=1}^\infty$ are asymptotically freely independent and they satisfy (ASOF.1) and (ASOF.2) from Definition 3. In particular, if $Y_N, Z_N, A_{N,k}$, and $B_{N,l}$ are given as in the previous theorem, then

$$\text{Cov}[\text{Tr}(Y_N), \text{Tr}(Z_N)] = \delta_{m_1, m_2} \sum_{l=1}^{m_1} \left(\prod_{k=1}^{2m_1} \text{tr}(A_{N,k} B_{N,2l-k}) \right) + O\left(N^{-\frac{1}{2}}\right) \quad (1.14)$$

The main result in [1] gives sufficient conditions on a unitary random matrix ensemble to be asymptotically liberating. Using a different approach than the one of [1], we have been able to prove that, under the same conditions, a unitary random matrix ensemble not only is asymptotically liberating but also satisfies a natural generalization of the boundedness condition in Definition 2 to cumulants of any order. More concretely, we have the following lemma.

Lemma 3 *Let $U_{N,i}$ be an N -by- N unitary random matrix for each index $i \in I$ and each integer $N \geq 1$.*

Suppose the unitary random matrix ensemble $\mathcal{U} = \{U_{N,i}\}_{i \in I}^{\infty}_{N=1}$ satisfies the following two conditions:

- (I) *the families of random matrices $\{U_{N,i_1}^* U_{N,i_2}\}_{i_1, i_2 \in I}$ and $\{W^* U_{N,i_1}^* U_{N,i_2} W\}_{i_1, i_2 \in I}$ are equal in distribution for every N -by- N signed permutation matrix W , and*
- (II) *for each positive integer m and indexes $i_1, i_2 \in I$ with $i_1 \neq i_2$ there is a constant $C_m(i_1, i_2)$ independent from N such that*

$$\left\| (U_{N,i_1}^* U_{N,i_2})(j_1, j_2) \right\|_m \leq C_m(i_1, i_2) N^{-1/2}$$

for all integers $j_1, j_2 \in \{1, 2, \dots, N\}$.

Now, given positive integers m_1, m_2, \dots, m_n , take $m'_k = m'_{k-1} + m_{k-1}$ for $k = 2, 3, \dots, n$ with $m'_1 = 0$ and consider the permutation $\gamma = (1, 2, \dots, m'_1 + m_1)(m'_2 + 1, m'_2 + 2, \dots, m'_2 + m_2) \cdots (m'_n + 1, \dots, m'_n + m_n)$. If some indexes $i_1, i_2, \dots, i_m \in I$ are such that $i_k \neq i_{\gamma(k)}$ for $k = 1, 2, \dots, m$ where $m = m_1 + m_2 + \dots + m_n$, then there exists a constant $C(i_1, i_2, \dots, i_m)$ such that for

$$Y_{N,k} = (U_{N,i_{m'_k+1}} A_{m'_k+1} U_{N,i_{m'_k+1}}^*) (U_{N,i_{m'_k+2}} A_{m'_k+2} U_{N,i_{m'_k+2}}^*) \cdots (U_{N,i_{m'_k+m_k}} A_{m'_k+m_k} U_{N,i_{m'_k+m_k}}^*)$$

with $A_1, A_2, \dots, A_m \in M_N(\mathbb{C})$ each of trace zero, we have

$$|c_n [\text{Tr}(Y_{N,1}), \text{Tr}(Y_{N,2}), \dots, \text{Tr}(Y_{N,n})]| \leq C(i_1, i_2, \dots, i_m) \|A_1\| \|A_2\| \cdots \|A_m\|$$

The fact that a unitary random matrix ensemble $\{U_{N,i}\}_{i \in I}^{\infty}_{N=1}$ satisfying (I) and (II) above is asymptotically liberating can now be seen as a particular case of the previous lemma. Moreover, if U_{N,i_1} and U_{N,i_2} are independent Haar-unitary (resp. Haar-orthogonal), then $U_{N,i_1}^* U_{N,i_2}$ is also Haar-unitary (resp. Haar-orthogonal), and hence, $U_{N,i_1}^* U_{N,i_2}$ satisfies (I) and (II) above. Therefore, independent Haar-unitary (Haar-orthogonal) random matrix ensembles are asymptotically liberating.

The customary definition of asymptotic free independence for random matrix ensembles involves the convergence of a sequence of linear functionals on non-commutative polynomials, see Proposition 14 and the comment right after its proof. In a similar way, multi-linear functionals on non-commutative polynomials can be used to analyze the behavior of moments of higher order, allowing us to show that unitary

random matrix ensembles satisfying (I) and (II) above induce the bounded cumulants property when used for conjugation.

Theorem 4 *Let $D_{N,i}$ be a self-adjoint N -by- N deterministic matrix, and let $U_{N,i}$ be an N -by- N unitary random matrix for each index $i \in I$ and each integer $N \geq 1$. Suppose the unitary random matrix ensemble $\{U_{N,i}\}_{i \in I}^{\infty}_{N=1}$ satisfies (I) and (II) from the previous lemma and (1.1) holds. Then, the ensemble $\{U_{N,i} D_{N,i} U_{N,i}^*\}_{i \in I}^{\infty}_{N=1}$ has the **bounded cumulants property**; namely, for all polynomials p_1, p_2, p_3, \dots in the algebra of non-commutative polynomials $\mathbb{C}\langle x_i \mid i \in I \rangle$ taking $Y_{N,k} = p_k(\{U_{N,i} D_{N,i} U_{N,i}^*\}_{i \in I})$ we have*

$$\sup_N \left| c_n [\text{Tr}(Y_{N,1}), \text{Tr}(Y_{N,2}), \dots, \text{Tr}(Y_{N,n})] \right| < \infty \tag{1.15}$$

for every integer $n \geq 1$.

The term *bounded cumulants property* is borrowed from [14] where it is used to prove several results concerning the limiting behavior of unitarily invariant random matrix ensembles and some other random matrix ensemble with this property.

A few technical comments are worth before we present the organization of the paper. Bounds of graph sums of square matrices, see [17] or Sect. 3, and the relations (4.4) and (5.3) are some key components to our results. In particular, (4.4) reveals the n -th cumulant from Lemma 3 can be written a sum where each term is a product of a cumulant $c_n[\pi]$ of the random variables $(U_{N,i_1}^* U_{N,i_2})(j_1, j_2)$ and a graph sum of the deterministic matrices A_l . Sharp bounds for graph sums are provided in Theorem 5, so the behavior and existence of higher-order moments depend largely on the cumulants $c_n[\pi]$, at least, in our approach. Estimates of $c_2[\pi]$ up to terms of order $N^{-m-1/2}$ are enough for Theorems 1 and 2 and constitute some of our main technical results, see Proposition 17. The sharpness of our estimates for $c_2[\pi]$ —and, consequently, of the terms of order $N^{-1/2}$ appearing in Theorems 1 and 2—is addressed in the last section. For higher-order moments with $n \geq 3$, a finer description of $c_n[\pi]$ than the one given here is required. A full description of $c_n[\pi]$ for the unitary matrices from Theorems 1 and 2 would mean to write graph sums of the discrete Fourier transform as a power series in $N^{1/2}$, such expression for arbitrary π and arbitrary N is unknown to us at the moment. For Haar-unitary and Haar-orthogonal ensembles, a full description of $c_n[\pi]$ as a power series in N^{-2} is already available via the Weingarten Calculus from [4] and [5], so higher-order moments might be computed using (4.4) in this case.

1.3 Organization of this Paper

The rest of this paper is organized as follows. In Sect. 2, we introduce the main definitions and the main notation for partitions, classical cumulants, matrices, and non-commutative polynomials; we also establish the distribution of random signed permutation matrices and random signature matrices. In Sect. 3, we review and prove multiple results on graph sums of square matrices. Roughly speaking, a graph sum of square matrices is a sum of products of entries of square matrices with the constraint

that some of the entries from distinct matrices are indexed by the same summation variable. Then, Sects. 4 and 5 are devoted to the proofs of our main results; concretely, Lemma 3 and Theorem 4 are proved in Sect. 4, whereas Theorems 1 and 2 are proved in Sect. 5. Finally, in Sect. 6, we give some concluding remarks including open questions and further research projects.

2 Preliminaries

2.1 Set Partitions, the Möbius Inversion Function, and Classical Cumulants

A *partition* of a non-empty set S is a set of non-empty and pair-wise disjoint subsets of S whose union is S , i.e., a set π is a partition of S if $B \subset S$ and $B \neq \emptyset$ for every $B \in \pi$, $B \cap B' \neq \emptyset$ implies $B = B'$ for all $B, B' \in \pi$, and $\cup_{B \in \pi} B = S$. The elements of a partition are called *blocks*, a block is said to be *even* if it has even cardinality, and similarly, a block is said to be *odd* if it has odd cardinality. A partition containing only even blocks is called *even*, but if all of its blocks have exactly two elements, we refer to it as a *pairing*. The total number of block in partition π is denoted by $\#(\pi)$ and we let $P(S)$, $P_{\text{even}}(S)$, and $P_2(S)$ denote the set of all partitions of S , the set of all even partitions of S , and the set of all pairing partitions of S , respectively.

Example The sets $\theta_1 = \{-1, -3, -2, 2, \{1, 3\}\}$, $\theta_2 = \{-1, -2, \{2\}, \{1, -3, 3\}\}$, and $\theta_3 = \{-1, -3, \{1, 3\}, \{-2, 2\}\}$ are all partitions of $\{-1, 1, 2, -2, -3, 3\}$. The partitions θ_1 and θ_3 are both even, but while θ_3 is a pairing, θ_1 is not. The partition θ_2 is neither even nor odd since it contains two odd blocks, $\{2\}$ and $\{1, -3, 3\}$, and one even block, $\{-1, 2\}$.

We let $[m]$ and $[\pm m]$ denote the sets of integers $\{1, 2, \dots, m\}$ and $\{-1, 1, -2, 2, \dots, -m, m\}$, respectively. The sets $[m]$ and $[\pm m]$ are used extensively in this paper, so we will omit the square brackets when referring to any of their sets of partitions. Thus, for instance, we write $P_{\text{even}}(\pm m)$ instead of $P_{\text{even}}([\pm m])$. Having fixed integers $m_1, m_2 \geq 1$ and a partition $\pi \in P(\pm(m_1 + m_2))$, we denote by π_1 and π_2 the restrictions of π to $[\pm m_1]$ and $[\pm(m_1 + m_2)] \setminus [\pm m_1]$, respectively.

Every partition $\pi \in P(S)$ defines an *equivalence relation*, denoted by \sim_π , that has the blocks of π as equivalence classes. Thus, given elements $k, l \in S$, we write $k \sim_\pi l$ only if k and l belong to the same block of π . With this notation in mind, a partition $\pi \in P(\pm m)$ is called *symmetric* if $k \sim_\pi l$ implies $-k \sim_\pi -l$.

The set of partitions $P(S)$ becomes a *partially ordered set* with the partial order \leq defined as follows: given partitions π and θ in $P(S)$, we write $\pi \leq \theta$, and say that π is a *refinement* of θ , if every block of π is contained in some block of θ . Note that $\pi \leq \theta$ if and only if $k \sim_\pi l$ implies $k \sim_\theta l$ for all $k, l \in S$. In the previous example, the partition π_3 is a refinement of π_1 , and there is no other refinement between π_1, π_2 , and π_3 .

Consider now the function $\zeta : P(S) \times P(S) \rightarrow \{1, 0\}$ defined by

$$\zeta(\theta, \eta) = \begin{cases} 1 & \text{if } \theta \leq \eta \\ 0 & \text{otherwise.} \end{cases}$$

This function is called the *zeta function* of $P(S)$. It turns out that if S is a finite set, then the system of equations

$$\sum_{\eta \leq \pi \leq \theta} \zeta(\eta, \pi) \mu(\pi, \theta) = \begin{cases} 1 & \text{if } \eta = \theta \\ 0 & \text{otherwise} \end{cases} \quad \text{for } \eta, \theta \in P(S) \tag{2.1}$$

determines a function $\mu : P(S) \times P(S) \rightarrow \mathbb{Z}$ called the *Möbius function* of $P(S)$ which can be explicitly computed, but first, let us establish the convention that whenever we write $\eta = \{B_{i_1}, B_{i_2}, \dots, B_{i_r}\}$ for a partition η , it is always assumed that blocks B_{i_k} and B_{i_l} are the same only if $i_k = i_l$. Suppose now we are given partitions π and θ in $P(S)$. If $\pi \leq \theta$, we can write $\theta = \{B_1, B_2, \dots, B_r\}$ and $\pi = \{B_{1,1}, B_{1,2}, \dots, B_{1,m_1}, \dots, B_{n,m_r}\}$ with $B_k = \cup_{l=1}^{m_k} B_{k,l}$ for each k , and, in this case, we have

$$\mu(\pi, \theta) = \prod_{k=1}^n (-1)^{m_k-1} (m_k - 1)! \tag{2.2}$$

On the other hand, if π is not a refinement of θ , we have $\mu(\pi, \theta) = 0$. The *Möbius inversion formula* states that given arbitrary functions $f, g : P(S) \rightarrow \mathbb{C}$, we have the relation

$$\forall \theta \in P(S) \quad f(\theta) = \sum_{\substack{\pi \in P(S) \\ \pi \geq \theta}} g(\pi) \iff \forall \pi \in P(S) \quad g(\pi) = \sum_{\substack{\theta \in P(S) \\ \theta \geq \pi}} \mu(\pi, \theta) f(\theta) \tag{2.3}$$

The computation of Möbius function, Eq. (2.2), and the Möbius inversion formula, Eq. (2.3), is well known, and their proofs can be found in [20, Lecture 10].

Let (Ω, \mathcal{F}, P) be a classical probability space, and let $L^{-\infty}(\Omega, \mathcal{F}, P)$ denote the set of complex-valued random variables on (Ω, \mathcal{F}, P) with finite moments of all orders. The classical n -th cumulant on $L^{-\infty}(\Omega, \mathcal{F}, P)$ is the n -linear functional $c_n : L^{-\infty}(\Omega, \mathcal{F}, P) \times \dots \times L^{-\infty}(\Omega, \mathcal{F}, P) \rightarrow \mathbb{C}$ defined by

$$c_n[x_1, x_2, x_3, \dots, x_n] = \sum_{\pi \in P(n)} \mu(\pi, 1_n) \prod_{B \in \pi} \mathbb{E} \left[\prod_{b \in B} x_b \right] \tag{2.4}$$

for random variables $x_1, x_2, x_3, \dots, x_n \in L^{-\infty}(\Omega, \mathcal{F}, P)$ and where $\mathbb{E}[\cdot]$ denotes the corresponding expected value. Note that if x_k is a constant for some $k \in [n]$ and $n \geq 2$, then $c_n[x_1, x_2, \dots, x_n] = 0$.

2.2 The Kernel Notation, Tuples, and Permutations

Let S_1 and S_2 be non-empty sets. We make the convention that for a function $\mathbf{j} : S_1 \rightarrow S_2$, we put $j_k = \mathbf{j}(k)$ for every $k \in S_1$; additionally, if $S_1 = [\pm m]$ for some integer $m \geq$

1, we identify the function $\mathbf{j} : S_1 \rightarrow S_2$ with the tuple $(j_{-1}, j_1, j_{-2}, \dots, j_{-m}, j_m)$. Moreover, the *kernel* of a function $\mathbf{j} : S_1 \rightarrow S_2$, denoted by $\ker(\mathbf{j})$, is defined as the partition of S_1 whose blocks are all of the non-empty pre-images of \mathbf{j} , i.e.,

$$\ker(\mathbf{j}) = \{\mathbf{j}^{-1}(s) \neq \emptyset \mid s \in S_2\} = \{\{k \in S_1 \mid j_k = s\} \neq \emptyset \mid s \in S_2\}.$$

The group of all permutations on a non-empty set S is denoted by $\text{Sym}(S)$; however, if $S = [m]$ or $S = [\pm m]$ for some positive integer m , we simply write $\text{Sym}(m)$ and $\text{Sym}(\pm m)$, respectively. Given permutations $\sigma_l \in \text{Sym}(S_l)$ for $l = 1, 2$, we let $\mathbf{j} \circ \sigma_1 : S_1 \rightarrow S_2$ and $\sigma_2 \circ \mathbf{j} : S_1 \rightarrow S_2$ denote the usual composition of functions, so we have

$$\mathbf{j} \circ \sigma_1(k) = j_{\sigma_1(k)} \quad \text{and} \quad \sigma_2 \circ \mathbf{j}(k) = \sigma_2(j_k) \quad \forall k \in S_1.$$

Example The function $\mathbf{j} : [\pm 3] \rightarrow [4]$ given by

$$\mathbf{j}(-1) = \mathbf{j}(2) = \mathbf{j}(3) = 4, \quad \mathbf{j}(1) = \mathbf{j}(-3) = 1, \quad \text{and} \quad \mathbf{j}(-2) = 3,$$

or, equivalently, $(j_{-1}, j_1, j_{-2}, j_2, j_{-3}, j_3) = (4, 1, 3, 4, 1, 4)$, has kernel

$$\ker(\mathbf{j}) = \{\{-1, 2, 3\}, \{1, -3\}, \{-2\}\}.$$

Additionally, if $\sigma_1 \in \text{Sym}(\pm 3)$ is given $\sigma_1(k) = -k$ for every $k \in [\pm 3]$ and $\sigma_2 \in \text{Sym}(4)$ is the cyclic permutation $(1, 2, 3, 4)$, then $\mathbf{j} \circ \sigma_1 = (1, 4, 4, 3, 4, 1)$ and $\sigma_2 \circ \mathbf{j} = (1, 2, 4, 1, 2, 1)$.

Given a permutation $\sigma \in \text{Sym}(S)$ and a partition $\pi \in P(S)$, we let $\sigma \circ \pi$ be the partition in $P(S)$ given by

$$\sigma \circ \pi = \{\sigma(B) \mid B \in \pi\} = \{\{\sigma(k) \mid k \in B\} \mid B \in \pi\}.$$

The map $\pi \mapsto \sigma \circ \pi$ is a poset automorphism; in particular, it is order-preserving, so for all partitions $\pi, \theta \in P(S)$ we get

$$\pi \leq \theta \iff \sigma \circ \pi \leq \sigma \circ \theta.$$

Remark Note that a partition $\pi \in P(S_1)$ and a function $\mathbf{j} : S_1 \rightarrow S_2$ satisfy $\pi \leq \ker(\mathbf{j})$ if and only if the function \mathbf{j} is constant when restricted to each of the blocks of π , i.e., $j_k = j_l$ whenever $k, l \in B$ for some block $B \in \pi$.

Moreover, for any permutations $\sigma_l \in \text{Sym}(S_l)$ with $l = 1, 2$, we have that $\ker(\mathbf{j} \circ \sigma_1) = \sigma_1^{-1} \circ \ker(\mathbf{j})$ and $\ker(\mathbf{j}) = \ker(\sigma_2 \circ \mathbf{j})$.

2.3 Some Random Matrices and the Joint Distribution of their Entries

Let I be a non-empty set. Suppose $\{X_i\}_{i \in I}$ and $\{Y_i\}_{i \in I}$ are two families of N -by- N random matrices defined on the same probability space. We say that $\{X_i\}_{i \in I}$ and

$\{Y_i\}_{i \in I}$ are equal in distribution if we have

$$\mathbb{E} \left[\prod_{k=1}^m X_{i_k}(j_{-k}, j_k) \right] = \mathbb{E} \left[\prod_{k=1}^m Y_{i_k}(j_{-k}, j_k) \right]$$

for all integers $m \geq 1$, indexes $i_1, i_2, \dots, i_m \in I$, and functions $\mathbf{j} : [\pm m] \rightarrow [N]$.

A matrix $X \in \text{Mat}_N(\mathbb{C})$ is a *signature matrix* if there exist signs $\epsilon_1, \dots, \epsilon_N \in \{-1, 1\}$ such that

$$X(i, j) = \begin{cases} \epsilon_i & \text{if } i = j \\ 0 & \text{otherwise.} \end{cases}$$

An N -by- N random matrix X is a *uniformly distributed signature matrix* if it is uniformly distributed on the set of N -by- N signature matrices; in this case, for all functions $\mathbf{i}, \mathbf{j} : S \rightarrow [N]$ we have

$$\mathbb{E} \left[\prod_{k \in S} X(i_k, j_k) \right] = \begin{cases} 1, & \text{if } \mathbf{i} = \mathbf{j} \text{ and } \ker(\mathbf{i}) \text{ is an even partition} \\ 0, & \text{otherwise} \end{cases} \tag{2.5}$$

A matrix $W \in \text{Mat}_N(\mathbb{C})$ is a *signed permutation matrix* if there exist signs $\epsilon_1, \dots, \epsilon_N \in \{-1, 1\}$ and a permutation $\sigma \in \text{Sym}(N)$ such that

$$W(i, j) = \epsilon_i \delta_{i, \sigma(j)} = \begin{cases} \epsilon_i & \text{if } i = \sigma(j) \\ 0 & \text{otherwise} \end{cases}.$$

An N -by- N random matrix W is a *uniformly distributed signed permutation matrix* if it is uniformly distributed on the set of N -by- N signed permutation matrices; if that is the case, for all functions $\mathbf{i}, \mathbf{j} : S \rightarrow [N]$ we get

$$\mathbb{E} \left[\prod_{s \in S} W(i_s, j_s) \right] = \begin{cases} \frac{(N - \#(\pi))!}{N!}, & \text{if } \pi = \ker(\mathbf{i}) = \ker(\mathbf{j}) \in P_{\text{even}}(S) \\ 0, & \text{otherwise} \end{cases} \tag{2.6}$$

Remark Suppose $\{V_i\}_{i \in I}$ is a family of N -by- N random matrices distribution-invariant under conjugation by signed permutation matrices, i.e., the families $\{V_i\}_{i \in I}$ and $\{W^* V_i W\}_{i \in I}$ are equal in distribution for every signed permutation matrix W . Then, for all integers $m \geq 1$, indexes $i_1, i_2, \dots, i_m \in I$, and functions $\mathbf{j} : [\pm m] \rightarrow [N]$, we have

$$\mathbb{E} \left[\prod_{k=1}^m V_{i_k}(j_{-k}, j_k) \right] = \prod_{k=1}^m \epsilon_{\sigma(j_{-k})} \epsilon_{\sigma(j_k)} \mathbb{E} \left[\prod_{k=1}^m V_{i_k}(\sigma(j_{-k}), \sigma(j_k)) \right] \tag{2.7}$$

for all signs $\epsilon_1, \dots, \epsilon_N \in \{-1, 1\}$ and permutations $\sigma \in \text{Sym}(N)$.

2.4 Non-commutative Polynomials and their Evaluation on Families of Random Matrices

Let I be a non-empty set. We denote by $\mathbb{C}\langle x_i \mid i \in I \rangle$ the algebra of non-commutative polynomials on the family of variables $\{x_i \mid i \in I\}$. Let us recall that $\mathbb{C}\langle x_i \mid i \in I \rangle$ is the algebra over \mathbb{C} with a basis consisting of all the words in the alphabet $\{x_i \mid i \in I\}$, including the empty word which acts as multiplicative identity, and the product of two basis elements is given by concatenation. Thus, a basis element is a word of the form

$$x_{i_1}x_{i_2} \cdots x_{i_r}$$

for some integer $r \geq 0$ and some indexes $i_1, i_2, \dots, i_r \in I$, and if $x_{j_1}x_{j_2} \cdots x_{j_r}$ is another basis element, we have

$$(x_{i_1}x_{i_2} \cdots x_{i_r})(x_{j_1}x_{j_2} \cdots x_{j_s}) = x_{i_1}x_{i_2} \cdots x_{i_r}x_{j_1}x_{j_2} \cdots x_{j_s}.$$

Given polynomials p_1, p_2, \dots, p_m in the algebra $\mathbb{C}\langle x_i \mid i \in I \rangle$ and a set $S = \{k_1 < k_2 < \dots < k_n\} \subset [m]$, we let

$$\prod_{k \in S} p_k := p_{k_1}p_{k_2} \cdots p_{k_n}. \tag{2.8}$$

Suppose we are given random matrix ensembles $\{X_{N,i}\}_{N=1}^\infty$ with $i \in I$ where each $X_{N,i}$ is a N -by- N random matrix. For each non-commutative polynomial $p \in \mathbb{C}\langle x_i \mid i \in I \rangle$, we denote by

$$p(\{X_{N,i}\}_{i \in I})$$

the random matrix obtained from replacing each x_i appearing in the polynomial p with the random matrix $X_{N,i}$ for every $i \in I$ and the constant term of p , say α , with the scalar multiple of the identity matrix αI_N . For instance, if $p(x_1, x_2) = x_1x_2 - x_2^2 + 4$, then

$$p(\{X_{N,i}\}_{i \in \{1,2\}}) = X_{N,1}X_{N,2} - X_{N,2}^2 + 4I_N.$$

3 Graph Sums of Square Matrices

In this section, we review and prove some useful results on graph sums of square matrices. A *graph sum* of given matrices $A_1, A_2, \dots, A_m \in \text{Mat}_N(\mathbb{C})$ is a sum of the form

$$\sum_{\substack{j: [\pm m] \rightarrow [N] \\ \ker(j) \geq \pi}} A_1(j_{-1}, j_1)A_2(j_{-2}, j_2) \cdots A_m(j_{-m}, j_m) = \sum_{\substack{j: [\pm m] \rightarrow [N] \\ \ker(j) \geq \pi}} \prod_{k=1}^m A_k(j_{-k}, j_k) \tag{3.1}$$

for some partition $\pi \in P(\pm m)$. Note that the condition $\ker(\mathbf{j}) \geq \pi$ in the sum above is simply a restatement of a set of equalities between the indexes $j_{\pm k}$. For example, if we let $\pi = \{\{1, -2\}, \{2, -3\}, \dots, \{m-1, -m\}, \{m, -1\}\}$, then $\ker(\mathbf{j}) \geq \pi$ only if $j_1 = j_{-2}, j_2 = j_{-3}, \dots, j_{m-1} = j_{-m}$, and $j_m = j_{-1}$, and thus, we get

$$\sum_{\substack{\mathbf{j}: [\pm m] \rightarrow [N] \\ \ker(\mathbf{j}) \geq \pi}} \prod_{k=1}^m A_k(j_{-k}, j_k) = \text{Tr}(A_1 A_2 \cdots A_m).$$

It is worth mentioning that although the labeling of the entries of A_k in (3.1) is not customary, it has proven to be suitable for many of our calculations; moreover, for a bijection $\sigma : [\pm m] \rightarrow S$, the relation

$$\sum_{\substack{\mathbf{j}: S \rightarrow [N] \\ \ker(\mathbf{j}) \geq \hat{\pi}}} \prod_{k=1}^m A_k(j_{\sigma(-k)}, j_{\sigma(k)}) = \sum_{\substack{\mathbf{j}: [\pm m] \rightarrow [N] \\ \ker(\mathbf{j}) \geq \sigma^{-1} \circ \hat{\pi}}} \prod_{k=1}^m A_k(j_{-k}, j_k) \quad \forall \hat{\pi} \in P(S) \quad (3.2)$$

provides the link between the labeling of the entries of A_k in (3.1) and any other labeling. For instance, if $\sigma : [\pm m] \rightarrow [2m]$ is given by $\sigma(-k) = 2k - 1$ and $\sigma(k) = 2k$ for $1 \leq k \leq m$, then

$$\sum_{\substack{\mathbf{j}: [2m] \rightarrow [N] \\ \ker(\mathbf{j}) \geq \hat{\pi}}} \prod_{k=1}^m A_k(j_{2k-1}, j_{2k}) = \text{Tr}(A_1) \text{Tr}(A_2) \cdots \text{Tr}(A_m) = \sum_{\substack{\mathbf{j}: [\pm m] \rightarrow [N] \\ \ker(\mathbf{j}) \geq \pi}} \prod_{k=1}^m A_k(j_{-k}, j_k)$$

where $\hat{\pi} = \{\{1, 2\}, \{3, 4\}, \dots, \{2m-1, 2m\}\}$ and $\pi = \sigma^{-1} \circ \hat{\pi} = \{\{-1, 1\}, \{-2, 2\}, \dots, \{-m, m\}\}$. The type of sums above are named graph sums because they can be associated with certain graphs that, as we will see next, help us analyze the corresponding sums.

3.1 Bounds of Graph Sums of General Square Matrices

The main result in [17] concerns more general graph sums, allowing the matrices A_k in (3.1) to be rectangular and not necessarily square. For graph sums of square matrices, however, the result takes the following form.

Theorem 5 *Suppose π is a partition in $P(\pm m)$. Then, there exists a rational number $\tau_\pi \in \{1, \frac{3}{2}, 2, \dots\}$ depending only on the partition π such that for every integer $N \geq 1$ the following two conditions hold:*

(a) *for all matrices $A_1, A_2, \dots, A_m \in \text{Mat}_N(\mathbb{C})$, we have*

$$\left| \sum_{\substack{\mathbf{j}: [\pm m] \rightarrow [N] \\ \ker(\mathbf{j}) \geq \pi}} \prod_{k=1}^m A_k(j_{-k}, j_k) \right| \leq N^{\tau_\pi} \prod_{k=1}^m \|A_k\|$$

(b) there are some nonzero matrices $B_1, B_2, \dots, B_m \in \text{Mat}_N(\mathbb{C})$ satisfying

$$\left| \sum_{\substack{j: [\pm m] \rightarrow [N] \\ \ker(j) \geq \pi}} \prod_{k=1}^m B_k(j_{-k}, j_k) \right| = N^{\tau_\pi} \prod_{k=1}^m \|B_k\|$$

Note that τ_π is uniquely determined by (a) and (b). We call τ_π the **graph sum exponent** of π .

It is also shown in [17] that the graph sum exponent τ_π can be algorithmically computed analyzing the two-edge connectedness of a graph associated with π . For the reader’s convenience, we recount such algorithm next.

- Step 1. Given a partition $\pi \in P(\pm m)$, consider the undirected graph \mathcal{G}_π resulting from, first, taking edges E_1, E_2, \dots, E_m with endpoints $-1, +1, -2, +2, \dots, -m, +m$, respectively, and, then, identifying endpoints when they belong to the same block of π .
- Step 2. Identify the cutting edges and the two-edge connected components of \mathcal{G}_π . Recall that a *cutting edge* of a graph, also known as a *bridge*, is an edge whose removal increases the number of connected components. Moreover, a graph is *two-edge connected* if it is connected and has no cutting edges, and, consequently, a *two-edge connected component* of a graph is a subgraph that is maximal, under the usual graph inclusion, in the set of all two-edge connected subgraphs
- Step 3. Letting \mathcal{F}_π denote the graph with vertex set given by the set of all two-edge connected components of \mathcal{G}_π and edge set given by the set of all cutting edges of \mathcal{G}_π , the graph sum exponent τ_π is given by

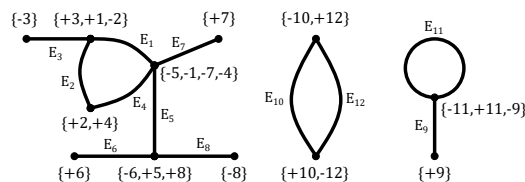
$$\tau_\pi = \sum_{v \text{ vertex in } \mathcal{F}_\pi} l(v) \quad \text{where} \quad l(v) := \begin{cases} \frac{1}{2} & \text{if } \deg(v) = 1, \\ 1 & \text{if } \deg(v) = 0, \\ 0 & \text{otherwise.} \end{cases} \quad (3.3)$$

and $\deg(v)$ denotes the degree of the vertex v in the graph \mathcal{F}_π .

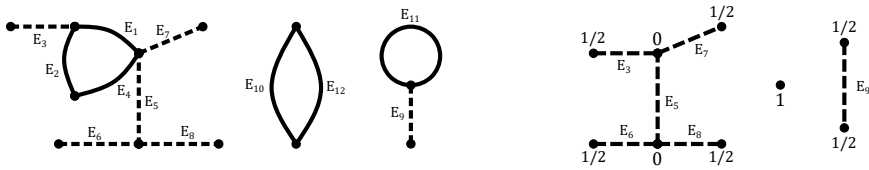
Example The undirected graph \mathcal{G}_π associated with the partition

$$\pi = \left\{ \begin{array}{l} \{-3\}, \{+3, +1, -2\}, \{-5, -1, -7, -4\}, \{+7\}, \{+2, +4\}, \{+6\}, \\ \{-6, +5, +8\}, \{-8\}, \{-10, +12\}, \{+10, -12\}, \{-11, +11, -9\}, \{+9\} \end{array} \right\} \\ \in P(\pm 12)$$

can be represented as



Hence, the cutting edges of \mathcal{G}_π are $E_3, E_5, E_6, E_7, E_8,$ and E_9 ; moreover, the two-edge connected components of \mathcal{G}_π are exactly what remains of \mathcal{G}_π after removing all of its cutting edges. The graph \mathcal{F}_π can be obtained from \mathcal{G}_π by shrinking each of the two-edge connected components of \mathcal{G}_π to a vertex, and thus, if we represent the cutting edges of \mathcal{G}_π with dashed lines, we obtain



where \mathcal{F}_π is the graph on the right and next to each of its vertices we have placed the corresponding contribution $l(v)$ to the graph sum exponent τ_π . Therefore, we have $\tau_\pi = 4$.

Having described the algorithm to compute τ_π , we can now show that graph sum exponents of even partitions can be easily calculated.

Proposition 6 *If $\pi \in P(\pm m)$ is an even partition, then the graph sum exponent τ_π equals the number of connected components of \mathcal{G}_π .*

Proof By Equation (3.3), it suffices to show that the graph \mathcal{G}_π has no cutting edges. Suppose \mathcal{G}_π has a cutting edge. If we remove such cutting edge, we get two disjoint graphs, each of which has one single vertex of odd degree and the other vertices of even degree. But, this contradicts the handshaking lemma that in any graph the sum of degrees over all its vertices must be even. Thus, \mathcal{G}_π has no cutting edges, and hence, all its connected components are two-edge connected. \square

Now, resulting from endowing each edge E_k in the graph \mathcal{G}_π with the direction that goes from $+k$ to $-k$, the directed graph $\vec{\mathcal{G}}_\pi$ can sometimes be used to describe the corresponding graph sum. In particular, a graph sum factors as a product of traces of matrices when all connected components of \mathcal{G}_π are bouquets, to which we refer as multiple loops, or cycles, each connected component gives rise to a trace. For example, for the partition

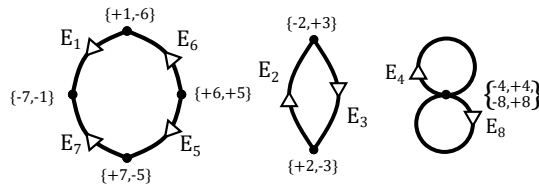
$$\pi = \{\{1, -6\}, \{6, 5\}, \{-5, 7\}, \{-7, -1\}, \{-2, 3\}, \{-3, 2\}, \{-4, 4\}\}$$

and given matrices $A_1, A_2, \dots, A_7 \in \text{Mat}_N(\mathbb{C})$, we have the graph sum

$$\sum_{\substack{\mathbf{j}: \{\pm 7\} \rightarrow [N] \\ \ker(\mathbf{j}) \geq \pi}} \prod_{k=1}^7 A_k(j_{-k}, j_k) = \text{Tr} \left(A_1 A_6 A_5^T A_7^T \right) \text{Tr} (A_2 A_3) \text{Tr} (A_4 \circ A_8) \quad (3.4)$$

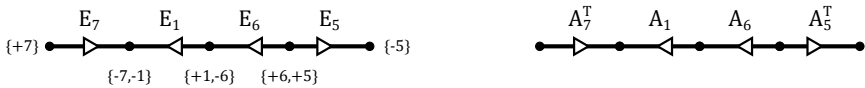
where the right-hand side can be deduced from analyzing the directed graph $\vec{\mathcal{G}}_\pi$ as follows:

- (1) The corresponding directed graph $\vec{\mathcal{G}}_\pi$ has exactly three connected components, two cycles and one double-loop, and can be represented as



Each cycle and each one multiple-loop gives rise to a trace in the right-hand side of (3.4).

- (2) If a connected component of $\vec{\mathcal{G}}_\pi$ is a cycle, we unfold it to obtain a horizontal line and replace each edge E_k by the matrix A_k if the direction of E_k goes from right to left in the horizontal line; otherwise, we replace E_k by A_k^T , the transpose of A_k . We then put the matrices A_k or A_k^T in a trace $\text{Tr}(\cdot)$ as they appear when we read the resulting horizontal line from left to right. For instance, the longest cycle of $\vec{\mathcal{G}}_\pi$ gives



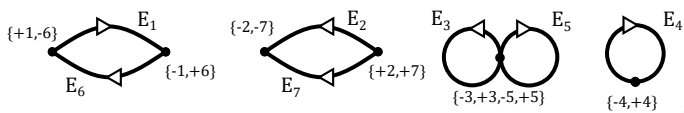
And so, we obtain the trace $\text{Tr}(A_7^T A_1 A_6 A_5^T)$ in (3.4). Note that $\text{Tr}(A_1 A_6 A_5^T A_7^T)$ and $\text{Tr}(A_2 A_3)$ do not depend on how the cycles in $\vec{\mathcal{G}}_\pi$ are unfolded since for any matrices $A, B \in \text{Mat}_N(\mathbb{C})$ we have $\text{Tr}(AB) = \text{Tr}(BA)$, $\text{Tr}(A) = \text{Tr}(A^T)$, and $(AB)^T = B^T A^T$.

- (3) On the other hand, a multiple-loop in $\vec{\mathcal{G}}_\pi$ with edges $E_{k_1}, E_{k_2}, \dots, E_{k_n}$ yields the trace of the Hadamard product of $A_{k_1}, A_{k_2}, \dots, A_{k_n}$. This way, we get $\text{Tr}(A_4 \circ A_8)$ in (3.4).

Thus, if π is now given by

$$\pi = \{-1, +6\}, \{+1, -6\}, \{-2, -7\}, \{+2, +7\}, \{-3, +3, -5, +5\}, \{-4, +4\},$$

the corresponding directed graph $\vec{\mathcal{G}}_\pi$ can be represented as



and hence, we obtain

$$\sum_{\substack{j: [\pm 7] \rightarrow [N] \\ \ker(j) \geq \pi}} \prod_{k=1}^7 A_k(j_{-k}, j_k) = \text{Tr}(A_1 A_6) \text{Tr}(A_2 A_7^T) \text{Tr}(A_3 \circ A_5) \text{Tr}(A_4).$$

3.2 Bounds of Graph Sums of The Discrete Fourier Transform Matrix

Although the bound for graph sums given by Theorem 5 is optimal in the set of all square matrices, it might not be optimal for some graph sums involving the discrete Fourier transform matrix. Let us recall that the N -by- N discrete Fourier transform matrix is the symmetric matrix H with entries given by

$$H(j_1, j_2) = \omega^{(j_1-1)(j_2-1)} \tag{3.5}$$

where $\omega = \exp(-\frac{2\pi}{N}\sqrt{-1})$ is a primitive N -th root of unity. Now, letting $\mathbf{h}(\mathbf{j})$ be given by

$$\mathbf{h}(\mathbf{j}) = \prod_{k=1}^m H(j_{-2k+1}, j_{2k-1})H^*(j_{-2k}, j_{2k}) \tag{3.6}$$

for each function $\mathbf{j} : [\pm 2m] \rightarrow [N]$, Theorem 5 gives us that

$$\left| \sum_{\substack{\mathbf{j}:[\pm 2m] \rightarrow [N] \\ \ker(\mathbf{j}) \geq \pi}} \mathbf{h}(\mathbf{j}) \right| \leq N^{\tau_\pi} \prod_{k=1}^m \|H\| \prod_{k=1}^m \|H^*\| = N^{m+\tau_\pi} \tag{3.7}$$

for any partition $\pi \in P(\pm 2m)$; on the other hand, since $\mathbf{h}(\mathbf{j})$ has absolute value 1, we also obtain

$$\left| \sum_{\substack{\mathbf{j}:[\pm 2m] \rightarrow [N] \\ \ker(\mathbf{j}) \geq \pi}} \mathbf{h}(\mathbf{j}) \right| \leq \sum_{\substack{\mathbf{j}:[\pm 2m] \rightarrow [N] \\ \ker(\mathbf{j}) \geq \pi}} 1 = N^{\#(\pi)}. \tag{3.8}$$

Thus, if π is the partition $\{\{2k - 1, -2k + 1, 2k, -2k\} \mid k = 1, 2, \dots, m\}$, then the graph sum exponent τ_π equals m , and hence, $\tau_\pi + m = 2m$, but also $\#(\pi) = m$, so (3.8) is a sharper bound than (3.7) in this case. In general, we prefer (3.8) over (3.7) since (3.8) is invariant under re-labeling of the entries of H and H^* in (3.6); namely, given a permutation $\sigma \in \text{Sym}(\pm 2m)$ and letting

$$\mathbf{h}(\mathbf{j} \circ \sigma) = \prod_{k=1}^m H(j_{\sigma(-2k+1)}, j_{\sigma(2k-1)})H^*(j_{\sigma(-2k)}, j_{\sigma(2k)})$$

for any function $\mathbf{j} : [\pm 2m] \rightarrow [N]$, the inequality in (3.8) implies

$$\left| \sum_{\substack{\mathbf{j}:[\pm 2m] \rightarrow [N] \\ \ker(\mathbf{j}) \geq \pi}} \mathbf{h}(\mathbf{j} \circ \sigma) \right| \leq N^{\#(\sigma^{-1} \circ \pi)} = N^{\#(\pi)}$$

since we have the relation

$$\sum_{\substack{\mathbf{j}:[\pm 2m] \rightarrow [N] \\ \ker(\mathbf{j}) \geq \pi}} \mathbf{h}(\mathbf{j} \circ \sigma) = \sum_{\substack{\mathbf{j}:[\pm 2m] \rightarrow [N] \\ \ker(\mathbf{j}) \geq \sigma^{-1} \circ \pi}} \mathbf{h}(\mathbf{j}). \tag{3.9}$$

Moreover, in the proof of Theorem 1, we will need to consider sums of the form

$$\sum_{\substack{\mathbf{j}:[\pm 2m] \rightarrow [N] \\ \ker(\mathbf{j}) = \pi}} \mathbf{h}(\mathbf{j} \circ \sigma) = \sum_{\substack{\mathbf{j}:[\pm 2m] \rightarrow [N] \\ \ker(\mathbf{j}) = \sigma^{-1} \circ \pi}} \mathbf{h}(\mathbf{j}) \tag{3.10}$$

where $m = m_1 + m_2$ for some integers $m_1, m_2 \geq 1$ and $\sigma \in \text{Sym}(\pm 2m)$ is the permutation with cycle decomposition given by

$$\begin{aligned} \sigma = & (-1, 1, -2, 2, \dots, -2m_1, 2m_1) \\ & (-2m_1 - 1, 2m_1 + 1, \dots, -2m_1 - 2m_2, 2m_1 + 2m_2). \end{aligned} \tag{3.11}$$

Although the sum in (3.10) is not a graph sum, it can be determined up to a term of order $N^{\# \pi - 1}$ analyzing (3.9) since for every partition $\pi \in P(\pm 2m)$ we have

$$\sum_{\substack{\mathbf{j}:[\pm 2m] \rightarrow [N] \\ \ker(\mathbf{j}) = \pi}} \mathbf{h}(\mathbf{j}) = \sum_{\substack{\mathbf{j}:[\pm 2m] \rightarrow [N] \\ \ker(\mathbf{j}) \geq \pi}} \mathbf{h}(\mathbf{j}) - \sum_{\substack{\theta \in P(\pm 2m) \\ \theta > \pi}} \sum_{\substack{\mathbf{j}:[\pm 2m] \rightarrow [N] \\ \ker(\mathbf{j}) = \theta}} \mathbf{h}(\mathbf{j}). \tag{3.12}$$

The rest of this section is devoted to find and classify partitions π such that (3.8) becomes an equality. To do that, let us first associate a polynomial to each partition $\pi \in P(\pm 2m)$.

The polynomial p_π . Given a partition $\pi = \{B_1, B_2, \dots, B_r\} \in P(\pm 2m)$, we let $p_\pi(x_1, x_2, \dots, x_r)$, or simply p_π , be the polynomial obtained from the expression

$$-x_{-1}x_1 + x_{-2}x_2 - x_{-3}x_3 + \dots + x_{-2m}x_{2m} \tag{3.13}$$

after replacing each variable x_k by x_l whenever k belongs to the block B_l . For instance, if $\pi = \{B_1 = \{-1, 3\}, B_2 = \{-3, 1\}, B_3 = \{-2, 2\}, B_4 = \{-4, 4\}\}$, then

$$p_\pi(x_1, x_2, x_3, x_4) = -x_1x_2 + x_3x_3 - x_2x_1 + x_4x_4.$$

Equivalently, the polynomial $p_\pi(x_1, x_2, \dots, x_r)$ is the image of (3.13) under the unique homomorphism from $\mathbb{Z}[x_{-1}, x_1, \dots, x_{-2m}, x_{2m}]$ to $\mathbb{Z}[x_1, x_2, \dots, x_r]$ such that $x_k \mapsto x_l$ whenever $k \in B_l$. Note that $p_\pi(x_1, x_2, \dots, x_r)$ has degree either 0 or 2 and can also be explicitly defined as

$$p_\pi(x_1, x_2, \dots, x_r) = \sum_{1 \leq t \leq s \leq r} a_{t,s} x_t x_s \tag{3.14}$$

where

$$a_{t,t} = \sum_{\substack{k \in [2m] \\ -k, k \in B_t}} (-1)^k \text{ and } a_{t,s} = \sum_{\substack{k \in [2m] \\ -k \in B_t, k \in B_s}} (-1)^k + \sum_{\substack{l \in [2m] \\ l \in B_t, -l \in B_s}} (-1)^l \text{ for } t \neq s; \tag{3.15}$$

moreover, $p_\pi(x_1, x_2, \dots, x_r)$ satisfies the relation

$$\sum_{\substack{\mathbf{j}: [\pm 2m] \rightarrow [N] \\ \ker(\mathbf{j}) \geq \pi}} \mathbf{h}(\mathbf{j}) = \sum_{j_1, j_2, \dots, j_r=0}^{N-1} e^{\frac{2\pi\sqrt{-1}}{N} p_\pi(j_1, j_2, \dots, j_r)}. \tag{3.16}$$

Therefore, (3.8) becomes an equality precisely when $p_\pi(x_1, x_2, \dots, x_r)$ is the zero polynomial. On the other hand, if $p_\pi(x_1, x_2, \dots, x_r)$ is a nonzero polynomial, we can then find a sharper bound than (3.8) via the reciprocity theorem for generalized Gauss sums, see [3, Section 1.2] for a proof of this theorem.

The reciprocity theorem for generalized Gauss sums Suppose a, b, c are integers with $a, c \neq 0$ and $ac + b$ even. Then,

$$S(a, b, c) := \sum_{j=0}^{|c|-1} e^{\pi\sqrt{-1} \frac{aj^2+bj}{c}} = \left| \frac{c}{a} \right|^{\frac{1}{2}} e^{\pi\sqrt{-1} \frac{|ac|-b^2}{4ac}} \sum_{j=0}^{|a|-1} e^{\pi\sqrt{-1} \frac{-cj^2-bj}{a}} \tag{3.17}$$

Proposition 7 If $p(x_1, x_2, \dots, x_r)$ is a nonzero polynomial of degree at most 2 in $\mathbb{Z}[x_1, x_2, \dots, x_r]$, then there exists a constant C_p independent of N such that

$$\left| \sum_{j_1, j_2, \dots, j_r=0}^{N-1} e^{-\frac{2\pi\sqrt{-1}}{N} p(j_1, j_2, \dots, j_r)} \right| \leq C_p N^{r-\frac{1}{2}}.$$

Proof Suppose $p(x_1, \dots, x_r) \in \mathbb{Z}[x_1, \dots, x_r]$ is a nonzero polynomial of degree at most 2. Without loss of generality, we can assume that there is a nonzero linear polynomial $q_1(x_1, \dots, x_r) = \alpha_1 x_1 + \alpha_2 x_2 + \dots + \alpha_r x_r \in \mathbb{Z}[x_1, x_2, \dots, x_r]$ and a polynomial $q_2(x_2, \dots, x_r) \in \mathbb{Z}[x_2, x_3, \dots, x_r]$ of degree at most 2 such that

$$p(x_1, \dots, x_r) = x_1 q_1(x_1, \dots, x_r) + q_2(x_2, \dots, x_r).$$

Since we have the inequality

$$\left| \sum_{j_1, j_2, \dots, j_r=0}^{N-1} e^{-\frac{2\pi\sqrt{-1}}{N} p(j_1, j_2, \dots, j_r)} \right| \leq \sum_{j_2, \dots, j_r=0}^{N-1} \left| \sum_{j_1=0}^{N-1} e^{-\frac{2\pi\sqrt{-1}}{N} j_1 q_1(j_1, j_2, \dots, j_r)} \right|,$$

we only need to show that there is a constant C_p independent from N such that

$$\sum_{j_2, \dots, j_r=0}^{N-1} \left| \sum_{j_1=0}^{N-1} e^{-\frac{2\pi\sqrt{-1}}{N} j_1 q_1(j_1, j_2, \dots, j_r)} \right| \leq C_p N^{r-\frac{1}{2}}.$$

Suppose $\alpha_1 \neq 0$. Then, we have that

$$\begin{aligned} \sum_{j_1=0}^{N-1} e^{-\frac{2\pi\sqrt{-1}}{N} j_1 q(j_1, j_2, \dots, j_m)} &= \sum_{j_1=0}^{N-1} e^{\pi\sqrt{-1} \frac{-2\alpha_1 j_1^2 - 2\sum_{k=2}^r \alpha_k j_k j_1}{N}} \\ &= S\left(-2\alpha_1, -2\sum_{k=2}^r \alpha_k j_k, N\right) \end{aligned}$$

where $S(a, b, c)$ denotes the generalized Gauss quadratic sum as in (3.17). Thus, by the reciprocity theorem for generalized Gauss sums, we get

$$\left| S\left(-2\alpha_1, -2\sum_{k=2}^r \alpha_k j_k, N\right) \right| \leq \left| \frac{N}{-2\alpha_1} \right|^{\frac{1}{2}} |-2\alpha_1| = |2\alpha_1 N|^{\frac{1}{2}},$$

and therefore, we obtain

$$\sum_{j_2, \dots, j_r=0}^{N-1} \left| \sum_{j_1=0}^{N-1} e^{-\frac{2\pi\sqrt{-1}}{N} j_1 q_1(j_1, j_2, \dots, j_r)} \right| \leq |2\alpha_1|^{\frac{1}{2}} N^{r-\frac{1}{2}}.$$

Now, suppose $\alpha_1 = 0$. Recall that

$$\sum_{j_1=0}^{N-1} e^{-\frac{2\pi\sqrt{-1}}{N} j_1 q_1(j_1, j_2, \dots, j_r)} = \begin{cases} N, & \text{if } q_1(j_1, \dots, j_r) = \sum_{l=2}^r \alpha_l j_l \equiv 0 \pmod{N} \\ 0, & \text{otherwise} \end{cases}$$

So, we have

$$\begin{aligned} &\sum_{j_2, \dots, j_r=0}^{N-1} \left| \sum_{j_1=0}^{N-1} e^{-\frac{2\pi\sqrt{-1}}{N} j_1 q_1(j_1, \dots, j_r)} \right| \\ &= N \cdot \# \left\{ (j_2, \dots, j_r) \in [0, N-1]^{r-1} : \sum_{l=2}^r \alpha_l j_l \equiv 0 \pmod{N} \right\}. \end{aligned}$$

But, since the polynomial $q_1(x_1, \dots, x_r) = \alpha_1 x_1 + \dots + \alpha_r x_r$ is nonzero, we must have $\alpha_k \neq 0$ for some $k \neq 1$, and hence, the equation

$$\alpha_k x + \beta \equiv 0 \pmod{N}$$

has at most $|\alpha_k|$ solutions in the set $\{0, 1, \dots, N - 1\}$ for any given integer β . Thus, we have

$$\# \left\{ (j_2, \dots, j_r) \in [0, N - 1]^{r-1} : \alpha_k j_k + \sum_{\substack{l=2 \\ l \neq k}}^r \alpha_l j_l \equiv 0 \pmod N \right\} \leq |\alpha_k| N^{r-2},$$

and therefore, we get

$$\sum_{j_2, \dots, j_r=0}^{N-1} \left| \sum_{j_1=0}^{N-1} e^{-\frac{2\pi\sqrt{-1}}{N} j_1 q_1(j_1, j_2, \dots, j_r)} \right| \leq |\alpha_k| N^{r-1}.$$

□

As an immediate consequence from (3.12), (3.16), and Proposition 7, we have the following.

Corollary 8 *If $p_\pi(x_1, x_2, \dots, x_r)$ is a nonzero polynomial for some partition $\pi = \{B_1, B_2, \dots, B_r\} \in P(\pm 2m)$, then there is a constant C independent from N so that*

$$\left| \sum_{\substack{\mathbf{j}: [\pm 2m] \rightarrow [N] \\ \ker(\mathbf{j}) = \pi}} \mathbf{h}(\mathbf{j}) \right| \leq C N^{\#(\pi) - \frac{1}{2}}.$$

The next two propositions establish necessary and sufficient conditions for $p_\pi(x_1, x_2, \dots, x_r)$ to be the zero polynomial. Roughly speaking, the polynomial $p_\pi(x_1, x_2, \dots, x_r)$ is zero if and only if the blocks of the partition π group the elements of the set $[\pm 2m]$ in such a way that the positive and negative signs appearing in (3.13) cancel each other out.

Proposition 9 *Suppose $\pi = \{B_1, B_2, \dots, B_{2m}\}$ is a pairing partition in $P(\pm 2m)$. Then the polynomial $p_\pi(x_1, x_2, \dots, x_{2m})$ is zero if and only if π is a symmetric partition such that $k \sim_\pi l$ implies $k + l$ odd for all integers $k, l \in [\pm 2m]$.*

Proof Suppose $p_\pi(x_1, x_2, \dots, x_{2m})$ is the zero polynomial and take $a_{t,s}$ as (3.15) for $1 \leq t \leq s \leq 2m$. To prove π is a symmetric partition such that $k \sim_\pi l$ implies $k + l$ odd for all integers $k, l \in [\pm 2m]$, it suffices to show that for every integer $k \in [2m]$ there exists an integer $l \in [2m]$ such that $k + l$ is odd and either $k \sim_\pi l$ and $-k \sim_\pi -l$ or $k \sim_\pi -l$ and $-k \sim_\pi l$. Fix $k \in [2m]$ and let $t', s' \in [2m]$ such that $k \in B_{t'}$ and $-k \in B_{s'}$. Since $p_\pi(x_1, \dots, x_{2m}) = \sum_{1 \leq t \leq s \leq r} a_{t,s} x_t x_s$ is the zero polynomial, we must have $a_{t',s'} = 0$. Now, if $t' \neq s'$, from (3.15) we get that

$$a_{t',s'} = (-1)^k + \sum_{\substack{l \in [2m] \setminus \{k\} \\ l \in B_{t'}, -l \in B_{s'}}} (-1)^l + \sum_{\substack{l \in [2m] \\ -l \in B_{t'}, l \in B_{s'}}} (-1)^l = 0, \tag{3.18}$$

which implies there exists $l \in [2m]$ such that $(-1)^k + (-1)^l$ is zero and either $l \in B_{t'}$ and $-l \in B_{s'}$ or $-l \in B_{t'}$ and $l \in B_{s'}$. But this is equivalent to the desired conclusion. A similar argument works for the case $s = t$.

Now, if the partition π is a symmetric pairing in $P(\pm 2m)$ such that $k \sim_{\pi} l$ implies $k+l$ odd for all integers $k, l \in [\pm 2m]$, we can write $\pi = \{B_1, B_2, \dots, B_{2m}\}$ with $B_1 = \{-k_1, -l_1\}$, $B_2 = \{k_1, l_1\}$, $B_3 = \{-k_2, -l_2\}$, $B_4 = \{k_2, l_2\}, \dots, B_{2m} = \{k_m, l_{2m}\}$ and $k_1, l_1, k_2, l_2, \dots, l_m \in [\pm 2m]$ satisfying $k_i + l_i$ odd for $i = 1, 2, \dots, m$. Moreover, since $\bigcup_{i=1}^{2m} B_i = [\pm 2m]$ and $(-1)^k = (-1)^{-k}$ for $k \in [\pm 2m]$, we have

$$-x_{-1}x_1 + x_{-2}x_2 - x_{-3}x_3 + \dots + x_{-2m}x_{2m} = \sum_{i=1}^m [(-1)^{k_i} x_{-k_i} x_{k_i} + (-1)^{l_i} x_{-l_i} x_{l_i}].$$

Therefore, from the definition of $p_{\pi}(x_1, x_2, \dots, x_{2m})$ and the fact that $k_i + l_i$ is odd for $i = 1, 2, \dots, m$, we get

$$p_{\pi}(x_1, x_2, \dots, x_{2m}) = \sum_{i=1}^m [(-1)^{k_i} x_{2i-1}x_{2i} + (-1)^{l_i} x_{2i-1}x_{2i}] = 0.$$

□

Proposition 10 *Let $\pi = \{B_1, B_2, \dots, B_n\}$ be a partition in $P(\pm 2m)$. If there is a partition $\theta \in P(\pm 2m)$ such that $\theta \leq \pi$ and p_{θ} is the zero polynomial, then p_{π} is also the zero polynomial. Conversely, if p_{π} is the zero polynomial, then there is a symmetric pairing partition $\theta \leq \pi$ such that p_{θ} is the zero polynomial.*

Proof Suppose $\theta \leq \pi$ and p_{θ} is the zero polynomial. Write $\theta = \{B_{1,1}, B_{1,2}, \dots, B_{1,m_1}, \dots, B_{n,m_n}\}$ with $B_i = \cup_{j=1}^{m_i} B_{i,j}$ for $i = 1, 2, \dots, n$. Take $\mathcal{A} = \mathbb{Z}[x_1, x_{-1}, \dots, x_{2m}, x_{-2m}]$, $\mathcal{B} = \mathbb{Z}[x_{1,1}, x_{1,2}, \dots, x_{1,m_1}, \dots, x_{n,m_n}]$, and $\mathcal{C} = \mathbb{Z}[x_1, x_2, \dots, x_n]$ and let $\Phi : \mathcal{A} \rightarrow \mathcal{B}$ and $\Psi : \mathcal{B} \rightarrow \mathcal{C}$ be the unique homomorphisms such that $\Phi(x_k) = x_{i,j}$ if $k \in B_{i,j}$ and $\Psi(x_{i,j}) = x_i$. Note that $(\Psi \circ \Phi)(x_k) = x_l$ only if $k \in B_l$, and thus, by definition of p_{π} and p_{θ} , we have that

$$p_{\pi} = \Psi \circ \Phi \left(\sum_{k=1}^m (-1)^k x_{-k} x_k \right) = \Psi(p_{\theta}).$$

Hence, if p_{θ} is the zero polynomial, so is p_{π} .

Suppose now p_{π} is the zero polynomial and let θ be a minimal element of the set $\{\widehat{\pi} \in P(\pm 2m) : \widehat{\pi} \leq \pi \text{ and } p_{\widehat{\pi}} = 0\}$ endowed with the partial order inherited from $P(\pm 2m)$. Since p_{θ} is the zero polynomial, it follows from the first part of Proposition 9’s proof that for every integer $k \in [2m]$ there exists an integer $l \in [2m]$ such that $k + l$ is odd and either $k \sim_{\theta} l$ and $-k \sim_{\theta} -l$ or $k \sim_{\theta} -l$ and $-k \sim_{\theta} l$. Therefore, θ lacks singletons and either θ is a pairing partition or θ has a block with at least three elements. Let us assume $\theta = \{C_1, C_2, \dots, C_n\}$ has a block with at least three elements, say C_n . The previous property of θ —borrowed from the first part of Proposition 9’s

proof—implies there are integers $k, l \in [2m]$ such that $k + l$ is odd and at least one of the following conditions holds:

- (1) $+k, +l \in C_n$ and $-k \sim_\theta -l$
- (2) $+k, -l \in C_n$ and $-k \sim_\theta +l$
- (3) $-k, -l \in C_n$ and $+k \sim_\theta +l$
- (4) $-k, +l \in C_n$ and $+k \sim_\theta -l$

Assume (1) holds. Then, $C_n \setminus \{k, l\}$ is not empty, and hence, letting $\widehat{C}_i = C_i$ for $i = 1, 2, \dots, n - 1$, $\widehat{C}_n = C_n \setminus \{k, l\}$, and $\widehat{C}_{n+1} = \{k, l\}$, we have $\widehat{\theta} = \{\widehat{C}_1, \widehat{C}_2, \dots, \widehat{C}_{n+1}\}$ is a partition of $[\pm 2m]$ such that $\widehat{\theta} \preceq \theta$, i.e., $\theta \geq \widehat{\theta}$ but $\theta \neq \widehat{\theta}$. Let us show that $p_{\widehat{\theta}}$ must be the zero polynomial, contradicting the minimality of θ . Take $\mathcal{A} = \mathbb{Z}[x_1, x_{-1}, \dots, x_m, x_{-m}]$, $\mathcal{B} = \mathbb{Z}[x_1, x_2, \dots, x_n]$, and $\widehat{\mathcal{B}} = \mathbb{Z}[x_1, x_2, \dots, x_{n+1}]$ and let $\Phi : \mathcal{A} \rightarrow \mathcal{B}$ and $\widehat{\Phi} : \mathcal{A} \rightarrow \widehat{\mathcal{B}}$ be the unique homomorphisms such that $\Phi(x_i) = x_j$ if $i \in C_j$ and $\widehat{\Phi}(x_i) = x_j$ if $i \in \widehat{C}_j$. Since $\Phi(x_i) = \widehat{\Phi}(x_i)$ for $i \in [\pm 2m] \setminus \{k, l\}$, we have

$$\sum_{\substack{i=1 \\ i \neq k, l}}^{2m} (-1)^i \Phi(x_{-i}) \Phi(x_i) = \sum_{\substack{i=1 \\ i \neq k, l}}^{2m} (-1)^i \widehat{\Phi}(x_{-i}) \widehat{\Phi}(x_i).$$

Moreover, since $-k \sim_\theta -l$, we have $\Phi(x_{-k}) = \Phi(x_{-l}) = \widehat{\Phi}(x_{-k}) = \widehat{\Phi}(x_{-l})$, so we get

$$\begin{aligned} 0 &= (-1)^k \Phi(x_{-k}) \Phi(x_k) + (-1)^l \Phi(x_{-l}) \Phi(x_l) \\ &= (-1)^k \widehat{\Phi}(x_{-k}) \widehat{\Phi}(x_k) + (-1)^l \widehat{\Phi}(x_{-l}) \widehat{\Phi}(x_l) \end{aligned}$$

since $k + l$ is odd, $\Phi(x_k) = \Phi(x_l) = x_n$, and $\widehat{\Phi}(x_k) = \widehat{\Phi}(x_l) = x_{n+1}$. Thus, we obtain

$$p_{\widehat{\theta}} = \sum_{i=1}^{2m} (-1)^i \widehat{\Phi}(x_{-i}) \widehat{\Phi}(x_i) = \sum_{i=1}^{2m} (-1)^i \Phi(x_{-i}) \Phi(x_i) = p_\theta = 0$$

But then, θ is not minimal, and therefore, (1) does not hold. Similar arguments show that neither (2), nor (3), nor (4) hold. Therefore, the partition θ must be a pairing, and, in fact, a symmetric pairing by Proposition 9. □

As mentioned earlier, in proving Theorem 1, we need to consider sums as in (3.10). Note that if $p_{\sigma^{-1} \circ \pi}$ is the zero polynomial for some permutation $\sigma \in \text{Sym}(\pm 2m)$, then $\mathbf{h}(\mathbf{j}) = 1$ for any function $\mathbf{j} : [\pm 2m] \rightarrow [N]$ satisfying $\ker(\mathbf{j}) \geq \sigma^{-1} \circ \pi$, and hence, we would get

$$\sum_{\substack{\mathbf{j}: [\pm 2m] \rightarrow [N] \\ \ker(\mathbf{j}) = \pi}} \mathbf{h}(\mathbf{j} \circ \sigma) = \sum_{\substack{\mathbf{j}: [\pm 2m] \rightarrow [N] \\ \ker(\mathbf{j}) = \sigma^{-1} \circ \pi}} \mathbf{h}(\mathbf{j}) = \frac{N!}{(N - \#(\pi))!}.$$

On the other hand, if the polynomial $p_{\sigma^{-1} \circ \pi}$ is nonzero, we have that (3.10) is of order $N^{\#(\pi)-1/2}$ by Corollary 8. We will now use the previous results to classify all symmetric pairing partitions so that $p_{\sigma^{-1} \circ \pi}$ is the zero polynomial.

Lemma 11 *Let $m = m_1 + m_2$ for some integers $m_1, m_2 \geq 1$, and let σ be the permutation given by (3.11). Suppose k and l are integers in $[2m]$ and π is a symmetric pairing partition in $P(\pm 2m)$ such that $p_{\sigma^{-1} \circ \pi}$ is the zero polynomial. If $-k \sim_{\pi} l$, then $\sigma^{-t}(-k) \sim_{\pi} \sigma^t(l)$ for every integer $t \geq 0$. On the other hand, if $-k \sim_{\pi} -l$, then $\sigma^t(-k) \sim_{\pi} \sigma^t(-l)$ for every integer $t \geq 0$.*

Proof Note that $\hat{k} \sim_{\pi} \hat{l}$ implies $\sigma(-\sigma^{-1}(\hat{k})) \sim_{\pi} \sigma(-\sigma^{-1}(\hat{l}))$. Indeed, by Proposition 10, the partition $\sigma^{-1} \circ \pi$ is symmetric since $p_{\sigma^{-1} \circ \pi}$ is the zero polynomial, and hence, $-\sigma^{-1}(\hat{k}) \sim_{\sigma^{-1} \circ \pi} -\sigma^{-1}(\hat{l})$ provided $\hat{k} \sim_{\pi} \hat{l}$, but in that case we must have $\sigma(-\sigma^{-1}(\hat{k})) \sim_{\pi} \sigma(-\sigma^{-1}(\hat{l}))$. Note also that for every integer $\hat{k} \in [\pm 2m]$ we have

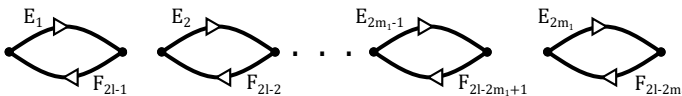
$$\sigma(-\sigma^{-1}(\hat{k})) = \begin{cases} \sigma(\hat{k}) & \text{if } \hat{k} > 0 \\ \sigma^{-1}(\hat{k}) & \text{if } \hat{k} < 0 \end{cases}$$

since for $1 \leq k \leq 2m$ we have $\sigma^{-1}(k) = -k$, $-\sigma^{-1}(-k) < 0$, and $\sigma(-k) = k$.

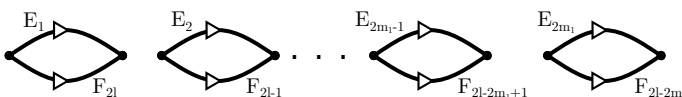
Now, suppose $\sigma^{-t}(-k) \sim_{\pi} \sigma^t(l)$ for some integer $t \geq 0$. If t is even, then $\hat{k} = \sigma^{-t}(-k) < 0 < \sigma^t(l) = \hat{l}$, and hence $\sigma^{-t-1}(-k) = \sigma(-\sigma^{-1}(\hat{k})) \sim_{\pi} \sigma(-\sigma^{-1}(\hat{l})) = \sigma^{t+1}(l)$. On the other hand, if t is odd, we have $\sigma^{-t}(-k) > 0 > \sigma^t(l)$, and hence $\sigma^{-t-1}(-k) = -\sigma^{-t}(-k) \sim_{\pi} -\sigma^t(l) = \sigma^{t+1}(l)$ since π is symmetric. Thus, $-k \sim_{\pi} l$ implies $\sigma^{-t}(-k) \sim_{\pi} \sigma^t(l)$ for every integer $t \geq 0$ by induction on t . Similarly, assuming $-k \sim_{\pi} -l$, we get $\sigma^t(-k) \sim_{\pi} \sigma^t(-l)$ for all $t \geq 0$. \square

Remark 12 The results regarding the polynomials p_{π} and $p_{\sigma^{-1} \circ \pi}$ being zero can be restated in terms of the graphs \mathcal{G}_{π} and $\vec{\mathcal{G}}_{\pi}$ from Sect. 3.1. For instance, in the following proposition we show that the polynomial $p_{\sigma^{-1} \circ \pi}$ is zero for a given symmetric partition $\pi \in P(\pm 2m)$ with $m = m_1 + m_2$ if and only if one of the following conditions for the directed graph $\vec{\mathcal{G}}_{\pi}$, where F_t denotes the edge E_{2m_1+t} for $t = 1, 2, \dots, 2m_2$, holds:

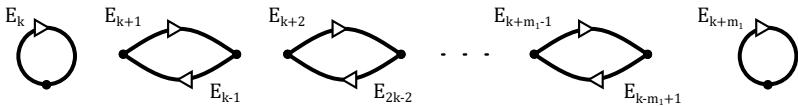
- (1) $m_1 = m_2$ and there is an integer $1 \leq l \leq m_2$ so that the graph $\vec{\mathcal{G}}_{\pi}$ can be represented as



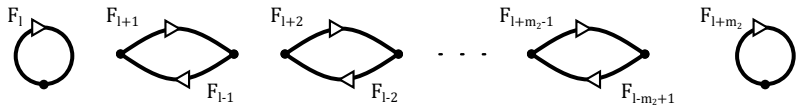
- (2) $m_1 = m_2$ and there is an integer $1 \leq l \leq m_2$ so that the graph $\vec{\mathcal{G}}_{\pi}$ can be represented as



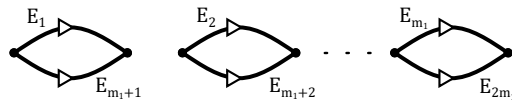
- (3) $\vec{\mathcal{G}}_{\pi}$ is the disjoint union of $\vec{\mathcal{G}}_{\pi_1}$ and $\vec{\mathcal{G}}_{\pi_2}$, there is an integer $1 \leq k \leq 2m_1$ so that $\vec{\mathcal{G}}_{\pi_1}$ can be represented as



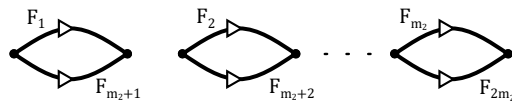
and there is an integer $2m_1 + 1 \leq l \leq 2m_1 + 2m_2$ so that $\vec{\mathcal{G}}_{\pi_2}$ can be represented as



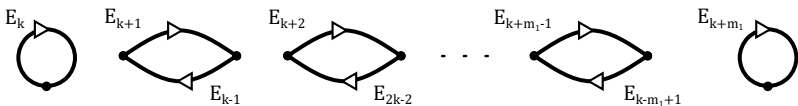
- (4) m_1 and m_2 are odd integers, the graph $\vec{\mathcal{G}}_{\pi}$ is the disjoint union of $\vec{\mathcal{G}}_{\pi_1}$ and $\vec{\mathcal{G}}_{\pi_2}$, the graph $\vec{\mathcal{G}}_{\pi_1}$ can be represented as



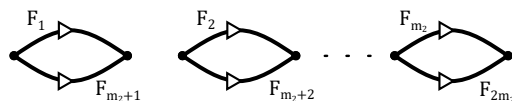
and the graph $\vec{\mathcal{G}}_{\pi_2}$ can be represented as



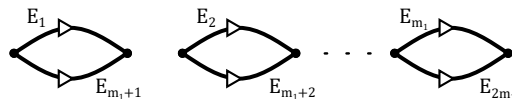
- (5) m_2 is odd, $\vec{\mathcal{G}}_{\pi}$ is the disjoint union of $\vec{\mathcal{G}}_{\pi_1}$ and $\vec{\mathcal{G}}_{\pi_2}$, there is an integer $1 \leq k \leq 2m_1$ so that $\vec{\mathcal{G}}_{\pi_1}$ can be represented as



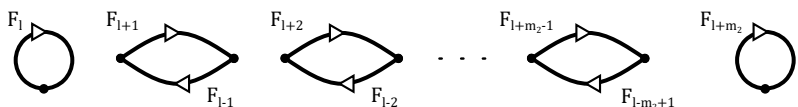
and the graph $\vec{\mathcal{G}}_{\pi_2}$ can be represented as



- (6) m_1 is odd, the graph $\vec{\mathcal{G}}_{\pi}$ is the disjoint union of $\vec{\mathcal{G}}_{\pi_1}$ and $\vec{\mathcal{G}}_{\pi_2}$, the graph $\vec{\mathcal{G}}_{\pi_1}$ can be represented as



and there is an integer $1 \leq l \leq 2m_1$ so that $\vec{\mathcal{G}}_{\pi_2}$ can be represented as



In the graphs above, $2l - t$, $2l + t - 1$, and $k \pm t$ are taken modulo $2m_1$ for $t = 1, 2, \dots, 2m_1$ and $l \pm t$ is taken modulo $2m_2$ for $t = 1, 2, \dots, 2m_2$.

Proposition 13 *Let $m = m_1 + m_2$ for some integers $m_1, m_2 \geq 1$, and let σ be the permutation given by (3.11). Suppose π is a symmetric pairing partition of $[\pm 2m]$ and denote by π_1 and π_2 the restrictions of π to $[\pm 2m_1]$ and $[\pm 2m] \setminus [\pm 2m_1]$, respectively. Then, $p_{\sigma^{-1} \circ \pi}$ is the zero polynomial if and only if one of the following conditions holds:*

- (1) $\pi \neq \pi_1 \sqcup \pi_2$, $m_1 = m_2$, and there are integers $1 \leq k \leq 2m_2$ and $2m_1 + 1 \leq l \leq 2m_1 + 2m_2$ such that $k + l$ is even and

$$\pi = \{ \{ \sigma^t(-k), \sigma^{-t}(l) \} \mid t = 1, 2, \dots, 4m_1 \}.$$

- (2) $\pi \neq \pi_1 \sqcup \pi_2$, $m_1 = m_2$, and there are integers $1 \leq k \leq 2m_2$ and $2m_1 + 1 \leq l \leq 2m_1 + 2m_2$ such that $k + l$ is odd and

$$\pi = \{ \{ \sigma^t(-k), \sigma^t(-l) \} \mid t = 1, 2, \dots, 4m_1 \}.$$

- (3) $\pi = \pi_1 \sqcup \pi_2$ and there are integers $1 \leq k \leq 2m_1$ and $2m_1 + 1 \leq l \leq 2m_1 + 2m_2$ such that

$$\pi_1 = \{ \{ \sigma^{t_1}(-k), \sigma^{-t_1}(k) \} \mid t_1 = 1, 2, \dots, 2m_1 \}$$

and

$$\pi_2 = \{ \{ \sigma^{t_2}(-l), \sigma^{-t_2}(l) \} \mid t_2 = 1, 2, \dots, 2m_2 \}.$$

- (4) $\pi = \pi_1 \sqcup \pi_2$, m_1 and m_2 are odd integers,

$$\pi_1 = \{ \{ \sigma^{t_1}(-1), \sigma^{t_1}(-m_1 - 1) \} \mid t_1 = 1, \dots, 2m_1 \},$$

and

$$\pi_2 = \{ \{ \sigma^{t_2}(-2m_1 - 1), \sigma^{t_2}(-2m_1 - m_2 - 1) \} \mid t_2 = 1, \dots, 2m_2 \}.$$

- (5) $\pi = \pi_1 \sqcup \pi_2$, m_2 is odd, there is an integer $1 \leq k \leq 2m_1$ such that

$$\pi_1 = \{ \{ \sigma^{t_1}(-k), \sigma^{-t_1}(k) \} \mid t_1 = 1, 2, \dots, 2m_1 \},$$

and

$$\pi_2 = \{ \{ \sigma^{t_2}(-2m_1 - 1), \sigma^{t_2}(-2m_1 - m_2 - 1) \} \mid t_2 = 1, \dots, 2m_2 \}.$$

- (6) $\pi = \pi_1 \sqcup \pi_2$, m_1 is odd,

$$\pi_1 = \{ \{ \sigma^{t_1}(-1), \sigma^{t_1}(-m_1 - 1) \} \mid t_1 = 1, \dots, 2m_1 \},$$

and there is an integer $2m_1 + 1 \leq l \leq 2m_1 + 2m_2$ such that

$$\pi_2 = \{ \{ \sigma^{t_2}(-l), \sigma^{-t_2}(l) \} \mid t_2 = 1, 2, \dots, 2m_2 \}.$$

Proof Put $\hat{\pi} = \sigma^{-1} \circ \pi$. Suppose $\hat{\pi} = \{B_1, B_2, \dots, B_r\}$ and let Φ be the unique homomorphism from $\mathbb{Z}[x_{-1}, x_1, \dots, x_{-2m}, x_{2m}]$ to $\mathbb{Z}[x_1, x_2, \dots, x_r]$ such that $\Phi(x_i) = x_j$ if $i \in B_j$. If condition (1) holds, then $\hat{\pi} = \{\{\sigma^t(-k), \sigma^{-t-2}(l)\} \mid t = 1, 2, \dots, 4m_1\}$ and $\sigma^t(-k) + \sigma^{-t-2}(l)$ is odd for $t = 1, 2, \dots, 4m_1$. Thus, since we can write

$$2 \cdot \sum_{i=1}^{2m} (-1)^i x_{-i} x_i = \sum_{t=1}^{2m_1} (-1)^{\sigma^{2t}(-k)} x_{\sigma^{2t}(-k)} x_{\sigma^{2t+1}(-k)} + \sum_{t=1}^{2m_1} (-1)^{\sigma^{-2t-2}(l)} x_{\sigma^{-(2t+1)-2}(l)} x_{\sigma^{-2t-2}(l)},$$

we get $p_{\hat{\pi}} = \Phi(\sum_{i=1}^{2m} (-1)^i x_{-i} x_i) = 0$. It follows from similar arguments that $p_{\hat{\pi}}$ is the zero polynomial if (2) holds. Now, if (4) holds and we take $l = 2m_1 + 1$, we have that $\sigma^t(-k) + \sigma^{-t-2}(k)$ and $\sigma^t(-l) + \sigma^t(-m_2 - l)$ are odd and $\hat{\pi} = \{\{\sigma^t(-k), \sigma^{-t-2}(k)\}, \{\sigma^t(-l), \sigma^t(-m_2 - l)\} \mid t \geq 0\}$. Thus, since we can write

$$\begin{aligned} \sum_{i=1}^{2m} (-1)^i x_{-i} x_i &= \frac{1}{2} \sum_{t=1}^{2m_1} (-1)^{\sigma^{2t}(-k)} x_{\sigma^{2t}(-k)} x_{\sigma^{2t+1}(-k)} \\ &\quad + \frac{1}{2} \sum_{t=1}^{2m_1} (-1)^{\sigma^{-2t-2}(k)} x_{\sigma^{-(2t+1)-2}(k)} x_{\sigma^{-2t-2}(k)} \\ &\quad + \sum_{t=1}^{m_2} (-1)^{\sigma^{2t}(-l)} x_{\sigma^{2t}(-l)} x_{\sigma^{2t+1}(-l)} \\ &\quad + \sum_{t=1}^{m_2} (-1)^{\sigma^{2t}(-m_2-l)} x_{\sigma^{2t}(-m_2-l)} x_{\sigma^{2t+1}(-m_2-l)} \end{aligned}$$

we get $p_{\hat{\pi}} = 0$. Similar arguments show that if either (3), (5), or (6) holds, then $p_{\hat{\pi}}$ is the zero polynomial.

Suppose now $p_{\hat{\pi}}$ is the zero polynomial and let $\hat{\pi}_1$ and $\hat{\pi}_2$ be the restrictions of $\hat{\pi}$ to $[\pm 2m_1]$ and $[\pm(2m_1 + 2m_2)] \setminus [\pm 2m_1]$, respectively. We will consider two cases $\hat{\pi} \neq \hat{\pi}_1 \sqcup \hat{\pi}_2$ and $\hat{\pi} = \hat{\pi}_1 \sqcup \hat{\pi}_2$. Assume first $\hat{\pi} \neq \hat{\pi}_1 \sqcup \hat{\pi}_2$. By Proposition 9, there are integers $1 \leq k \leq 2m_1$ and $2m_1 + 1 \leq l \leq 2m_1 + 2m_2$ such that $k + l$ is odd and one of the following holds:

- (1') $k \sim_{\hat{\pi}} -l$ and $-k \sim_{\hat{\pi}} l$.
- (2') $k \sim_{\hat{\pi}} l$ and $-k \sim_{\hat{\pi}} -l$.

Suppose (2') holds. Then, $-k = -\sigma(-k) \sim_{\pi} -\sigma(-l) = -l$, and by Lemma 11, we have that $\sigma^t(-k) \sim_{\pi} \sigma^t(-l)$ for every integer $t \geq 0$. Moreover, since $-k = \sigma^{4m_1}(-k)$, $\sigma^{4m_1}(-k) \sim_{\pi} \sigma^{4m_1}(-l)$, and π is a pairing, we must have $-l = \sigma^{4m_1}(-l)$. But, the equation $-l = \sigma^t(-l)$ holds only if t is an integer multiple of $4m_2$, and hence, $4m_1$ is a multiple of $4m_2$. Similarly, $4m_2$ is a multiple of $4m_1$, and therefore, $4m_1 = 4m_2$, and the partition $\hat{\pi}$ satisfies condition (2). A similar argument shows

that $\hat{\pi}$ satisfies condition (1) if we suppose (1') holds. Assume now $\hat{\pi} = \hat{\pi}_1 \sqcup \hat{\pi}_2$. By Proposition 9, there is an integer $1 < \hat{k} \leq 2m_1$ satisfying one of the following:

- (a) $1 \sim_{\hat{\pi}} \hat{k}, -1 \sim_{\hat{\pi}} -\hat{k}$, and $1 + \hat{k}$ is odd.
- (b) $1 \sim_{\hat{\pi}} -\hat{k}, -1 \sim_{\hat{\pi}} \hat{k}$, and $1 + \hat{k}$ is odd.

and there is an integer $2m_1 + 1 < \hat{l} \leq 2m_1 + 2m_2$ satisfying one of the following:

- (A) $2m_1 + 1 \sim_{\hat{\pi}} \hat{l}, -2m_1 - 1 \sim_{\hat{\pi}} -\hat{l}$, and $2m_1 + 1 + \hat{l}$ is odd.
- (B) $2m_1 + 1 \sim_{\hat{\pi}} -\hat{l}, -2m_1 - 1 \sim_{\hat{\pi}} \hat{l}$, and $2m_1 + 1 + \hat{l}$ is odd.

If (a) holds, we know that $\sigma^t(-1) \sim_{\pi} \sigma^t(-\hat{k})$ for every integer $t \geq 0$ by Lemma 11. But then, since $-\hat{k} = \sigma^{2\hat{k}-2}(-1)$, $\sigma^{2\hat{k}-2}(-1) \sim_{\pi} \sigma^{2\hat{k}-2}(-\hat{k})$, and π is a pairing, we must have $\sigma^{2\hat{k}-2}(-\hat{k}) = -1$, or, equivalently, $4\hat{k} - 4$ is a multiple of $4m_1$. Therefore, $m_1 = \hat{k} - 1$ is odd, and $\sigma^{t_1}(-1) \sim_{\hat{\pi}} \sigma^{t_1}(-m_1 - 1)$, and hence,

$$\pi_1 = \{ \{ \sigma^{t_1}(-1), \sigma^{t_1}(-m_1 - 1) \} \mid t_1 = 1, 2, \dots, 4m_1 \}$$

On the other hand, if (b) holds, it follows from Lemma 11 that $\sigma^t(1) \sim_{\pi} \sigma^{-t}(-\hat{k}')$ for every integer $t \geq 0$. Moreover, since \hat{k}' has the same parity as $1 + \hat{k}$, we have $\hat{k}' = 2k - 1$ for some integer $k \geq 1$. But then, since $k = \sigma^{2k-2}(1) = -\sigma^{2-2k}(2k - 1)$ and $\sigma^{2k-2}(1) \sim_{\pi} \sigma^{2-2k}(2k - 1)$, we have $k \sim_{\pi} -k$, and therefore,

$$\pi_1 = \{ \{ \sigma^{t_1}(k), -\sigma^{-t_1}(-k) \} \mid t_1 = 1, 2, \dots, 2m_1 \}$$

Similar arguments show that if (A) holds, then m_2 is odd and

$$\pi_2 = \{ \{ \sigma^{t_2}(-2m_1 - 1), \sigma^{t_2}(-2m_1 - m_2 - 1) \} \mid t_2 = 1, 2, \dots, 4m_2 \},$$

and if (B) holds, then there is an integer l such that

$$\pi_2 = \{ \{ \sigma^{t_2}(l), \sigma^{-t_2}(-l) \} \mid t_2 = 1, 2, \dots, 2m_2 \}$$

This completes the proof that if $p_{\hat{\pi}}$ is the zero polynomial, then $\hat{\pi}$ must satisfy either (1), (2), (3), (4), (5), or (6). □

4 The Bounded Cumulants Property

In this section, we first prove Lemma 3, and then, before we can apply it to get the conclusion in Theorem 4, we need to establish the relations between the notion of asymptotic free independence, the bounded cumulants property, and linear functionals on an algebra of non-commutative polynomials.

Proof of Lemma 3 Put $V_k = U_{N,i_k}^* U_{N,i_{\gamma(k)}}$ for $k = 1, 2, \dots, m$ and note that

$$\text{Tr}(Y_k) = \text{Tr} \left(A_{m'_k+1} V_{m'_k+1} A_{m'_k+2} V_{m'_k+2} \cdots A_{m'_k+m_k} V_{m'_k+m_k} \right).$$

Now, letting $\mathbf{a}(\mathbf{j}), \mathbf{v}_1(\mathbf{j}), \mathbf{v}_2(\mathbf{j}), \dots, \mathbf{v}_n(\mathbf{j})$ be given by

$$\mathbf{a}(\mathbf{j}) = \prod_{k=1}^m A_k(j_{-k}, j_k) \text{ and } \mathbf{v}_k(\mathbf{j}) = \prod_{l=m'_k+1}^{m'_k+m_k} V_l(j_l, j_{-\gamma(l)}) \text{ for } k = 1, 2, \dots, n$$

for each function $\mathbf{j} : [\pm m] \rightarrow [N]$, we have that

$$c_n [\text{Tr}(Y_1), \dots, \text{Tr}(Y_n)] = \sum_{\mathbf{j}:[\pm m] \rightarrow [N]} \mathbf{a}(\mathbf{j}) c_n [\mathbf{v}_1(\mathbf{j}), \mathbf{v}_2(\mathbf{j}), \dots, \mathbf{v}_n(\mathbf{j})] \tag{4.1}$$

since the matrices A_k are deterministic and the classical cumulants are multi-linear. By hypothesis, the family of random matrices $\{V_l\}_{l=1}^m$ is distribution-invariant under conjugation by signed permutation matrices, thus given a function $\mathbf{j} : [\pm m] \rightarrow [N]$ we have

$$c_n [\mathbf{v}_1(\mathbf{j}), \dots, \mathbf{v}_n(\mathbf{j})] = \prod_{k=1}^m \epsilon_{\sigma(j_k)} \epsilon_{\sigma(j_{-k})} c_n [\mathbf{v}_1(\sigma \circ \mathbf{j}), \dots, \mathbf{v}_n(\sigma \circ \mathbf{j})]$$

for all signs $\epsilon_1, \epsilon_2, \dots, \epsilon_N \in \{\pm 1\}$ and permutations $\sigma \in \text{Sym}(N)$. This implies that

$$c_n [\mathbf{v}_1(\mathbf{j}), \dots, \mathbf{v}_n(\mathbf{j})] = 0$$

whenever $\ker(\mathbf{j})$ contains at least one block of odd size, and

$$c_n [\mathbf{v}_1(\mathbf{j}), \dots, \mathbf{v}_n(\mathbf{j})] = c_n [\mathbf{v}_1(\mathbf{j}'), \dots, \mathbf{v}_n(\mathbf{j}')]]$$

provided a function $\mathbf{j}' : [\pm m] \rightarrow [N]$ satisfies $\ker(\mathbf{j}') = \ker(\mathbf{j})$. Thus, letting $c_n[\pi]$ denote the common value $c_n[\mathbf{v}_1(\mathbf{j}), \dots, \mathbf{v}_n(\mathbf{j})]$ among all those functions $\mathbf{j} : [\pm m] \rightarrow [N]$ satisfying $\ker(\mathbf{j}) = \pi$, Equation (4.1) becomes

$$c_n [\text{Tr}(Y_1), \dots, \text{Tr}(Y_n)] = \sum_{\pi \in P_{\text{even}}(\pm m)} c_n[\pi] \sum_{\substack{\mathbf{j}:[\pm m] \rightarrow [N] \\ \ker(\mathbf{j})=\pi}} \mathbf{a}(\mathbf{j}). \tag{4.2}$$

Moreover, the Möbius inversion formula in (2.3) implies

$$\sum_{\substack{\mathbf{j}:[\pm m] \rightarrow [N] \\ \ker(\mathbf{j})=\pi}} \mathbf{a}(\mathbf{j}) = \sum_{\substack{\theta \in P(\pm m) \\ \theta \geq \pi}} \mu(\pi, \theta) \sum_{\substack{\mathbf{j}:[\pm m] \rightarrow [N] \\ \ker(\mathbf{j}) \geq \theta}} \mathbf{a}(\mathbf{j})$$

since for all partitions $\theta \in P(\pm m)$ we have the relation

$$\sum_{\substack{\mathbf{j}:[\pm m] \rightarrow [N] \\ \ker(\mathbf{j}) \geq \theta}} \mathbf{a}(\mathbf{j}) = \sum_{\substack{\pi \in P(\pm m) \\ \pi \geq \theta}} \sum_{\ker(\mathbf{j})=\pi} \mathbf{a}(\mathbf{j}).$$

Hence, we get

$$c_n [\text{Tr} (Y_1) , \dots , \text{Tr} (Y_n)] = \sum_{\pi \in P_{\text{even}}(\pm m)} \sum_{\substack{\theta \in P_{\text{even}}(\pm m) \\ \theta \geq \pi}} c_n [\pi] \mu(\pi, \theta) \sum_{\substack{\mathbf{j}: [\pm m] \rightarrow [N] \\ \ker(\mathbf{j}) \geq \theta}} \mathbf{a}(\mathbf{j}) \tag{4.3}$$

Note that if a partition $\theta \in P(\pm m)$ has a block of the form $\{k, -k\}$, then

$$\sum_{\substack{\mathbf{j}: [\pm m] \rightarrow [N] \\ \ker(\mathbf{j}) \geq \theta}} \mathbf{a}(\mathbf{j}) = \text{Tr} (A_k) (\star)$$

where (\star) is a sum excluding the entries of A_k . Therefore, since each A_k is assumed to be of trace zero, we have

$$c_n [\text{Tr} (Y_1) , \dots , \text{Tr} (Y_n)] = \sum_{\pi \in P_{\text{even}}(\pm m)} \sum_{\substack{\theta \in P_{\chi}(\pm m) \\ \theta \geq \pi}} c_n [\pi] \mu(\pi, \theta) \sum_{\substack{\mathbf{j}: [\pm m] \rightarrow [N] \\ \ker(\mathbf{j}) \geq \theta}} \mathbf{a}(\mathbf{j}) \tag{4.4}$$

where $P_{\chi}(\pm m)$ denotes the set of all partitions in $P_{\text{even}}(\pm m)$ with no blocks of the form $\{k, -k\}$.

Now, for a partition $\theta \in P_{\chi}(\pm m)$, each connected component of the graph \mathcal{G}_{θ} , constructed as in Sect. 3.1, has at least two edges, and hence, \mathcal{G}_{θ} has at most $\frac{m}{2}$ connected components. Thus, from Theorem 5, Proposition 6, and the equality in (4.4), we get

$$|c_n [\text{Tr} (Y_1) , \dots , \text{Tr} (Y_n)]| \leq \sum_{\pi \in P_{\text{even}}(\pm m)} \sum_{\substack{\theta \in P_{\chi}(\pm m) \\ \theta \geq \pi}} |c_n [\pi]| |\mu(\pi, \theta)| N^{\frac{m}{2}} \prod_{k=1}^m \|A_k\| .$$

Since the sums above are over the finite sets $P_{\text{even}}(\pm m)$ and $P_{\chi}(\pm m)$, our proof will be complete if we show that there is a constant C_n independent from N such that

$$|c_n [\mathbf{v}_1(\mathbf{j}), \dots , \mathbf{v}_n(\mathbf{j})]| \leq C_n N^{-\frac{m}{2}}$$

for all functions $\mathbf{j} : [\pm m] \rightarrow [N]$. Let $\mathbf{j} : [\pm m] \rightarrow [N]$ be arbitrary. By Hölder’s inequality, letting $m_B := \sum_{k \in B} m_k$ for any given subset B of $[n]$, we have

$$\left\| \prod_{k \in B} \mathbf{v}_k(\mathbf{j}) \right\|_1 = \left\| \prod_{k \in B} \prod_{l=m'_k+1}^{m'_k+m_k} V_l(j_l, j_{-\gamma(l)}) \right\|_1 \leq \prod_{k \in B} \prod_{l=m'_k+1}^{m'_k+m_k} \|V_l(j_l, j_{-\gamma(l)})\|_{m_B} .$$

But, by hypothesis, the p -norms of the entries of $\sqrt{N}V_l$ are uniformly bounded, i.e., there are constants $C_p = \max_{k=1}^m C_p(i_k, i_{\gamma(k)})$ with $p = 1, 2, \dots, m$ such that

$$\|V_l(j_l, j_{-\gamma(l)})\|_p \leq C_p(i_l, i_{\gamma(l)})N^{-\frac{1}{2}} \leq C_p N^{-\frac{1}{2}}$$

for all integers $1 \leq j_l, j_{-\gamma(l)} \leq N$ and $l = 1, 2, \dots, m$, and hence, we get

$$\left\| \prod_{k \in B} \mathbf{v}_k(\mathbf{j}) \right\|_1 \leq \prod_{k \in B} \prod_{l=m'_k+1}^{m'_k+m_k} C_{m_B} N^{-\frac{1}{2}} = \left(C_{m_B} N^{-\frac{1}{2}} \right)^{m_B}.$$

Now, the moment–cumulants relation in (2.4) implies

$$|c_n[\mathbf{v}_1(\mathbf{j}), \dots, \mathbf{v}_n(\mathbf{j})]| \leq \sum_{\pi \in P(n)} |\mu(\pi, 1_n)| \prod_{B \in \pi} \left\| \prod_{k \in B} \mathbf{v}_k(\mathbf{j}) \right\|_1,$$

so it follows that

$$\begin{aligned} |c_n[\mathbf{v}_1(\mathbf{j}), \dots, \mathbf{v}_n(\mathbf{j})]| &\leq \sum_{\pi \in P(n)} |\mu(\pi, 1_n)| \prod_{B \in \pi} \left(C_{m_B} N^{-\frac{1}{2}} \right)^{m_B} \\ &= N^{-\frac{m}{2}} \sum_{\pi \in P(n)} |\mu(\pi, 1_n)| \prod_{B \in \pi} (C_{m_B})^{m_B}. \end{aligned}$$

And the proof of Lemma 3 is now complete. □

Now, asymptotic free independence and the bounded cumulants property can be stated in terms of some linear functionals, and, by doing so, we can show the bounded cumulants property is actually equivalent to a condition that is a consequence of Lemma 3, see Proposition 15 and Corollary 16. Thus, to prove Theorem 4, we first examine the relations between the notion of asymptotic free independence, the bounded cumulants property, and linear functionals on an algebra of non-commutative polynomials first.

Multi-linear Functionals on Non-commutative Polynomials and Notions from Free Probability

Let I be a non-empty set. Let \mathcal{A} denote the algebra of non-commutative polynomials $\mathbb{C}\langle x_i \mid i \in I \rangle$, and let $\mathcal{A}_i \subset \mathcal{A}$ denote the algebra of polynomials $\mathbb{C}\langle x_i \rangle$ for each index $i \in I$. Suppose we are given random matrix ensembles $\{X_{N,i}\}_{N=1}^\infty$ with $i \in I$ where each $X_{N,i}$ is a N -by- N random matrix and consider the sequence of unital linear functional $\{\varphi_N : \mathcal{A} \rightarrow \mathbb{C}\}_{N=1}^\infty$ where each φ_N is defined by

$$\varphi_N[p] := \mathbb{E}[\text{tr}(p(\{X_{N,i}\}_{i \in I}))] \quad \forall p \in \mathcal{A}. \tag{4.5}$$

Note that the two conditions necessary for the random matrix ensembles $\{X_{N,i}\}_{N=1}^\infty$ with $i \in I$ to be asymptotically freely independent, namely (AF.1) and (AF.2) from Definition 1, can be stated in terms of the linear functionals φ_N as

$$(AF.1) \quad \lim_{N \rightarrow \infty} \varphi_N [p] \text{ exists for every } p \in \mathcal{A}_i \text{ and every } i \in I, \text{ and}$$

$$(AF.2) \quad \lim_{N \rightarrow \infty} \varphi_N [(p_1 - \varphi_N [p_1])(p_2 - \varphi_N [p_2]) \cdots (p_m - \varphi_N [p_m])] = 0 \text{ whenever } p_k \in \mathcal{A}_{i_k} \text{ with } i_1 \neq i_2, i_2 \neq i_3, \dots, i_{m-1} \neq i_m$$

Moreover, assuming that (AF.1) holds, we can replace each $\varphi_N [p_k]$ appearing in (AF.2) by $\varphi [p_k] := \lim_{N \rightarrow \infty} \varphi_N [p_k]$; more concretely, we have the following.

Proposition 14 *Suppose each ensemble $\{X_{N,i}\}_{N=1}^\infty$ has a limiting distribution, namely $\varphi [p] := \lim_{N \rightarrow \infty} \varphi_N [p]$ exists for every $p \in \mathcal{A}_i$ and every $i \in I$. Then the ensembles $\{X_{N,i}\}_{N=1}^\infty$ with $i \in I$ are asymptotically freely independent if and only if the following holds:*

$$(AF.2') \quad \lim_{N \rightarrow \infty} \varphi_N [(p_1 - \varphi [p_1])(p_2 - \varphi [p_2]) \cdots (p_m - \varphi [p_m])] = 0 \text{ whenever } p_k \in \mathcal{A}_{i_k} \text{ with } i_1 \neq i_2, i_2 \neq i_3, \dots, i_{m-1} \neq i_m$$

Moreover, if either (AF.2) or (AF.2') holds, then $\lim_{N \rightarrow \infty} \varphi_N [p]$ exists for every $p \in \mathcal{A}$.

Proof Let J be the set of all positive integers m satisfying the following property: if $p_1 \in \mathcal{A}_{i_1}, p_2 \in \mathcal{A}_{i_2}, \dots, p_m \in \mathcal{A}_{i_m}$ with $i_1, i_2, \dots, i_m \in I$ and $i_1 \neq i_2, i_2 \neq i_3, \dots, i_{m-1} \neq i_m$, then $\lim_{N \rightarrow \infty} \varphi_N [p_1 p_2 \cdots p_m]$ exists. Since the algebras \mathcal{A}_i with $i \in I$ generate \mathcal{A} and each φ_N is linear, $\lim_{N \rightarrow \infty} \varphi_N [p]$ exists for every $p \in \mathcal{A}$ if the set J contains every positive integer. Now, by hypothesis, 1 belongs to J , so let us assume 1, 2, $\dots, m - 1$ belong to J and suppose p_1, p_2, \dots, p_m are as above. Thus, if $S = \{k_1 < k_2 < \dots < k_{|S|}\}$ is a strict subset of $[m]$, the limits

$$\lim_{N \rightarrow \infty} (-1)^{|S^c|} \prod_{k \in S^c} \varphi_N [p_k] \varphi_N \left[\prod_{k \in S} p_k \right] \quad \text{and} \quad \lim_{N \rightarrow \infty} (-1)^{|S^c|} \prod_{k \in S^c} \varphi [p_k] \varphi_N \left[\prod_{k \in S} p_k \right],$$

where S^c denotes the complement of S in the set $[m]$ and $|S^c|$ denotes the cardinality of S^c , exist. Moreover, if (AF.2) holds, the equality

$$\begin{aligned} \varphi_N [(p_1 - \varphi_N [p_1]) \cdots (p_m - \varphi_N [p_m])] &= \varphi_N [p_1 \cdots p_m] \\ &+ \sum_{S \subsetneq [m]} (-1)^{|S^c|} \prod_{k \in S^c} \varphi_N [p_k] \varphi_N \left[\prod_{k \in S} p_k \right], \end{aligned}$$

implies $\lim_{N \rightarrow \infty} \varphi_N [p_1 \cdots p_m]$ exists. And therefore, J contains every positive integer by induction on m . Similarly, if (AF.2') holds, then $\lim_{N \rightarrow \infty} \varphi_N [p_1 \cdots p_m]$ exists, and hence J contains every positive integer, since each $\varphi_N [p_k]$ in the equality above can be replaced by $\varphi [p_k]$.

Let us now show that (AF.2) and (AF.2') are equivalent. Suppose $p_1 \in \mathcal{A}_{i_1}, p_2 \in \mathcal{A}_{i_2}, \dots, p_m \in \mathcal{A}_{i_m}$ with $i_1, i_2, \dots, i_m \in I$ and $i_1 \neq i_2, i_2 \neq i_3, \dots, i_{m-1} \neq i_m$ and

take $q_k = p_k - \varphi [p_k]$ for $k = 1, 2, \dots, m$. We then have $\lim_{N \rightarrow \infty} \varphi_N [q_k] = 0$ and the equality

$$\begin{aligned} &\varphi_N [(p_1 - \varphi_N [p_1]) \cdots (p_m - \varphi_N [p_m])] \\ &= \varphi_N [q_1 \cdots q_m] + \sum_{S \subsetneq [m]} (-1)^{|S^c|} \prod_{k \in S^c} \varphi_N [q_k] \varphi_N \left[\prod_{k \in S} q_k \right] \\ &= \varphi_N [(q_1 - \varphi_N [q_1]) \cdots (q_m - \varphi_N [q_m])] \end{aligned}$$

Thus, if condition (AF.2') holds, then $\lim_{N \rightarrow \infty} \varphi_N [p]$ exists for every $p \in \mathcal{A}$, and hence,

$$0 = \lim_{N \rightarrow \infty} (-1)^{|S^c|} \prod_{k \in S^c} \varphi_N [q_k] \varphi_N \left[\prod_{k \in S} q_k \right] \quad \forall S \subsetneq [m];$$

additionally, we have $\lim_{N \rightarrow \infty} \varphi_N [(p_1 - \varphi [p_1]) \cdots (p_m - \varphi [p_m])] = \lim_{N \rightarrow \infty} \varphi_N [q_1 \cdots q_m] = 0$, and thus

$$\lim_{N \rightarrow \infty} \varphi_N [(p_1 - \varphi_N [p_1]) \cdots (p_m - \varphi_N [p_m])] = 0.$$

This shows that (AF.2') implies (AF.2). Similarly, (AF.2) implies (AF.2'). □

In the literature, however, the most common definition of asymptotic free independence for random matrix ensembles in terms of the linear functionals φ_N defined by (4.5) goes as follows: $\{X_{N,i}\}_{N=1}^\infty$ with $i \in I$ are asymptotically freely independent if they have a joint limiting (algebraic) distribution, i.e., $\lim_{N \rightarrow \infty} \varphi_N [p]$ exist for every polynomial $p \in \mathcal{A}$, and letting $\varphi := \lim_{N \rightarrow \infty} \varphi_N$, we have

$$\varphi[(p_1 - \varphi [p_1])(p_2 - \varphi [p_2]) \cdots (p_m - \varphi [p_m])] = 0$$

whenever $p_k \in \mathcal{A}_{i_k}$ with $i_1 \neq i_2, i_2 \neq i_3, \dots, i_{m-1} \neq i_m$. The previous proposition shows equivalence between the common definition of asymptotic free independence and the one given in the introduction of this paper.

Now, the bounded cumulants property for the random matrix ensemble $\{\{X_{N,i}\}_{i \in I}\}_{N=1}^\infty$ can also be established in terms of multi-linear functionals. If for each integer $n \geq 1$, we consider the n -linear map $\rho_N : \mathcal{A} \times \cdots \times \mathcal{A} \rightarrow \mathbb{C}$ defined by

$$\rho_N [p_1, p_2, \dots, p_n] = c_n [\text{Tr}(p_1(\{X_{N,i}\}_{i \in I})), \dots, \text{Tr}(p_n(\{X_{N,i}\}_{i \in I}))] \quad (4.6)$$

for all $p_1, p_2, \dots, p_n \in \mathcal{A}$ and where $c_n[\cdot, \dots, \cdot]$ denotes the classical cumulant, from Sect. 2.1, the random matrix ensemble $\{\{X_{N,i}\}_{i \in I}\}_{N=1}^\infty$ has then the bounded cumulants property if only if

$$\sup_N |\rho_N [p_1, p_2, \dots, p_n]| < \infty \quad (4.7)$$

for all $p_1, p_2, \dots, p_n \in \mathcal{A}$ and all integers $n \geq 1$. Moreover, under some mild assumptions, each polynomial p_k appearing in (4.7) can be replaced by

$$(p_1^{(k)} - \varphi_N[p_1^{(k)}])(p_2^{(k)} - \varphi_N[p_2^{(k)}]) \cdots (p_{m_k}^{(k)} - \varphi_N[p_{m_k}^{(k)}])$$

for some polynomials $p_1^{(k)} \in \mathcal{A}_{i_1^{(k)}}$, $p_2^{(k)} \in \mathcal{A}_{i_2^{(k)}}$, \dots , $p_{m_k}^{(k)} \in \mathcal{A}_{i_{m_k}^{(k)}}$ and still get the bounded cumulants property.

Proposition 15 *Suppose $\varphi_N : \mathcal{A} \rightarrow \mathbb{C}$ is a unital linear functional and $\rho_N : \mathcal{A} \times \cdots \times \mathcal{A} \rightarrow \mathbb{C}$ is an n -linear functional for each integer $N \geq 1$. If the limits $\lim_{N \rightarrow \infty} \varphi_N [p]$ and $\lim_{N \rightarrow \infty} \rho_N [p_1, p_2, \dots, p_n]$ exist for all $p \in \mathcal{A}$, $p_1 \in \mathcal{A}_{i_1}$, $p_2 \in \mathcal{A}_{i_2}$, \dots , $p_n \in \mathcal{A}_{i_n}$ with $i_1, i_2, \dots, i_n \in I$, then the following are equivalent:*

- (1) $\sup_N |\rho_N [p_1, p_2, \dots, p_n]| < \infty$ for all $p_1, p_2, \dots, p_n \in \mathcal{A}$
- (2) $\sup_N |\rho_N [q_1, q_2, \dots, q_n]| < \infty$ if each q_k is of the form

$$q_k = p_1^{(k)} p_2^{(k)} \cdots p_{m_k}^{(k)}$$

with $p_j^{(k)} \in \mathcal{A}_{i_j^{(k)}}$ and $i_1^{(k)} \neq i_2^{(k)}, i_2^{(k)} \neq i_3^{(k)}, \dots, i_{m_k-1}^{(k)} \neq i_{m_k}^{(k)}$

- (3) $\sup_N |\rho_N [q_{N,1}, q_{N,2}, \dots, q_{N,n}]| < \infty$ if each $q_{N,k}$ is of the form

$$q_{N,k} = (p_1^{(k)} - \varphi_N[p_1^{(k)}])(p_2^{(k)} - \varphi_N[p_2^{(k)}]) \cdots (p_{m_k}^{(k)} - \varphi_N[p_{m_k}^{(k)}])$$

with $p_j^{(k)} \in \mathcal{A}_{i_j^{(k)}}$ and $i_1^{(k)} \neq i_2^{(k)}, i_2^{(k)} \neq i_3^{(k)}, \dots, i_{m_k-1}^{(k)} \neq i_{m_k}^{(k)}$

Proof Conditions (1) and (2) are equivalent since each ρ_N is n -linear and the algebra \mathcal{A} is generated by the sub-algebras $\{\mathcal{A}_i\}_{i \in I}$. We only need to prove that (1) implies (3) and (3) implies (2).

Suppose (1) holds and let $q_{N,k}$ is as in (3) for $k = 1, 2, \dots, n$. Then, by multilinearity, we have

$$\begin{aligned} &\rho_N [q_{N,1}, \dots, q_{N,n}] \\ &= \sum_{J_1 \subset [m_1], \dots, J_n \subset [m_n]} \left(\prod_{k=1}^n \prod_{j \in J_k^c} (-1)^{|J_k^c|} \varphi_N [p_j^{(k)}] \right) \cdot \rho_N \left[\vec{\prod}_{j \in J_1} p_j^{(1)}, \dots, \vec{\prod}_{j \in J_n} p_j^{(n)} \right] \end{aligned}$$

The sum above is a finite sum, and, by hypothesis, each of its elements is uniformly bounded with respect to N . Hence, (3) follows.

Let us assume now (3) holds, and let J be the set of all positive integers m satisfying the following property: If $m = m_1 + m_2 + \cdots + m_n$ for some positive integers m_1, m_2, \dots, m_n , and $p_j^{(k)} \in \mathcal{A}_{i_j^{(k)}}$ for $j = 1, 2, \dots, m_k$ and $i_1^{(k)} \neq i_2^{(k)}, i_2^{(k)} \neq i_3^{(k)}, \dots, i_{m_k-1}^{(k)} \neq i_{m_k}^{(k)}$ for $k = 1, 2, \dots, n$, then $\sup_N |\rho_N (q_1, q_2, \dots, q_n)| < \infty$

where each q_k is given by $q_k = p_1^{(k)} p_2^{(k)} \cdots p_{m_k}^{(k)}$. Note that we are done if we show that $J = \{n, n + 1, n + 2, \dots\}$. By hypothesis, n belongs to J , so let us assume $n, n + 1, \dots, m - 1$ belong to J and let $p_j^{(k)}$, $q_{N,k}$ and q_k as above. Consider the equality

$$\begin{aligned} & \rho_N [q_{N,1}, \dots, q_{N,n}] - \rho_N [q_1, \dots, q_n] \\ &= \sum_{\substack{J_1 \subset [m_1], \dots, J_n \subset [m_n] \\ \cup_k J_k^c \neq \emptyset}} \left(\prod_{k=1}^n \prod_{j \in J_k^c} (-1)^{|J_k^c|} \varphi_N [p_i^{(k)}] \right) \cdot \rho_N \left[\vec{\prod}_{j \in J_1} p_j^{(1)}, \dots, \vec{\prod}_{j \in J_n} p_j^{(n)} \right]. \end{aligned}$$

given by n -linearity of ρ_N . Now, since (3) holds, $\rho_N(q_{N,1}, \dots, q_{N,n})$ is uniformly bounded with respect to N and, by induction hypothesis, so is $\rho_N[\vec{\prod}_{j \in J_1} p_j^{(1)}, \dots, \vec{\prod}_{j \in J_n} p_j^{(n)}]$ if at least one J_k is not $[m_k]$. Thus, $\rho_N(q_1, \dots, q_n)$ is also uniformly bounded with respect to N , and hence, m belongs to J . \square

The multi-linear functionals $\rho_N : \mathcal{A} \times \cdots \times \mathcal{A} \rightarrow \mathbb{C}$ given by (4.6) are *tracial in each entry*, i.e., for ever integer $k \in [n]$ and polynomials $q_0, q_1, \dots, q_n \in \mathcal{A}$, we have

$$\rho_N [q_1, \dots, q_{k-1}, q_0 q_k, q_{k+1}, \dots, q_n] = \rho_N [q_1, \dots, q_{k-1}, q_k q_0, q_{k+1}, \dots, q_n].$$

This traciality allows us to impose the condition that $i_{m_k}^{(k)} \neq i_1^{(k)}$ in (2) and (3) from Proposition 15 and still get uniform boundedness of $\rho_N [p_1, p_2, \dots, p_n]$ with respect to N .

Corollary 16 *Suppose \mathcal{A} , \mathcal{A}_i , φ_N , and ρ_N are as in Proposition 15. If ρ_N is tracial in each entry, then condition (1) from Proposition 15 is equivalent to any of the following:*

- (2') $\sup_N | [q_1, q_2, \dots, q_n] | < \infty$ if each q_k is of the form $q_k = p_1^{(k)} p_2^{(k)} \cdots p_{m_k}^{(k)}$ with $p_j^{(k)} \in \mathcal{A}_{i_j^{(k)}}$ and $i_1^{(k)} \neq i_2^{(k)}, i_2^{(k)} \neq i_3^{(k)}, \dots, i_{m_k-1}^{(k)} \neq i_{m_k}^{(k)}$, and $i_{m_k}^{(k)} \neq i_1^{(k)}$
- (3') $\sup_N | \rho_N [q_{N,1}, q_{N,2}, \dots, q_{N,n}] | < \infty$ if each $q_{N,k}$ is of the form

$$q_{N,k} = (p_1^{(k)} - \varphi_N [p_1^{(k)}]) (p_2^{(k)} - \varphi_N [p_2^{(k)}]) \cdots (p_{m_k}^{(k)} - \varphi_N [p_{m_k}^{(k)}])$$

with $p_j^{(k)} \in \mathcal{A}_{i_j^{(k)}}$ and $i_1^{(k)} \neq i_2^{(k)}, i_2^{(k)} \neq i_3^{(k)}, \dots, i_{m_k-1}^{(k)} \neq i_{m_k}^{(k)}$, and $i_{m_k}^{(k)} \neq i_1^{(k)}$

Proof Note that while condition (2) from Proposition 15 allows the indexes i_1^k and $i_{m_k}^k$ to be possibly the same, condition (2') above explicitly prohibits this. Thus, by traciality of ρ_N in each entry, we have that (2') and (2) are equivalent, and hence, it only remains to show that (3') above implies (3) from Proposition 15.

Assume (3') holds and let J be the set of all positive integers m satisfying the following property: if $m = m_1 + m_2 + \cdots + m_n$ for some positive integers m_1, m_2, \dots, m_n ,

and $p_j^{(k)} \in \mathcal{A}_{i_j^{(k)}}$ for $j = 1, 2, \dots, m_k$ and $i_1^{(k)} \neq i_2^{(k)}, i_2^{(k)} \neq i_3^{(k)}, \dots, i_{m_k-1}^{(k)} \neq i_{m_k}^{(k)}$ for $k = 1, 2, \dots, n$, then

$$\sup_N |\rho_N [q_{N,1}, q_{N,2}, \dots, q_{N,n}]| < \infty \tag{4.8}$$

where each $q_{N,k}$ as above. By hypothesis, n belongs to J , so let us assume $n, n + 1, \dots, m - 1$ belong to J and let $p_j^{(k)}, q_{N,k}$ and q_k as above. Thus, if $i_{m_k}^{(k)} \neq i_1^{(k)}$ for $k = 1, 2, \dots, n$, Inequality (4.8) holds. On the other hand, if $i_{m_k}^{(k)} = i_1^{(k)}$ for some $k \in \{1, 2, \dots, n\}$, let us consider polynomials $\tilde{p}_{N,k}$ and $\tilde{r}_{N,k}$ given by

$$\begin{aligned} \tilde{p}_{N,k} &= (p_{m_k}^{(k)} - \varphi_N[p_{m_k}^{(k)}])(p_1^{(k)} - \varphi_N[p_1^{(k)}]) \\ \tilde{r}_{N,k} &= (p_2^{(k)} - \varphi_N[p_2^{(k)}])(p_3^{(k)} - \varphi_N[p_3^{(k)}]) \cdots (p_{m_k-1}^{(k)} - \varphi_N[p_{m_k-1}^{(k)}]) \end{aligned}$$

By traciality of ρ_N in the k -th entry, we have

$$\rho_N [q_{N,1}, \dots, q_{N,k}, \dots, q_{N,n}] = \rho_N [q_{N,1}, \dots, \tilde{p}_{N,k}\tilde{r}_{N,k}, \dots, q_{N,n}];$$

moreover, from the relation

$$\begin{aligned} \tilde{p}_{N,k} &= (p_{m_k}^{(k)}p_1^{(k)} - \varphi_N[p_{m_k}^{(k)}p_1^{(k)}]) + \varphi_N[p_{m_k}^{(k)}p_1^{(k)}] - \varphi_N[p_{m_k}^{(k)}]\varphi_N[p_1^{(k)}] \\ &\quad - \varphi_N[p_{m_k}^{(k)}](p_1^{(k)} - \varphi_N[p_1^{(k)}]) - \varphi_N[p_1^{(k)}](p_{m_k}^{(k)} - \varphi_N[p_{m_k}^{(k)}]) \end{aligned}$$

we get the equality

$$\begin{aligned} \rho_N [q_{N,1}, \dots, q_{N,n}] &= \rho_N [q_{N,1}, \dots, (p_{m_k}^{(k)}p_1^{(k)} - \varphi_N[p_{m_k}^{(k)}p_1^{(k)}])\tilde{r}_{N,k}, \dots, q_{N,n}] \\ &\quad + \varphi_N[p_{m_k}^{(k)}p_1^{(k)}]\rho_N [q_{N,1}, \dots, \tilde{r}_{N,k}, \dots, q_{N,n}] \\ &\quad - \varphi_N[p_{m_k}^{(k)}]\varphi_N[p_1^{(k)}]\rho_N [q_{N,1}, \dots, \tilde{r}_{N,k}, \dots, q_{N,n}] \\ &\quad - \varphi_N[p_1^{(k)}]\rho_N [q_{N,1}, \dots, (p_{m_k}^{(k)} - \varphi_N[p_{m_k}^{(k)}])\tilde{r}_{N,k}, \dots, q_{N,n}] \\ &\quad - \varphi_N[p_{m_k}^{(k)}]\rho_N [q_{N,1}, \dots, (p_1^{(k)} - \varphi_N[p_1^{(k)}])\tilde{r}_{N,k}, \dots, q_{N,n}] \end{aligned}$$

by linearity of ρ_N in the k -th entry. But then, by induction hypothesis, every element in the right-hand side of the equality above is uniformly bounded with respect to N , and therefore, so is $\rho_N [q_{N,1}, \dots, q_{N,n}]$. □

Having proved Proposition 14 and Corollary 16, we can now show that, under the hypothesis of Theorem 4, the family of random matrix ensembles $\{\{U_{N,i} D_{N,i} U_{N,i}^*\}_{N=1}^\infty\}_{i \in I}$ has the bounded cumulants property.

Proof of Theorem 4 Let \mathcal{A} denote the algebra of non-commutative polynomials $\mathbb{C} \langle x_i \mid i \in I \rangle$, and let $\mathcal{A}_i \subset \mathcal{A}$ denote the algebra $\mathbb{C} [x_i]$ for each index $i \in I$. For each integer $N \geq 1$, take $X_{N,i} = U_{N,i} D_{N,i} U_{N,i}^*$ for every index $i \in I$ and let $\varphi_N : \mathcal{A} \rightarrow \mathbb{C}$ be the unital linear map defined by (4.5). Note that if $p \in \mathcal{A}_j$

for some $j \in I$, then $p(\{X_{N,i}\}_{i \in I}) = U_{N,j}p(D_{N,j})U_{N,j}^*$, and hence, the limit $\lim_{N \rightarrow \infty} \varphi_N[p]$ exists for every $p \in \mathcal{A}_i$ and every $i \in I$. Now, suppose we are given polynomials $p_1 \in \mathcal{A}_{i_1}, p_2 \in \mathcal{A}_{i_2}, \dots, p_m \in \mathcal{A}_{i_m}$ with $i_1, i_2, \dots, i_m \in I$ and $i_1 \neq i_2, i_2 \neq i_3, \dots, i_{m-1} \neq i_m$, and $i_m \neq i_1$. Note that

$$N\varphi_N [(p_1 - \varphi_N [p_1])(p_2 - \varphi_N [p_2]) \cdots (p_m - \varphi_N [p_m])] = \mathbb{E}[\text{Tr}(Y_N)]$$

where

$$Y_N = (U_{N,i_1}A_{N,i_1}U_{N,i_1}^*)(U_{N,i_2}A_{N,i_2}U_{N,i_2}^*) \cdots (U_{N,i_m}A_{N,i_m}U_{N,i_m}^*)$$

and each A_{N,i_j} is of trace zero and given by

$$\begin{aligned} A_{N,i_j} &= U_{N,i_j}^* (p_j(X_{N,i_j}) - \mathbb{E}[\text{tr}(p_j(X_{N,i_j}))])U_{N,i_j} \\ &= p_j(D_{N,i_j}) - \text{tr}(p_j(D_{N,i_j}))I_N. \end{aligned}$$

Thus, by Lemma 3, there is a constant C depending only on the indexes i_j such that

$$|N\varphi_N [(p_1 - \varphi_N [p_1])(p_2 - \varphi_N [p_2]) \cdots (p_m - \varphi_N [p_m])]| \leq C \prod_{j=1}^m \|A_{N,i_j}\|.$$

But then, since $\sup_N \|D_{N,i}\| < \infty$ and $\lim_{N \rightarrow \infty} \text{tr}(D_{N,i}^k)$ exists for every $k \geq 1$ and any $i \in I$, we have $\sup_N \|A_{N,i_j}\| < \infty$, and therefore,

$$\lim_{N \rightarrow \infty} \varphi_N [(p_1 - \varphi_N [p_1])(p_2 - \varphi_N [p_2]) \cdots (p_m - \varphi_N [p_m])] = 0. \tag{4.9}$$

Each linear functional φ_N is tracial, i.e., $\varphi_N[pq] = \varphi_N[qp]$ for all $p, q \in \mathcal{A}$, and thus, following similar arguments to those in the proof of Corollary 16, we can remove the condition $i_m \neq i_1$ and still get (4.9). Therefore, by Proposition 14, the random matrix ensembles $\{U_{N,i}D_{N,i}U_{N,i}^*\}_{N=1}^\infty$ with $i \in I$ are asymptotically free, $\lim_{N \rightarrow \infty} \varphi_N[p]$ exists for every $p \in \mathcal{A}$, and (1.15) holds for $n = 1$.

Fix now an arbitrary integer $n \geq 2$ and let $\rho_N : \mathcal{A} \times \cdots \times \mathcal{A} \rightarrow \mathbb{C}$ be the n -linear map given by (4.6) for every integer $N \geq 1$. Note that

$$\rho_N(p_1, p_2, \dots, p_n) = \mathfrak{c}_n [\text{Tr}(p_1(D_{N,i_1})), \dots, \text{Tr}(p_n(D_{N,i_n}))] = 0$$

if $p_1 \in \mathcal{A}_{i_1}, p_2 \in \mathcal{A}_{i_2}, \dots, p_n \in \mathcal{A}_{i_n}$ for some $i_1, i_2, \dots, i_n \in I$. Thus, since n is arbitrary, the family of ensembles $\{\{U_{N,i}D_{N,i}U_{N,i}^*\}_{N=1}^\infty\}_{i \in I}$ has the bounded cumulants property if the multi-linear functional ρ_N satisfies (3') from Corollary 16, namely

$$\sup_N |\rho_N [q_{N,1}, q_{N,2}, \dots, q_{N,n}]| < \infty$$

whenever each $q_{N,k}$ is of the form

$$q_{N,k} = (p_1^{(k)} - \varphi_N[p_1^{(k)}])(p_2^{(k)} - \varphi_N[p_2^{(k)}]) \cdots (p_{m_k}^{(k)} - \varphi_N[p_{m_k}^{(k)}])$$

with $p_j^{(k)} \in \mathcal{A}_{i_j^{(k)}}$ and $i_1^{(k)} \neq i_2^{(k)}, i_2^{(k)} \neq i_3^{(k)}, \dots, i_{m_k-1}^{(k)} \neq i_{m_k}^{(k)}$, and $i_{m_k}^{(k)} \neq i_1^{(k)}$. Suppose $i_j^{(k)}, p_j^{(k)}$, and $q_{N,k}$ are as above and take $Y_{N,k} = q_{N,k} (\{X_{N,i}\}_{i \in I})$ for $k = 1, 2, \dots, n$. Then, we have

$$\rho_N [q_{N,1}, q_{N,2}, \dots, q_{N,n}] = c_n [\text{Tr}(Y_{N,1}), \text{Tr}(Y_{N,2}), \dots, \text{Tr}(Y_{N,n})].$$

Moreover, letting $A_{N,i_j^{(k)}} = p_j^{(k)}(D_{N,i_j^{(k)}}) - \text{tr}(p_j^{(k)}(D_{N,i_j^{(k)}}))I_N$ for each $i_j^{(k)}$ and every $N \geq 1$, we get $A_{N,i_j^{(k)}}$ is of trace zero, $\sup_N \|A_{N,i_j^{(k)}}\| < \infty$, and

$$Y_{N,k} = (U_{N,i_1^{(k)}} A_{N,i_1^{(k)}} U_{N,i_1^{(k)}}^*) (U_{N,i_2^{(k)}} A_{N,i_2^{(k)}} U_{N,i_2^{(k)}}^*) \cdots (U_{N,i_{m_k}^{(k)}} A_{N,i_{m_k}^{(k)}} U_{N,i_{m_k}^{(k)}}^*).$$

Therefore, by Lemma 3, there is a constant C depending only on the indexes $i_j^{(k)}$ such that

$$|\rho_N [q_{N,1}, q_{N,2}, \dots, q_{N,n}]| \leq C \prod_{k=1}^n \prod_{j=1}^{m_k} \|A_{N,i_j^{(k)}}\| < \infty.$$

□

5 Fluctuation Moments

The proofs of Theorems 1 and 2 are very similar, and thus, in order to avoid redundancies, this section is devoted to prove only Theorem 1; nonetheless, what has to be modified to obtain the conclusions from Theorem 2 is pointed out in the next section.

Let $X_{N,1}$ and $X_{N,2}$ be as in Theorem 1. Assume $Y_N = Y_{N,1} Y_{N,2} \cdots Y_{N,2m_1}$ and $Z_N = Z_{N,1} Z_{N,2} \cdots Z_{N,2m_2}$ where $Y_{N,k}$ and $Z_{N,l}$ are given by (1.5) for some polynomials $p_1, p_2, \dots, p_{2m_1}, q_1, q_2, \dots, q_{2m_2} \in \mathbb{C}[x]$ and some indexes $i_1, i_2, \dots, i_{2m_1}, j_1, j_2, \dots, j_{2m_2} \in \{1, 2\}$ satisfying $i_1 = j_1$ and (1.6). Note that

$$Y_N = (U_{N,i_1} A_{N,1} U_{N,i_1}^*) (U_{N,i_2} A_{N,2} U_{N,i_2}^*) \cdots (U_{N,i_{2m_1}} A_{N,2m_1} U_{N,i_{2m_1}}^*)$$

and

$$Z_N = (U_{N,j_1} B_{N,1} U_{N,j_1}^*) (U_{N,j_2} B_{N,2} U_{N,j_2}^*) \cdots (U_{N,j_{2m_2}} B_{N,2m_2} U_{N,j_{2m_2}}^*)$$

with $A_{N,k}$ and $B_{N,l}$ defined as in (1.11); moreover, we have $i_{2k-1} = j_{2l-1} = i_1 \neq i_2 = i_{2k} = j_{2l}$. Thus, following similar arguments to those in the proof of Lemma 3,

we obtain

$$\text{Cov} [\text{Tr}(Y_N), \text{Tr}(Z_N)] = \sum_{\theta \in P_\chi(\pm 2m)} \left(\sum_{\substack{\pi \in P_{\text{even}}(\pm 2m) \\ \pi \leq \theta}} c_2[\pi] \mu(\pi, \theta) \right) \sum_{\substack{\mathbf{j}: [\pm 2m] \rightarrow [N] \\ \ker(\mathbf{j}) \geq \theta}} \mathbf{a}(\mathbf{j}) \tag{5.1}$$

where $P_\chi(\pm 2m)$ denotes the set of all even partitions of $[\pm 2m]$ with no blocks of the form $\{k, -k\}$, $\mu : P(\pm 2m) \times P(\pm 2m) \rightarrow \mathbb{C}$ is the Möbius inversion function, $\mathbf{a}(\mathbf{j})$ is given by

$$\mathbf{a}(\mathbf{j}) = \prod_{k=1}^{2m_1} A_{N,k}(j_{-k}, j_{+k}) \cdot \prod_{l=1}^{2m_2} B_{N,l}(j_{-2m_2-l}, j_{+2m_2+l}),$$

for function each $\mathbf{j} : [\pm 2m] \rightarrow [N]$, and if $\mathbf{j} : [\pm 2m] \rightarrow [N]$ satisfies $\ker(\mathbf{j}) = \pi$, then

$$c_2[\pi] = \text{cov} \left[\prod_{k=1}^{2m_1} V_k(j_{\sigma(-k)}, j_{\sigma(k)}), \prod_{k=2m_1+1}^{2m_1+2m_2} V_k(j_{\sigma(-k)}, j_{\sigma(k)}) \right] \tag{5.2}$$

with $V_{2k-1} = V_{2k}^* = U_{N,i_1}^* U_{N,i_2}$ for $k = 1, 2, \dots, m$ and $\sigma \in \text{Sym}(\pm 2m)$ is the cyclic permutation given by

$$\sigma = (-1, 1, -2, 2, \dots, -2m_1, 2m_1) \\ (-2m_1 - 1, 2m_1 + 1, \dots, -2m_1 - 2m_2, 2m_1 + 2m_2).$$

It turns out that (5.1) becomes

$$\text{Cov} [\text{Tr}(Y_N), \text{Tr}(Z_N)] = \sum_{\theta \in P_{\chi\chi}(\pm 2m)} \left(\sum_{\substack{\pi \in P_{\text{even}}(\pm 2m) \\ \pi \leq \theta}} c_2[\pi] \mu(\pi, \theta) \right) \sum_{\substack{\mathbf{j}: [\pm 2m] \rightarrow [N] \\ \ker(\mathbf{j}) \geq \theta}} \mathbf{a}(\mathbf{j}) + O(N^{-1}) \tag{5.3}$$

where $P_{\chi\chi}(\pm 2m)$ denotes the set of all partitions $\theta \in P_\chi(\pm 2m)$ such that the graph sum exponent τ_θ , defined in Sect. 3.1, equals m . Indeed, if we are given partitions $\pi \in P_{\text{even}}(\pm 2m)$ and $\theta \in P_\chi(\pm 2m)$ satisfying $\theta \geq \pi$, then Theorem 5 and Proposition 6

imply

$$\left| c_2 [\pi] \mu(\pi, \theta) \sum_{\substack{\mathbf{j}: [\pm 2m] \rightarrow [N] \\ \ker(\mathbf{j}) \geq \theta}} \mathbf{a}(\mathbf{j}) \right| \leq |c_2 [\pi]| |\mu(\pi, \theta)| N^{\tau_\theta} \prod_{k=1}^{2m_1} \|A_{N,k}\| \prod_{l=1}^{2m_2} \|B_{N,l}\| \tag{5.4}$$

where τ_θ is the number of connected components of the graph \mathcal{G}_θ . Now, by hypothesis, $\sup_N \|D_{N,i}\| < \infty$ and $\lim_{N \rightarrow \infty} \text{tr}(D_{N,i}^k)$ exists for every $k \geq 1$ and any $i \in \{1, 2\}$, so we have

$$\sup_N \prod_{k=1}^{2m_1} \|A_{N,k}\| \prod_{l=1}^{2m_2} \|B_{N,l}\| < \infty.$$

Moreover, every connected component of \mathcal{G}_θ contains at least two edges since θ is even and has no blocks of the form $\{-k, k\}$, and hence, the graph sum exponent τ_θ satisfies

$$\tau_\theta \leq m.$$

Additionally, since the unitary ensemble $\{\{U_{N,1}, U_{N,2}\}\}_{N=1}^\infty$ satisfies (II) from Lemma 3, it follows from the proof of Lemma 3 that there is a constant C_2 independent from N satisfying

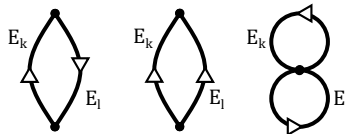
$$|c_2 [\pi]| \leq C_2 N^{-m}.$$

Therefore, from (5.4) we obtain

$$c_2 [\pi] \mu(\pi, \theta) \sum_{\substack{\mathbf{j}: [\pm 2m] \rightarrow [N] \\ \ker(\mathbf{j}) \geq \theta}} \mathbf{a}(\mathbf{j}) = O(N^{-1}) \tag{5.5}$$

unless the graph sum exponent $\tau_\theta = m$, and, consequently, we get (5.3).

Note that the condition $\tau_\theta = m$, for an even partition $\theta \in P(\pm 2m)$ with no blocks of the form $\{+k, -k\}$, forces each component of the undirected graph \mathcal{G}_θ to have exactly two edges. Thus, for any partition $\theta \in P_{\chi\chi}(\pm 2m)$, each component of the directed graph $\vec{\mathcal{G}}_\theta$ has one of the following forms:



And therefore, as illustrated at the end of Sect. 3.1, each graph sum $\sum_{\ker(\mathbf{j}) \geq \theta} \mathbf{a}(\mathbf{j})$ appearing in (5.3) can be written as a product of traces of matrices where each trace is

of the following forms: $\text{Tr}(C_{N,k}C_{N,l})$, $\text{Tr}(C_{N,k}C_{N,l}^T)$, or $\text{Tr}(C_{N,k} \circ C_{N,l})$ where $C_{N,k}$ and $C_{N,l}$ belong to the set $\{A_{N,1}, \dots, A_{N,2m_1}, B_{N,1}, \dots, B_{N,2m_2}\}$. Hence, letting $c[\pi]$ be given by (5.2) for each partition $\pi \in P(\pm 2m)$, the conclusions in Theorem 1 will follow from (5.3) once we determine the order of

$$\sum_{\substack{\pi \in P_{\text{even}}(\pm 2m) \\ \theta \geq \pi}} c_2[\pi] \mu(\pi, \theta). \tag{5.6}$$

Now, recall the values of Möbius inversion function are determined by (2.1), and given explicitly by (2.2). Thus, to determine the order of (5.6), it is enough to compute $c_2[\pi]$ for even partitions $\pi \in P(\pm 2m)$ satisfying $\pi \leq \theta$ for some other partition θ in the set $P_{\chi\chi}(\pm 2m)$.

Proposition 17 *Suppose θ is a partition in $P_{\chi\chi}(\pm 2m)$. If π is an even partition such that $\pi \leq \theta$ and $c_2[\pi]$ is given by (5.2), then the following holds:*

(1) for $U_{N,i_1}^* U_{N,i_2} = \frac{1}{\sqrt{N}} W^* H W$, we have

$$N^m c_2[\pi] = \begin{cases} 1 + O(N^{-1}) & \text{if there is a symmetric pairing partition} \\ & \hat{\theta} \leq \pi \text{ satisfying either (1) or} \\ & \text{(2) from Proposition 13} \\ O(N^{-1/2}) & \text{otherwise.} \end{cases}$$

(2) for $U_{N,i_1}^* U_{N,i_2} = \frac{1}{\sqrt{N}} W^* X H W$, we obtain

$$N^m c_2[\pi] = \begin{cases} 1 + O(N^{-1}) & \text{if there is a symmetric pairing partition} \\ & \hat{\theta} \leq \pi \text{ satisfying (1) from Proposition 13} \\ 1 + O(N^{-1}) & \text{if there is a symmetric pairing partition} \\ & \hat{\theta} \leq \pi \text{ satisfying (2) from Proposition 13 and the} \\ & \text{graph } \mathcal{G}_\pi \text{ has only double loops as components} \\ O(N^{-1/2}) & \text{otherwise.} \end{cases}$$

(3) for $U_{N,i_1}^* U_{N,i_2} = \frac{1}{N} W^* H^* X H W$, we get

$$N^m c_2[\pi] = \begin{cases} 1 + O(N^{-1}) & \text{if } m_1 = m_2 \text{ and there are integers} \\ & 1 \leq k \leq 2m_1 < l \leq 2m_1 + 2m_2 \text{ so} \\ & \text{that } \sigma^t(-k) \sim_\pi \sigma^{-t}(l) \text{ for every integer } t \geq 0 \\ 2 + O(N^{-1}) & \text{if there are integers } 1 \leq k \leq 2m_1 < l \leq 2m_1 + 2m_2 \\ & \text{so that for each integer } t \geq 0 \text{ we have} \\ & \sigma^{-t}(k) \sim_\pi \sigma^{t+1}(k) \text{ and } \sigma^{-t}(l) \sim_\pi \sigma^{t+1}(l) \\ O(N^{-1/2}) & \text{otherwise.} \end{cases}$$

The proof of Proposition 17 is based on the expected value of products of entries from X and W , see relations (2.5) and (2.6), and the results on graph sums of the discrete Fourier transform from Sect. 3.2; however, it requires some technical intermediate

steps, so we will omit it for now and leave it to the end of this section. Nonetheless, the computation of (5.6) up to a term of order $N^{-m-1/2}$ is quite simple assuming that Proposition 17 holds.

Lemma 18 *Suppose θ is a partition in $P_{\chi\chi}(\pm 2m)$ and let $c[\pi]$ be given by (5.2) for each partition $\pi \in P(\pm 2m)$. Then, the following holds:*

(1) for $U_{N,i_1}^* U_{N,i_2} = \frac{1}{\sqrt{N}} W^* H W$, we have

$$\sum_{\substack{\pi \in P_{\text{even}}(\pm 2m) \\ \pi \leq \theta}} N^m c_2[\pi] \mu(\pi, \theta) = \begin{cases} 1 + O(N^{-1/2}) & \text{if } \theta \text{ is a pairing partition satisfying either (1) or} \\ & \text{(2) from Proposition 13,} \\ O(N^{-1/2}) & \text{otherwise} \end{cases}$$

(2) for $U_{N,i_1}^* U_{N,i_2} = \frac{1}{\sqrt{N}} W^* X H W^*$, we obtain

$$\sum_{\substack{\pi \in P_{\text{even}}(\pm 2m) \\ \pi \leq \theta}} N^m c_2[\pi] \mu(\pi, \theta) = \begin{cases} 1 + O(N^{-1/2}) & \text{if } \theta \text{ is a pairing partition satisfying (1) from Pro-} \\ & \text{position 13,} \\ 1 + O(N^{-1/2}) & \text{if there exists a pairing partition } \hat{\theta} \leq \theta \text{ satisfying} \\ & \text{(2) from Proposition 13 and } \theta \text{ has only blocks of} \\ & \text{the form } \{k, -k, l, -l\}, \\ O(N^{-1/2}) & \text{otherwise} \end{cases}$$

(3) for $U_{N,i_1}^* U_{N,i_2} = \frac{1}{N} W^* H^* X H W$, we get

$$\sum_{\substack{\pi \in P_{\text{even}}(\pm 2m) \\ \pi \leq \theta}} N^m c_2[\pi] \mu(\pi, \theta) = \begin{cases} 1 + O(N^{-1/2}) & \text{if } m_1 = m_2 \text{ and there is an integer} \\ & 2m_1 + 1 \leq l \leq 2m_1 + 2m_2 \text{ such that} \\ & \theta = \{\sigma^t(-1), \sigma^{-t-1}(-l)\} \mid t \geq 0\}, \\ 2 + O(N^{-1/2}) & \text{if there are integers } 1 \leq l_1 \leq 2m_1 \text{ and} \\ & 2m_1 + 1 \leq l_2 \leq 2m_1 + 2m_2 \text{ so that } \theta = \theta_1 \sqcup \theta_2 \\ & \text{where } \theta_1 = \{\{\sigma^t(-l_1), \sigma^{-t-1}(-l_1)\} \mid t \geq 0\} \\ & \theta_2 = \{\{\sigma^t(-l_2), \sigma^{-t-1}(-l_2)\} \mid t \geq 0\}, \\ O(N^{-1/2}) & \text{otherwise.} \end{cases}$$

Proof Suppose $U_{N,i_1}^* U_{N,i_2} = W^* X H W / \sqrt{N}$. Propositions 13 and 17 imply that

$$\sum_{\substack{\pi \in P_{\text{Even}}(\pm 2m) \\ \pi \leq \theta}} N^m c_2[\pi] \mu(\pi, \theta) = O(N^{-1/2})$$

unless there are integers $1 \leq k \leq 2m_1 < l \leq 2m_1 + 2m_2$ satisfying one of the following:

- (i) $k + l$ is even and $\sigma^t(-k) \sim_\theta \sigma^{-t}(l)$ for all integers $t \geq 0$ or
- (ii) $k + l$ is odd, $\sigma^t(-k) \sim_\theta \sigma^t(-l)$ for all integers $t \geq 0$ and \mathcal{G}_θ has only double loops as components

Assuming that (i) above holds, consider the pairing partition $\hat{\theta} = \{\{\sigma^t(-k), \sigma^{-t}(l)\} \mid t \geq 0\}$ and note that Proposition 17 implies that

$$\sum_{\substack{\pi \in P_{\text{Even}}(\pm 2m) \\ \pi \leq \theta}} N^m c_2[\pi] \mu(\pi, \theta) = \sum_{\substack{\pi \in P_{\text{Even}}(\pm 2m) \\ \hat{\theta} \leq \pi \leq \theta}} N^m c_2[\pi] \mu(\pi, \theta) + O(N^{-1/2}). \tag{5.7}$$

Moreover, since $N^m c_2[\pi] = 1 + O(N^{-1})$ for any partition π satisfying $\hat{\theta} \leq \pi \leq \theta$, we get

$$\begin{aligned} \sum_{\substack{\pi \in P_{\text{Even}}(\pm 2m) \\ \pi \leq \theta}} N^m c_2[\pi] \mu(\pi, \theta) &= \sum_{\substack{\pi \in P_{\text{Even}}(\pm 2m) \\ \hat{\theta} \leq \pi \leq \theta}} \mu(\pi, \theta) + O(N^{-1/2}) \\ &= \begin{cases} 1 + O(N^{-1/2}) & \text{if } \hat{\theta} = \theta \\ O(N^{-1/2}) & \text{if } \hat{\theta} < \theta \end{cases} \end{aligned}$$

from equations in (2.1) defining the Möbius inversion function. On the other hand, if (ii) above holds, consider $\hat{\theta} = \{\{\sigma^t(-k), \sigma^t(-l)\} \mid t \geq 0\}$ instead and note that (5.7) above holds also in this case. Hence, since $N^m c_2[\theta] = 1 + O(N^{-1})$ and $N^m c_2[\pi] = O(N^{-1/2})$ for any partition $\theta \leq \pi < \theta$, we obtain

$$\begin{aligned} \sum_{\substack{\pi \in P_{\text{Even}}(\pm 2m) \\ \pi \leq \theta}} N^m c_2[\pi] \mu(\pi, \theta) &= N^m c_2[\theta] \mu(\theta, \theta) \\ &+ \sum_{\substack{\pi \in P_{\text{Even}}(\pm 2m) \\ \hat{\theta} \leq \pi < \theta}} N^m c_2[\pi] \mu(\pi, \theta) = 1 + O(N^{-1/2}) \end{aligned}$$

The other cases, namely $U_{N,i_1}^* U_{N,i_2} = W^* H W / \sqrt{N}$ and $U_{N,i_1}^* U_{N,i_2} = W^* H^* X H W / N$, are proved in the same way, one chooses a suitable pairing partition $\hat{\theta}$ such that (5.7) holds, and then the corresponding conclusion follows from Proposition 17 and the equations in (2.1) defining the Möbius function. □

As mentioned earlier, the proof of Theorem 1 is complete once we apply Lemma 18 to the relation (5.3). For instance, suppose $U_{N,i_1}^* U_{N,i_2} = W^* H^* X H W / N$. Then, Theorem 5, Lemma 18, and (5.3) imply that

$$\begin{aligned} \text{Cov} [\text{Tr}(Y_N), \text{Tr}(Z_N)] &= \delta_{m_1, m_2} \sum_{\theta \in \mathcal{P}_1} \sum_{\substack{\mathbf{j}: [\pm 2m] \rightarrow [N] \\ \ker(\mathbf{j}) \geq \theta}} \mathbf{a}(\mathbf{j}) \\ &+ \sum_{\theta \in \mathcal{P}_2} 2 \sum_{\substack{\mathbf{j}: [\pm 2m] \rightarrow [N] \\ \ker(\mathbf{j}) \geq \theta}} \mathbf{a}(\mathbf{j}) + O\left(N^{-\frac{1}{2}}\right) \end{aligned} \tag{5.8}$$

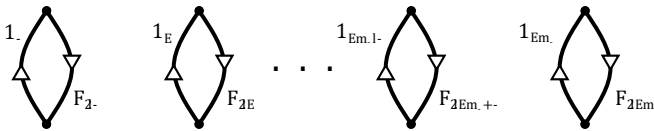
where \mathcal{P}_1 and \mathcal{P}_2 are subsets of $P_{X \times X}(\pm 2m)$ given by

$$\mathcal{P}_1 = \{ \{ \{ \sigma^t(-1), \sigma^{-t-1}(-l) \} \mid t = 0, 1, 2, \dots, 4m \} \mid l \in [2m] \setminus [2m_1] \}$$

and

$$\begin{aligned} \mathcal{P}_2 = \{ \{ \{ \sigma^t(-l_1), \sigma^{-t-1}(-l_1) \}, \{ \sigma^t(-l_2), \sigma^{-t-1}(l_2) \} \mid t \geq 0 \} \mid l_1 \\ \in [2m_1], l_2 \in [2m] \setminus [2m_1] \}. \end{aligned}$$

Now, note the set \mathcal{P}_1 has cardinality $2m_1$ provided $m_1 = m_2$. Moreover, $m_1 = m_2$ implies that a partition $\theta \in P(\pm 2m)$ belongs to the set \mathcal{P}_1 if and only if for some integer $1 \leq l \leq 2m_1$ the directed graph $\vec{\mathcal{G}}_\theta$ can be represented as



where F_k denotes the edge E_{2m_1+k} and $l - k$ is taken module $2m_1$ for $k = 1, 2, \dots, 2m_1$. Thus, for each integer $1 \leq l \leq 2m_1$, there exists a unique $\theta \in \mathcal{P}_1$ so that

$$\sum_{\substack{\mathbf{j}: [\pm m] \rightarrow [N] \\ \ker(\mathbf{j}) \geq \theta}} \mathbf{a}(\mathbf{j}) = \prod_{k=1}^{2m_1} \text{Tr} (A_{N, k} B_{N, l-k}),$$

and hence, we obtain

$$\begin{aligned} \text{Cov} [\text{Tr}(Y_N), \text{Tr}(Z_N)] &= \delta_{m_1, m_2} \sum_{l=1}^{2m_1} \left(\prod_{k=1}^{2m_1} \text{tr} (A_{N, k} B_{N, l-k}) \right) \\ &+ \sum_{\theta \in \mathcal{P}_2} 2 \sum_{\substack{\mathbf{j}: [\pm 2m] \rightarrow [N] \\ \ker(\mathbf{j}) \geq \theta}} \mathbf{a}(\mathbf{j}) + O\left(N^{-\frac{1}{2}}\right). \end{aligned}$$

On the other hand, the set \mathcal{P}_2 has cardinality $m_1 \cdot m_2$ since

$$\{ \{ \sigma^t(-l_1), \sigma^{-t-1}(-l_1) \} \mid t \geq 0 \} = \{ \{ \sigma^t(-m_1 - l_1), \sigma^{-t-1}(-m_1 - l_1) \} \mid t \geq 0 \}$$

and

$$\{ \{ \sigma^t(-l_2), \sigma^{-t-1}(-l_2) \} \mid t \geq 0 \} = \{ \{ \sigma^t(-m_2 - l_2), \sigma^{-t-1}(-m_2 - l_2) \} \mid t \geq 0 \}$$

for $l_1 = 1, 2, \dots, m_1$ and $l_2 = 1, 2, \dots, m_2$. Moreover, a partition $\theta \in P(\pm 2m)$ belongs to the set \mathcal{P}_2 if and only if for some integers $1 \leq l \leq m_1$ and $1 \leq l_2 \leq m_2$ the directed graph $\vec{\mathcal{G}}_\theta$ can be represented as



where $l_1 - k_1$ and $l_2 - k_2$ are taken modulo $2m_1$ and $2m_2$, respectively, for $k_1 = 1, 2, \dots, m_1$ and $k_2 = 1, 2, \dots, m_2$. Thus, for each partition $\theta \in \mathcal{P}_2$ there are integers $1 \leq l_1 \leq m_1$ and $1 \leq l_2 \leq m_2$ satisfying

$$\sum_{\substack{j: \{\pm m\} \rightarrow [N] \\ \ker(j) \geq \theta}} \mathbf{a}(j) = \prod_{k_1=1}^{m_1} \text{Tr}(A_{N, l_1+k_1-1} A_{N, l_1-k_1}) \cdot \prod_{k_2=1}^{m_2} \text{Tr}(B_{N, l_2+k_2-1} B_{N, l_2-k_2}).$$

Therefore, we have

$$\begin{aligned} \text{Cov} [\text{Tr}(Y_N), \text{Tr}(Z_N)] &= 2 \sum_{l_1=1}^{m_1} \sum_{l_2=1}^{m_2} \prod_{k_1=1}^{m_1} \text{tr}(A_{N, l_1+k_1-1} A_{N, l_1-k_1}) \\ &\quad \prod_{k_2=1}^{m_2} \text{tr}(B_{N, l_2+k_2-1} B_{N, l_2-k_2}) \\ &\quad + \delta_{m_1, m_2} \sum_{l=1}^{2m_1} \left(\prod_{k=1}^{2m_1} \text{tr}(A_{N, k} B_{N, l-k}) \right) + O(N^{-1/2}). \end{aligned}$$

The other cases, namely $U_{N, i_1}^* U_{N, i_2} = W^* H W / \sqrt{N}$ and $U_{N, i_1}^* U_{N, i_2} = W^* X H W / N$, are proved in the same way, applying Lemma 18 to the relation (5.3) we obtain similar relations to that in (5.8) that lead to (1) and (2) in Theorem 1.

The remaining of this section is devoted to the proof of Proposition 17. For clarity, we have considered two cases: $U_{N, i_1}^* U_{N, i_2} = W^* H^* X H W / N$ and $U_{N, i_1}^* U_{N, i_2} = W^* Y H W / \sqrt{N}$ where Y is either the identity matrix I_N or an N -by- N uniformly distributed signature matrix X . But first, let us introduce some more notation for partitions.

Given a partition $\pi \in P(\pm 2m)$, we let π_{even} and π_{odd} denote the restriction of π to the sets $\{k \in [\pm 2m] \mid k \text{ is even}\}$ and $\{k \in [\pm 2m] \mid k \text{ is odd}\}$, respectively. Moreover, we let π^{even} and π^{odd} denote the partitions of $\{k \in [\pm 4m] \mid k \text{ is even}\}$ and $\{k \in [\pm 4m] \mid k \text{ is odd}\}$, respectively, given by $\pi^{\text{even}} = \{2k \mid k \in B\} \mid B \in \pi$

and $\pi^{\text{odd}} = \{\{2k - \text{sign}(k) \mid k \in B\} \mid B \in \pi\}$ where $\text{sign}(k) = 1$, if k is positive, and $\text{sign}(k) = -1$, otherwise. For instance, if π is the partition in $P(\pm 6)$ given by

$$\pi = \{\{-1, 4\}, \{1, -3\}, \{-2, 3\}, \{2, -4\}\}$$

then

$$\begin{aligned} \pi_{\text{even}} &= \{\{4\}, \{-2\}, \{2, -4\}\}, & \pi_{\text{odd}} &= \{\{-1\}, \{1, -3\}, \{3\}\}, \\ \pi^{\text{even}} &= \{\{-2, 8\}, \{2, -6\}, \{-4, 6\}, \{4, -8\}\}, & \text{and} & \\ \pi^{\text{odd}} &= \{\{-1, 7\}, \{1, -5\}, \{-3, 5\}, \{3, -7\}\}. \end{aligned}$$

Case $U_{N,i_1}^* U_{N,i_2} = \frac{1}{\sqrt{N}} W^* Y H W$

Let Y be an N -by- N diagonal random matrix independent from W . Given a function $\mathbf{i} : [\pm 2m] \rightarrow [N]$, we let

$$\mathbf{h}(\mathbf{i}) = \mathbf{h}_1(\mathbf{i})\mathbf{h}_2(\mathbf{i}) \quad \text{and} \quad \mathbf{y}(\mathbf{i}) = \mathbf{y}_1(\mathbf{i})\mathbf{y}_2(\mathbf{i})$$

where $\mathbf{h}_1(\mathbf{i})$, $\mathbf{h}_2(\mathbf{i})$, $\mathbf{y}_1(\mathbf{i})$, and $\mathbf{y}_2(\mathbf{i})$ are given by

$$\begin{aligned} \mathbf{h}_1(\mathbf{i}) &= \prod_{k=1}^{m_1} H(i_{-2k+1}, i_{2k-1})H^*(i_{-2k}, i_{2k}), \\ \mathbf{h}_2(\mathbf{i}) &= \prod_{k=m_1+1}^{m_1+m_2} H(i_{-2k+1}, i_{2k-1})H^*(i_{-2k}, i_{2k}), \\ \mathbf{y}_1(\mathbf{i}) &= \prod_{k=1}^{m_1} Y(i_{-2k+1}, i_{-2k+1})Y(i_{2k-1}, i_{2k-1}), \\ \mathbf{y}_2(\mathbf{i}) &= \prod_{k=m_1+1}^{m_1+m_2} Y(i_{-2k+1}, i_{-2k+1})Y(i_{2k-1}, i_{2k-1}); \end{aligned}$$

additionally, if we are given a function $\mathbf{j} : [\pm 2m] \rightarrow [N]$, we put

$$\mathbf{w}(\mathbf{i}, \mathbf{j}) = \mathbf{w}_1(\mathbf{i}, \mathbf{j})\mathbf{w}_2(\mathbf{i}, \mathbf{j})$$

where $\mathbf{w}_1(\mathbf{i}, \mathbf{j})$ and $\mathbf{w}_2(\mathbf{i}, \mathbf{j})$ are given by

$$\begin{aligned} \mathbf{w}_1(\mathbf{i}, \mathbf{j}) &= \prod_{k=1}^{2m_1} W(i_k, j_k)W(i_{-k}, j_{-k}) \\ \text{and} \quad \mathbf{w}_2(\mathbf{i}, \mathbf{j}) &= \prod_{k=2m_1+1}^{2m_1+2m_2} W(i_k, j_k)W(i_{-k}, j_{-k}). \end{aligned}$$

Now, for every partition $\pi \in P(\pm 2m)$ and any function $\mathbf{j} : [\pm 2m] \rightarrow [N]$ satisfying $\ker(\mathbf{j}) = \pi$, we define $\mathfrak{C}_2[\pi]$ by

$$\begin{aligned} & \sum_{\substack{\mathbf{i}:[\pm 2m] \rightarrow [N] \\ \ker(\mathbf{i})=\pi}} \mathbf{h}(\mathbf{i} \circ \sigma) \mathbb{E}[\mathbf{w}(\mathbf{i}, \mathbf{j})] \mathbb{E}[\mathbf{y}(\mathbf{i})] \\ & - \sum_{\substack{\mathbf{i}:[\pm 2m] \rightarrow [N] \\ \ker(\mathbf{i})=\pi_1 \sqcup \pi_2}} \mathbf{h}(\mathbf{i} \circ \sigma) \mathbb{E}[\mathbf{w}_1(\mathbf{i}, \mathbf{j})] \mathbb{E}[\mathbf{w}_2(\mathbf{i}, \mathbf{j})] \mathbb{E}[\mathbf{y}_1(\mathbf{i})] \mathbb{E}[\mathbf{y}_2(\mathbf{i})] \\ & = \mathfrak{C}_2[\pi] \end{aligned} \tag{5.9}$$

where π_1 and π_2 denote the restrictions of π to $[\pm 2m_1]$ and $[\pm 2m] \setminus [\pm 2m_1]$, respectively, and $\sigma \in \text{Sym}(\pm 2m)$ is the cycle permutation given by

$$\begin{aligned} \sigma = & (-1, 1, -2, 2, \dots, -2m_1, 2m_1) \\ & (-2m_1 - 1, 2m_1 + 1, \dots, -2m_1 - 2m_2, 2m_1 + 2m_2). \end{aligned}$$

Proposition 19 *Let π be an even partition in $P(\pm 2m)$. Suppose $U_{N,i_1}^* U_{N,i_2} = W^* Y H W / \sqrt{N}$ where Y is an N -by- N diagonal matrix independent from W so that each entry $Y(i, i)$ takes values in the set $\{-1, 1\}$. If $\mathfrak{c}_2[\pi]$ and $\mathfrak{C}_2[\pi]$ are given by (5.2) and (5.9), respectively, then*

$$N^m \mathfrak{c}_2[\pi] = \mathfrak{C}_2[\pi] + O(N^{-1}) \tag{5.10}$$

Proof Fix a function $\mathbf{j} : [\pm 2m] \rightarrow [N]$ satisfying $\ker(\mathbf{j}) = \pi$. Note that the (j_{-2k+1}, j_{2k-1}) -entry of $U_{N,i_1}^* U_{N,i_2}$ and the (j_{-2k}, j_{2k}) -entry of $U_{N,i_2}^* U_{N,i_1}$ are given by

$$\sum_{i_{-2k+1}, i_{2k+1}=1}^N \frac{1}{\sqrt{N}} W^*(j_{-2k+1}, i_{-2k+1}) Y(i_{-2k+1}, i_{-2k+1}) H(i_{-2k+1}, i_{2k-1}) W(i_{2k-1}, j_{2k-1})$$

and

$$\begin{aligned} & \sum_{i_{-2k}, i_{2k}=1}^N \frac{1}{\sqrt{N}} W^*(j_{-2k}, i_{-2k}) \\ & H^*(i_{-2k}, i_{2k}) Y(i_{2k}, i_{2k}) W(i_{2k}, j_{2k}), \end{aligned}$$

respectively. Thus, from (5.2) and the linearity of the covariance, we have that

$$N^m \mathfrak{c}_2[\pi] = \sum_{\mathbf{i}:[\pm 2m] \rightarrow [N]} \mathbf{h}(\mathbf{i}) \cdot \text{cov}[\mathbf{w}_1(\mathbf{i}, \mathbf{j} \circ \sigma) \cdot \mathbf{y}_1(\mathbf{i}), \mathbf{w}_2(\mathbf{i}, \mathbf{j} \circ \sigma) \cdot \mathbf{y}_2(\mathbf{i})]$$

where $\mathbf{h}(\mathbf{i})$, $\mathbf{w}_1(\mathbf{i}, \mathbf{j})$, $\mathbf{w}_2(\mathbf{i}, \mathbf{j})$, $\mathbf{y}_1(\mathbf{i})$, $\mathbf{y}_2(\mathbf{i})$, and σ are defined as above. But, for every function $\mathbf{i} : [\pm 2m] \rightarrow [N]$, we have that

$$\mathbf{w}_k(\mathbf{i}, \mathbf{j}) = \mathbf{w}_k(\mathbf{i} \circ \sigma, \mathbf{j} \circ \sigma) \quad \text{and} \quad \mathbf{y}_k(\mathbf{i}) = \mathbf{y}_k(\mathbf{i} \circ \sigma) \quad \text{for } k = 1, 2,$$

so we obtain

$$N^m c_2[\pi] = \sum_{\mathbf{i} : [\pm 2m] \rightarrow [N]} \mathbf{h}(\mathbf{i} \circ \sigma) \cdot \text{cov}[\mathbf{w}_1(\mathbf{i}, \mathbf{j}) \cdot \mathbf{y}_1(\mathbf{i}), \mathbf{w}_2(\mathbf{i}, \mathbf{j}) \cdot \mathbf{y}_2(\mathbf{i})]. \quad (5.11)$$

Moreover, from (2.6) we get that

$$\mathbb{E}[\mathbf{w}_1(\mathbf{i}, \mathbf{j})\mathbf{w}_2(\mathbf{i}, \mathbf{j})] = 0 \quad \text{and} \quad \mathbb{E}[\mathbf{w}_1(\mathbf{i}, \mathbf{j})] \mathbb{E}[\mathbf{w}_2(\mathbf{i}, \mathbf{j})] = 0$$

provided $\ker(\mathbf{i}) \neq \pi$ and $\ker(\mathbf{i}) \not\geq \pi_1 \sqcup \pi_2$, respectively. And hence, equality in (5.11) becomes

$$\begin{aligned} N^m c_2[\pi] &= \sum_{\substack{\mathbf{i} : [\pm 2m] \rightarrow [N] \\ \ker(\mathbf{i}) = \pi}} \mathbf{h}(\mathbf{i} \circ \sigma) \mathbb{E}[\mathbf{w}_1(\mathbf{i}, \mathbf{j})\mathbf{w}_2(\mathbf{i}, \mathbf{j})] \mathbb{E}[\mathbf{y}_1(\mathbf{i})\mathbf{y}_2(\mathbf{i})] \\ &\quad - \sum_{\substack{\theta \in P(\pm 2m) \\ \theta \geq \pi_1 \sqcup \pi_2}} \sum_{\substack{\mathbf{i} : [\pm 2m] \rightarrow [N] \\ \ker(\mathbf{i}) = \theta}} \mathbf{h}(\mathbf{i} \circ \sigma) \mathbb{E}[\mathbf{w}_1(\mathbf{i}, \mathbf{j})] \mathbb{E}[\mathbf{w}_2(\mathbf{i}, \mathbf{j})] \\ &\quad \mathbb{E}[\mathbf{y}_1(\mathbf{i})] \mathbb{E}[\mathbf{y}_2(\mathbf{i})]. \end{aligned}$$

To obtain (5.10), it only remains to show that for $\theta \geq \pi_1 \sqcup \pi_2$, i.e., $\theta \geq \pi_1 \sqcup \pi_2$ but $\theta \neq \pi_1 \sqcup \pi_2$, implies

$$\sum_{\substack{\mathbf{i} : [\pm 2m] \rightarrow [N] \\ \ker(\mathbf{i}) = \theta}} \mathbf{h}(\mathbf{i} \circ \sigma) \mathbb{E}[\mathbf{w}_1(\mathbf{i}, \mathbf{j})] \mathbb{E}[\mathbf{w}_2(\mathbf{i}, \mathbf{j})] \mathbb{E}[\mathbf{y}_1(\mathbf{i})] \mathbb{E}[\mathbf{y}_2(\mathbf{i})] = O(N^{-1}).$$

Suppose $\theta \in P(\pm 2m)$ satisfies $\theta \geq \pi_1 \sqcup \pi_2$. Then, we must have $\#(\theta) < \#(\pi_1 \sqcup \pi_2) = \#(\pi_1) + \#(\pi_2)$, or, equivalently,

$$\#(\theta) - \#(\pi_1) - \#(\pi_2) \leq -1.$$

Now, $\mathbf{h}(\mathbf{i} \circ \sigma)$ has absolute value 1 for any function $\mathbf{i} : [\pm 2m] \rightarrow [N]$ and $|\mathbb{E}[\mathbf{y}_1(\mathbf{i})] \mathbb{E}[\mathbf{y}_2(\mathbf{i})]| \leq 1$, so (2.6) implies

$$\left| \sum_{\substack{\mathbf{i} : [\pm 2m] \rightarrow [N] \\ \ker(\mathbf{i}) = \theta}} \mathbf{h}(\mathbf{i} \circ \sigma) \mathbb{E}[\mathbf{w}_1(\mathbf{i}, \mathbf{j})] \mathbb{E}[\mathbf{w}_2(\mathbf{i}, \mathbf{j})] \mathbb{E}[\mathbf{y}_1(\mathbf{i})] \mathbb{E}[\mathbf{y}_2(\mathbf{i})] \right|$$

$$\begin{aligned} &\leq \frac{(N - \#(\pi_1))!}{N!} \cdot \frac{(N - \#(\pi_2))!}{N!} \cdot \left| \sum_{\substack{\mathbf{i}: [\pm 2m] \rightarrow [N] \\ \ker(\mathbf{i}) = \theta}} \mathbf{h}(\mathbf{i} \circ \sigma) \right| \\ &= O\left(N^{-\#(\pi_1) - \#(\pi_2) + \#(\theta)}\right) = O\left(N^{-1}\right). \end{aligned}$$

□

Proof of (1) from Proposition 17 Let Y be the identity matrix I_N . By Proposition 19, we only need to show that

$$\mathfrak{C}_2[\pi] = \begin{cases} 1 + O(N^{-1}) & \text{if there is a symmetric pairing partition} \\ & \hat{\theta} \leq \pi \text{ satisfying either (1) or (2)} \\ & \text{from Proposition 13,} \\ O(N^{-1/2}) & \text{otherwise.} \end{cases}$$

where $\mathfrak{C}_2[\pi]$ is given by (5.9). Note that from (2.6) and (5.9) we obtain the inequality

$$\begin{aligned} |\mathfrak{C}_2[\pi]| &\leq \frac{(N - \#(\pi))!}{N!} \left| \sum_{\substack{\mathbf{i}: [\pm 2m] \rightarrow [N] \\ \ker(\mathbf{i}) = \pi}} \mathbf{h}(\mathbf{i} \circ \sigma) \right| \\ &\quad + \frac{(N - \#(\pi_1))!}{N!} \frac{(N - \#(\pi_2))!}{N!} \left| \sum_{\substack{\mathbf{i}: [\pm 2m] \rightarrow [N] \\ \ker(\mathbf{i}) = \pi_1 \sqcup \pi_2}} \mathbf{h}(\mathbf{i} \circ \sigma) \right|. \end{aligned}$$

But then, if $p_{\sigma^{-1} \circ \pi}$ is a nonzero polynomial, so is $p_{\sigma^{-1} \circ \pi_1 \sqcup \pi_2}$ by Proposition 10, and therefore, the last inequality and Corollary 8 would imply $\mathfrak{C}_2[\pi] = O(N^{-1/2})$. And so, we can assume $p_{\sigma^{-1} \circ \pi}$ is the zero polynomial without loss of generality.

Now, for every function $\mathbf{i} : [\pm 2m] \rightarrow [N]$ satisfying $\ker(\mathbf{i}) = \pi$ we have $\mathbf{h}(\mathbf{i} \circ \sigma) = 1$ since $p_{\sigma^{-1} \circ \pi}$ is the zero polynomial; additionally, (2.6) gives $\mathbb{E}[\mathbf{w}(\mathbf{i}, \mathbf{j})] = \frac{(N - \#(\pi))!}{N!}$ since π is an even partition. Thus, from (5.9) we obtain

$$\mathfrak{C}_2[\pi] = 1 - \sum_{\substack{\mathbf{i}: [\pm 2m] \rightarrow [N] \\ \ker(\mathbf{i}) = \pi_1 \sqcup \pi_2}} \mathbf{h}(\mathbf{i} \circ \sigma) \mathbb{E}[\mathbf{w}_1(\mathbf{i}, \mathbf{j})] \mathbb{E}[\mathbf{w}_2(\mathbf{i}, \mathbf{j})]. \tag{5.12}$$

Moreover, by Proposition 10, there is a symmetric pairing partition $\hat{\theta} \leq \pi$ such that $p_{\sigma^{-1} \circ \hat{\theta}}$ is also the zero polynomial, and hence, the partition $\hat{\theta}$ must satisfy one of the conditions (1)-(6) from Proposition 13. Notice $\hat{\theta} = \hat{\theta}_1 \sqcup \hat{\theta}_2$, where $\hat{\theta}_1$ and $\hat{\theta}_2$ denote the restrictions of $\hat{\theta}$ to $[\pm 2m_1]$ and $[\pm 2m] \setminus [\pm 2m_1]$, respectively, implies

$$\mathfrak{C}_2[\pi] = 1 - \frac{(N - \#(\pi_1))!}{N!} \cdot \frac{(N - \#(\pi_2))!}{N!} \cdot \frac{N!}{(N - \#(\pi_1 \sqcup \pi_2))!} = O\left(N^{-1}\right). \tag{5.13}$$

Indeed, if $\hat{\theta} = \hat{\theta}_1 \sqcup \hat{\theta}_2$, then $\hat{\theta}_1$ and $\hat{\theta}_2$ must be even partitions, and so are π_1 and π_2 since $\hat{\theta} \leq \pi$ implies $\hat{\theta}_1 \leq \pi_1$ and $\hat{\theta}_2 \leq \pi_2$, so (2.6) gives

$$\mathbb{E}[\mathbf{w}_1(\mathbf{i}, \mathbf{j})] = \frac{(N - \#(\pi_1))!}{N!} \quad \text{and} \quad \mathbb{E}[\mathbf{w}_2(\mathbf{i}, \mathbf{j})] = \frac{(N - \#(\pi_2))!}{N!}$$

for every function $\mathbf{i} : [\pm 2m] \rightarrow [N]$ satisfying $\ker(\mathbf{i}) = \pi_1 \sqcup \pi_2$; moreover, Proposition 10 implies the polynomial $p_{\sigma^{-1} \circ \pi_1 \sqcup \pi_2}$ is also zero since $\hat{\theta} = \hat{\theta}_1 \sqcup \hat{\theta}_2 \leq \pi_1 \sqcup \pi_2$, and thus, we obtain

$$\mathbf{h}(\mathbf{i} \circ \sigma) = 1.$$

Hence, (5.13) follows from (5.12) provided $\hat{\theta}$ satisfies either (3), (4), (5), or (6) from Proposition 13.

Assume now $\hat{\theta}$ satisfies either (1) or (2) from Proposition 13. Then, either $\pi_1 \sqcup \pi_2$ contains some singletons, if $\{k, l\} \in \pi$ or $\{k, -l\} \in \pi$ for some integers $1 \leq k \leq 2m_1 < l \leq 2m_1 + 2m_2$, or $\pi_1 \sqcup \pi_2 = \{\{-k, k\} \mid k \in [\pm 2m]\}$, otherwise. In any case, the graph $\hat{\mathcal{G}}_{\pi_1 \sqcup \pi_2}$ satisfies none of the conditions (1)–(6) from Remark 12 since $m_1 + m_2 > 2$, and hence, the polynomial $p_{\sigma^{-1} \circ \pi_1 \sqcup \pi_2}$ is nonzero. Thus, by (2.6) and Corollary 8, we have

$$\left| \sum_{\substack{\mathbf{i}: [\pm 2m] \rightarrow [N] \\ \ker(\mathbf{i}) = \pi_1 \sqcup \pi_2}} \mathbf{h}(\mathbf{i} \circ \sigma) \mathbb{E}[\mathbf{w}_1(\mathbf{i}, \mathbf{j})] \mathbb{E}[\mathbf{w}_2(\mathbf{i}, \mathbf{j})] \right| \leq CN^{\#(\pi_1 \sqcup \pi_2) - \frac{1}{2}} \cdot \frac{(N - \#(\pi_1))!}{N!} \cdot \frac{(N - \#(\pi_2))!}{N!} \tag{5.14}$$

for some constant $C > 0$ independent from N . Therefore, from (5.12) we get that

$$\mathfrak{C}_2[\pi] = 1 + O(N^{-1/2}).$$

□

Proof of (2) from Proposition 17 Let Y be a random N -by- N signature matrix independent from W . Similar to the previous case, $U_{N,i_1}^* U_{N,i_2} = W^* H W / \sqrt{N}$, we can assume $p_{\sigma^{-1} \circ \pi}$ is the zero polynomial and it suffices to show that

$$\mathfrak{C}_2[\pi] = \begin{cases} 1 + O(N^{-1}) & \text{if there is a symmetric pairing partition} \\ & \hat{\theta} \leq \pi \text{ satisfying (1) from Proposition 13,} \\ 1 + O(N^{-1}) & \text{if there is a symmetric pairing partition } \hat{\theta} \leq \pi \\ & \text{satisfying (2) from Proposition 13 and the graph} \\ & \mathcal{G}_\pi \text{ has only double loops as components,} \\ O(N^{-1/2}) & \text{otherwise.} \end{cases}$$

Let $\pi_{\text{odd},1}$ and $\pi_{\text{odd},2}$ denote the restrictions of π_{odd} to $[\pm 2m_1]$ and $[\pm 2m] \setminus [\pm 2m_1]$, respectively. Note that if π_{odd} is not an even partition, then either $\pi_{\text{odd},1}$ or $\pi_{\text{odd},2}$ is not

even, and hence, we obtain $\mathfrak{C}_2[\pi] = 0$ since (2.5) would imply $\mathbb{E} [y_1(\mathbf{i})] \mathbb{E} [y_2(\mathbf{i})] = \mathbb{E} [y(\mathbf{i})] = 0$ for every function $\mathbf{i} : [\pm 2m] \rightarrow [N]$ satisfying $\ker(\mathbf{i}) = \pi$. Thus, we can further assume π_{odd} is even. It then follows from (2.5) and (2.6) that

$$\mathbf{h}(\mathbf{i} \circ \sigma) = 1, \quad \mathbb{E} [y(\mathbf{i})] = 1 \quad \text{and} \quad \mathbb{E} [\mathbf{w}(\mathbf{i}, \mathbf{j})] = \frac{(N - \#(\pi))!}{N!}$$

for $\mathbf{i} : [\pm 2m] \rightarrow [N]$ satisfying $\ker(\mathbf{i}) = \pi$, and hence, we obtain

$$\mathfrak{C}_2[\pi] = 1 - \sum_{\substack{\mathbf{i} : [\pm 2m] \rightarrow [N] \\ \ker(\mathbf{i}) = \pi_1 \sqcup \pi_2}} \mathbf{h}(\mathbf{i} \circ \sigma) \mathbb{E} [y_1(\mathbf{i})] \mathbb{E} [y_2(\mathbf{i})] \mathbb{E} [\mathbf{w}_1(\mathbf{i}, \mathbf{j})] \mathbb{E} [\mathbf{w}_2(\mathbf{i}, \mathbf{j})]. \tag{5.15}$$

By Proposition 10, there is a symmetric pairing partition $\hat{\theta} \leq \pi$ such that $p_{\sigma^{-1} \circ \hat{\theta}}$ is also the zero polynomial, and thus, the partition $\hat{\theta}$ must satisfy one of the conditions (1)-(6) from Proposition 13. However, if $\hat{\theta}$ satisfies either (3), (4), (5), or (6), then

$$\mathfrak{C}_2[\pi] = 1 - \frac{N!}{(N - \#(\pi_1 \sqcup \pi_2))!} \cdot \frac{(N - \#(\pi_1))!}{N!} \cdot \frac{(N - \#(\pi_2))!}{N!} = O(N^{-1}). \tag{5.16}$$

Indeed, suppose $\hat{\theta}$ satisfies either (3), (4), (5), or (6) from Proposition 13, let $\hat{\theta}_1$ and $\hat{\theta}_2$ denote the restrictions of $\hat{\theta}$ to $[\pm 2m_1]$ and $[\pm 2m] \setminus [\pm 2m_1]$, respectively, and let $\mathbf{i} : [\pm 2m] \rightarrow [N]$ be a function satisfying $\ker(\mathbf{i}) = \pi_1 \sqcup \pi_2$. Note that $\hat{\theta} = \hat{\theta}_1 \sqcup \hat{\theta}_2 \leq \pi_1 \sqcup \pi_2$ since $\hat{\theta} \leq \pi$ implies $\hat{\theta}_1 \leq \pi_1$ and $\hat{\theta}_2 \leq \pi_2$, and thus, by Proposition 10, the polynomial $p_{\sigma^{-1} \circ \pi_1 \sqcup \pi_2}$ is zero, and hence, we get

$$\mathbf{h}(\mathbf{i} \circ \sigma) = 1.$$

Moreover, π_1 and π_2 are even partitions since $\hat{\theta}$ is even and $\hat{\theta} = \hat{\theta}_1 \sqcup \hat{\theta}_2 \leq \pi$, so, from (2.6), we get

$$\mathbb{E} [\mathbf{w}_1(\mathbf{i}, \mathbf{j})] = \frac{(N - \#(\pi_1))!}{N!} \quad \text{and} \quad \mathbb{E} [\mathbf{w}_2(\mathbf{i}, \mathbf{j})] = \frac{(N - \#(\pi_2))!}{N!}.$$

The partitions $\pi_{\text{odd},1}$ and $\pi_{\text{odd},2}$ are also even since $\hat{\theta}_{\text{odd}}$ is even and $\hat{\theta} = \hat{\theta}_1 \sqcup \hat{\theta}_2 \leq \pi$ implies $\hat{\theta}_{\text{odd}} = \hat{\theta}_{\text{odd},1} \sqcup \hat{\theta}_{\text{odd},2}$, $\hat{\theta}_{\text{odd},1} \leq \pi_{\text{odd},1}$, and $\hat{\theta}_{\text{odd},2} \leq \pi_{\text{odd},2}$ where $\hat{\theta}_{\text{odd},1}$ and $\hat{\theta}_{\text{odd},2}$ denote the restrictions of $\hat{\theta}_{\text{odd}}$ to $[\pm 2m_1]$ and $[\pm 2m] \setminus [\pm 2m_1]$, respectively. Thus, from (2.5), we have

$$\mathbb{E} [y_1(\mathbf{i})] \mathbb{E} [y_2(\mathbf{i})] = 1.$$

Consequently, we obtain (5.16) from (5.15). Now, similar to the case $U_{N,i_1}^* U_{N,i_2} = W^* H W / \sqrt{N}$, if $\hat{\theta}$ satisfies either (1) or (2) from Proposition 13, then $p_{\sigma^{-1} \circ \pi_1 \sqcup \pi_2}$ is a

nonzero polynomial and (5.14) holds, so, from (5.15), we obtain

$$\mathfrak{C}_2[\pi] = 1 + O(N^{-1/2})$$

since we have $|\mathbb{E}[\mathbf{y}_1(\mathbf{i})] \mathbb{E}[\mathbf{y}_2(\mathbf{i})] = 1| \leq 1$ for any function $\mathbf{i} : [\pm 2m] \rightarrow [N]$.

It only remains to show that the undirected graph \mathcal{G}_π must have only double loops as connected components if $\hat{\theta}$ satisfies (2) from Proposition 13. So, suppose $\hat{\theta}$ satisfies (2) from Proposition 13. Note that if π has a block of the form $\{k, l\}$, then $k + l$ is odd, and hence, we must have either $\{k\}$ or $\{l\}$ is a block of π_{odd} , contradicting the assumption that π_{odd} is an even partition. Thus, π has only blocks of the form $\{k, l, -k, -l\}$, or, equivalently, the undirected graph \mathcal{G}_π has only double loops as connected components. \square

Case $U_{N,i_1}^* U_{N,i_2} = \frac{1}{N} W^* H^* X H W$

For each function $\mathbf{i} : [\pm 4m] \rightarrow [N]$, we let $\hat{\mathbf{h}}(\mathbf{i})$, $\hat{\mathbf{g}}(\mathbf{i})$, $\hat{\mathbf{x}}_1(\mathbf{i})$, and $\hat{\mathbf{x}}_2(\mathbf{i})$ be given by

$$\begin{aligned} \hat{\mathbf{h}}(\mathbf{i}) &= \prod_{k=1}^{2m} H^*(i_{-2k+1}, i_{2k-1}) H(i_{-2k}, i_{2k}), \\ \hat{\mathbf{g}}(\mathbf{i}) &= \prod_{k=1}^{2m} H^*(i_{-2k+1}, i_{-2k}) H(i_{2k}, i_{2k-1}), \\ \hat{\mathbf{x}}_1(\mathbf{i}) &= \prod_{k=1}^{2m_1} X(i_{-2k}, i_{2k}), \quad \text{and} \\ \hat{\mathbf{x}}_2(\mathbf{i}) &= \prod_{k=2m_1+1}^{2m_1+2m_2} X(i_{-2k}, i_{2k}); \end{aligned}$$

additionally, if we are given a function $\mathbf{j} : [\pm 2m] \rightarrow [N]$, we take

$$\mathbf{t} = (t_{-1}, t_1, t_{-3}, t_3, \dots, t_{4m_1+4m_2-1}) = (j_{-1}, j_1, j_{-2}, j_2, \dots, j_{-2m}, j_{2m}) \quad (5.17)$$

and let $\hat{\mathbf{w}}_1(\mathbf{i}, \mathbf{t})$ and $\hat{\mathbf{w}}_2(\mathbf{i}, \mathbf{t})$, also denoted $\hat{\mathbf{w}}_1(\mathbf{i})$ and $\hat{\mathbf{w}}_2(\mathbf{i})$, respectively, be defined by

$$\begin{aligned} \hat{\mathbf{w}}_1(\mathbf{i}, \mathbf{t}) &= \prod_{k=1}^{2m_1} W(i_{2k-1}, t_{2k-1}) W(i_{-2k+1}, t_{-2k+1}) \quad \text{and} \\ \hat{\mathbf{w}}_2(\mathbf{i}, \mathbf{t}) &= \prod_{k=2m_1+1}^{2m_1+2m_2} W(i_{2k+1}, t_{2k+1}) W(i_{-2k+1}, t_{-2k+1}). \end{aligned}$$

Now, given partitions $\pi \in P(\pm 2m)$ and $\alpha \in P_2(2m)$ and a function $\mathbf{j} : [\pm 2m] \rightarrow [N]$ satisfying $\ker(\mathbf{j}) = \pi$, we define $\mathfrak{C}_2[\pi, \alpha]$ by

$$\begin{aligned} & \sum_{\substack{\mathbf{i}:[\pm 4m] \rightarrow [N] \\ \ker(\mathbf{i}) = \widehat{\alpha} \sqcup \pi^{\text{odd}}} } \widehat{\mathbf{h}}(\mathbf{i} \circ \widehat{\sigma}) \mathbb{E}[\widehat{\mathbf{w}}(\mathbf{i})] \mathbb{E}[\widehat{\mathbf{x}}(\mathbf{i})] \\ & - \sum_{\substack{\mathbf{i}:[\pm 4m] \rightarrow [N] \\ \ker(\mathbf{i}) = \widehat{\alpha} \sqcup \pi_1^{\text{odd}} \sqcup \pi_2^{\text{odd}}} } \widehat{\mathbf{h}}(\mathbf{i} \circ \widehat{\sigma}) \mathbb{E}[\widehat{\mathbf{w}}_1(\mathbf{i})] \mathbb{E}[\widehat{\mathbf{w}}_2(\mathbf{i})] \mathbb{E}[\widehat{\mathbf{x}}_1(\mathbf{i})] \mathbb{E}[\widehat{\mathbf{x}}_2(\mathbf{i})] \\ & = N^m \mathfrak{C}_2[\pi, \alpha] \end{aligned} \tag{5.18}$$

where π_1^{odd} and π_2^{odd} denote the restrictions of π^{odd} to the sets $[\pm 4m_1]$ and $[\pm(4m_1 + 4m_2)] \setminus [\pm 4m_1]$, respectively, $\widehat{\alpha}$ is the partition given by $\widehat{\alpha} = \{-2k, 2k, -2l, 2l \mid \{k, l\} \in \alpha\}$, and $\widehat{\sigma} \in \text{Sym}(\pm 4m)$ is the permutation with cycle decomposition

$$\begin{aligned} \widehat{\sigma} = & (-1, 1, -2, 2, \dots, -4m_1, 4m_1) \\ & (-4m_1 - 1, 4m_1 + 1, -4m_2 - 2, \dots, 4m_1 + 4m_2). \end{aligned}$$

Proposition 20 *Let π be an even partition in $P(\pm 2m)$. Suppose $U_{N,i_1}^* U_{N,i_2} = W^* H^* X H W / N$. If $c_2[\pi]$ is given by (5.2) and $\mathfrak{C}_2[\pi, \alpha]$ is given by (5.18) for every pairing partition $\alpha \in P_2(2m)$, then*

$$N^{2m} c_2[\pi] = \left(\sum_{\alpha \in P_2(2m)} \mathfrak{C}_2[\pi, \alpha] \right) + O(N^{m-1}) \tag{5.19}$$

Proof Fix a function $\mathbf{j} : [\pm 2m] \rightarrow [N]$ satisfying $\ker(\mathbf{j}) = \pi$ and let \mathbf{t} be as in (5.17). The (j_{-k}, j_k) -entry of $U_{N,i_1}^* U_{N,i_2}$ is then given by the sum

$$\begin{aligned} & \sum_{i_{-2k+1}, i_{2k+1}, i_{-2k}, i_{2k}=1}^N W^*(t_{-2k+1}, i_{-2k+1}) H^*(i_{-2k+1}, i_{-2k}) X(i_{-2k}, i_{2k}) \\ & H(i_{2k}, i_{2k-1}) W(i_{2k-1}, t_{2k-1}), \end{aligned}$$

and hence, by Equation (5.2) and the linearity of the covariance, we get

$$N^{2m} c_2[\pi] = \sum_{\mathbf{i}:[\pm 4m] \rightarrow [N]} \widehat{\mathbf{g}}(\mathbf{i}) \cdot \text{cov}[\widehat{\mathbf{w}}_1(\mathbf{i}, \mathbf{t} \circ \widetilde{\sigma}) \cdot \widehat{\mathbf{x}}_1(\mathbf{i}), \widehat{\mathbf{w}}_2(\mathbf{i}, \mathbf{t} \circ \widetilde{\sigma}) \cdot \widehat{\mathbf{x}}_2(\mathbf{i})] \tag{5.20}$$

where $\widehat{\mathbf{g}}(\mathbf{i})$, $\widehat{\mathbf{w}}_1(\mathbf{i}, \mathbf{t})$, $\widehat{\mathbf{w}}_2(\mathbf{i}, \mathbf{t})$, $\widehat{\mathbf{x}}_1(\mathbf{i})$, and $\widehat{\mathbf{x}}_2(\mathbf{i})$ are defined as above and $\widetilde{\sigma} \in \text{Sym}(\pm 4m)$ is the permutation with cycle decomposition

$$\widetilde{\sigma} = (-1, 1, -3, 3, \dots, -4m_1 + 1, 4m_1 - 1)$$

$$(-4m_1 - 1, 4m_1 + 1, \dots, 4m_1 + 4m_2 - 1).$$

Note that for every function $\mathbf{i} : [\pm 4m] \rightarrow [N]$ we have

$$\widehat{\mathbf{h}}(\mathbf{i} \circ \widehat{\sigma}) = \widehat{\mathbf{g}}(\mathbf{i} \circ \widetilde{\sigma}), \quad \widehat{\mathbf{w}}_k(\mathbf{i}, \mathbf{t}) = \widehat{\mathbf{w}}_k(\mathbf{i} \circ \widetilde{\sigma}, \mathbf{t} \circ \widetilde{\sigma}), \quad \text{and} \quad \widehat{\mathbf{x}}_k(\mathbf{i}) = \widehat{\mathbf{x}}_k(\mathbf{i} \circ \widetilde{\sigma})$$

for $k = 1, 2$, so we get

$$N^{2m} c_2[\pi] = \sum_{\mathbf{i} : [\pm 4m] \rightarrow [N]} \widehat{\mathbf{h}}(\mathbf{i} \circ \widehat{\sigma}) \cdot \text{cov}[\widehat{\mathbf{w}}_1(\mathbf{i}, \mathbf{t}) \cdot \widehat{\mathbf{x}}_1(\mathbf{i}), \mathbf{w}_2(\mathbf{i}, \mathbf{t}) \cdot \widehat{\mathbf{x}}_2(\mathbf{i})].$$

Now, suppose $\theta = \ker(\mathbf{i})$ for a function $\mathbf{i} : [\pm 4m] \rightarrow [N]$. Since $\pi^{\text{odd}} = \ker(\mathbf{t})$, from (2.6) we have that

$$\mathbb{E}[\widehat{\mathbf{w}}_1(\mathbf{i}, \mathbf{t}) \widehat{\mathbf{w}}_2(\mathbf{i}, \mathbf{t})] = 0 \quad \text{and} \quad \mathbb{E}[\widehat{\mathbf{w}}_1(\mathbf{i}, \mathbf{t})] \mathbb{E}[\widehat{\mathbf{w}}_2(\mathbf{i}, \mathbf{t})] = 0$$

provided $\theta_{\text{odd}} \neq \pi^{\text{odd}}$ and $\theta_{\text{odd}} \not\sqsubseteq (\pi_1 \sqcup \pi_2)^{\text{odd}} = \pi_1^{\text{odd}} \sqcup \pi_2^{\text{odd}}$, respectively; moreover, (2.5) implies that

$$\mathbb{E}[\widehat{\mathbf{x}}_1(\mathbf{i}) \widehat{\mathbf{x}}_2(\mathbf{i})] = \mathbb{E}[\widehat{\mathbf{x}}_1(\mathbf{i})] \mathbb{E}[\widehat{\mathbf{x}}_2(\mathbf{i})] = 0$$

if θ_{even} is not an even partition, θ_{even} has a block of the form $\{2k, -2k\}$, or $2k \sim_{\theta} -2k$ for some $k \in [2m]$. Thus, we obtain

$$\begin{aligned} N^{2m} c_2[\pi] &= \sum_{\theta \in \widetilde{P}_{\pi}(\pm 4m)} \sum_{\substack{\mathbf{i} : [\pm 4m] \rightarrow [N] \\ \ker(\mathbf{i}) = \theta}} \widehat{\mathbf{h}}(\mathbf{i} \circ \widehat{\sigma}) \mathbb{E}[\widehat{\mathbf{w}}_1(\mathbf{i}, \mathbf{t}) \widehat{\mathbf{w}}_2(\mathbf{i}, \mathbf{t})] \mathbb{E}[\widehat{\mathbf{x}}_1(\mathbf{i}) \widehat{\mathbf{x}}_2(\mathbf{i})] \\ &\quad - \sum_{\theta \in \widetilde{P}_{\pi_1 \sqcup \pi_2}(\pm 4m)} \sum_{\substack{\mathbf{i} : [\pm 4m] \rightarrow [N] \\ \ker(\mathbf{i}) = \theta}} \widehat{\mathbf{h}}(\mathbf{i} \circ \widehat{\sigma}) \mathbb{E}[\widehat{\mathbf{w}}_1(\mathbf{i}, \mathbf{t})] \mathbb{E}[\widehat{\mathbf{w}}_2(\mathbf{i}, \mathbf{t})] \\ &\quad \mathbb{E}[\widehat{\mathbf{x}}_1(\mathbf{i})] \mathbb{E}[\widehat{\mathbf{x}}_2(\mathbf{i})] \end{aligned}$$

where $\widetilde{P}_{\beta}(\pm 4m)$ denotes the set of all partitions $\theta \in P(\pm 4m)$ such that $\theta_{\text{odd}} \geq \beta^{\text{odd}}$ and for every integer $k \in [2m]$ there exists $l \in [2m] \setminus \{k\}$ such that $2k \sim_{\theta} -2k \sim_{\theta} -2l \sim_{\theta} 2l$.

Now, letting $\widehat{P}_{\beta}(\pm 4m)$ denote the set of partitions $\theta \in \widetilde{P}_{\beta}(\pm 4m)$ so that $\theta = \theta_{\text{even}} \sqcup \theta_{\text{odd}}$, $\theta_{\text{odd}} = \beta^{\text{odd}}$, and every block of θ_{even} is of the form $\{2k, -2k, 2l, -2l\}$ with $k, l \in [2m]$ and $k \neq l$, note the mapping

$$\alpha \mapsto \widehat{\alpha} \sqcup \beta^{\text{odd}}$$

with $\widehat{\alpha} = \{\{2k, -2k, 2l, -2l\} \mid \{k, l\} \in \alpha\}$ gives a bijection between the set of pairing partitions $P_2(2m)$ and the set $\widehat{P}_{\beta}(\pm 4m)$ for any partition $\beta \in P(\pm 2m)$. Thus, to get

(5.19), it only remains to show that

$$\begin{aligned}
 N^{2m} c_2 [\pi] &= \sum_{\theta \in \tilde{P}_\pi(\pm 4m)} \sum_{\substack{\mathbf{i}: [\pm 4m] \rightarrow [N] \\ \ker(\mathbf{i}) = \theta}} \hat{\mathbf{h}}(\mathbf{i} \circ \hat{\sigma}) \mathbb{E} [\hat{\mathbf{w}}(\mathbf{i}, \mathbf{t})] \mathbb{E} [\hat{\mathbf{x}}(\mathbf{i})] \\
 &\quad - \sum_{\theta \in \tilde{P}_{\pi_1 \sqcup \pi_2}(\pm 4m)} \sum_{\substack{\mathbf{i}: [\pm 4m] \rightarrow [N] \\ \ker(\mathbf{i}) = \theta}} \hat{\mathbf{h}}(\mathbf{i} \circ \hat{\sigma}) \mathbb{E} [\hat{\mathbf{w}}_1(\mathbf{i}, \mathbf{t})] \mathbb{E} [\hat{\mathbf{w}}_2(\mathbf{i}, \mathbf{t})] \\
 &\quad \mathbb{E} [\hat{\mathbf{x}}_1(\mathbf{i})] \mathbb{E} [\hat{\mathbf{x}}_2(\mathbf{i})] + O(N^{m-1}).
 \end{aligned}$$

Suppose $\theta \in \tilde{P}_{\pi_1 \sqcup \pi_2}(\pm 4m)$. Then, since $\theta_{\text{odd}} \geq (\pi_1 \sqcup \pi_2)^{\text{odd}} = \pi_1^{\text{odd}} \sqcup \pi_2^{\text{odd}}$ and each block of θ_{even} has at least 4 elements, we get the inequality

$$\#(\theta) \leq \#(\theta_{\text{odd}}) + \#(\theta_{\text{even}}) \leq \#(\pi_1) + \#(\pi_2) + m$$

with equality only if $\theta = \theta_{\text{even}} \sqcup \theta_{\text{odd}}$, $\theta_{\text{odd}} = \pi_1^{\text{odd}} \sqcup \pi_2^{\text{odd}}$, and each block of θ_{even} has exactly 4 elements, i.e., $\theta \in \tilde{P}_{\pi_1 \sqcup \pi_2}(\pm 4m)$; moreover, (2.5) and (2.6) imply that

$$\begin{aligned}
 &\left| \sum_{\substack{\mathbf{i}: [\pm 4m] \rightarrow [N] \\ \ker(\mathbf{i}) = \theta}} \hat{\mathbf{h}}(\mathbf{i} \circ \hat{\sigma}) \mathbb{E} [\hat{\mathbf{w}}_1(\mathbf{i}, \mathbf{t})] \mathbb{E} [\hat{\mathbf{w}}_2(\mathbf{i}, \mathbf{t})] \mathbb{E} [\hat{\mathbf{x}}_1(\mathbf{i})] \mathbb{E} [\hat{\mathbf{x}}_2(\mathbf{i})] \right| \\
 &\leq \frac{(N - \#(\pi_1))!}{N!} \cdot \frac{(N - \#(\pi_2))!}{N!} \cdot \left| \sum_{\substack{\mathbf{i}: [\pm 4m] \rightarrow [N] \\ \ker(\mathbf{i}) = \theta}} \hat{\mathbf{h}}(\mathbf{i} \circ \hat{\sigma}) \right| = O(N^{-\#(\pi_1) - \#(\pi_2) + \#(\theta)}).
 \end{aligned}$$

Hence, if $\theta \in \tilde{P}_{\pi_1 \sqcup \pi_2}(\pm 4m) \setminus \hat{P}_{\pi_1 \sqcup \pi_2}(\pm 4m)$, we have

$$\sum_{\substack{\mathbf{i}: [\pm 4m] \rightarrow [N] \\ \ker(\mathbf{i}) = \theta}} \hat{\mathbf{h}}(\mathbf{i} \circ \hat{\sigma}) \mathbb{E} [\hat{\mathbf{w}}_1(\mathbf{i}, \mathbf{t})] \mathbb{E} [\hat{\mathbf{w}}_2(\mathbf{i}, \mathbf{t})] \mathbb{E} [\hat{\mathbf{x}}_1(\mathbf{i})] \mathbb{E} [\hat{\mathbf{x}}_2(\mathbf{i})] = O(N^{m-1}).$$

Similar arguments show that $\#(\theta) \leq m + \#(\pi)$ for every partition $\theta \in \tilde{P}_\pi(\pm 4m)$ with equality only if $\theta \in \hat{P}_\pi(\pm 4m)$, and hence, we get

$$\sum_{\substack{\mathbf{i}: [\pm 4m] \rightarrow [N] \\ \ker(\mathbf{i}) = \theta}} \hat{\mathbf{h}}(\mathbf{i} \circ \hat{\sigma}) \mathbb{E} [\hat{\mathbf{w}}(\mathbf{i}, \mathbf{t})] \mathbb{E} [\hat{\mathbf{x}}(\mathbf{i})] = O(N^{m-1})$$

for any $\theta \in \tilde{P}_\pi(\pm 4m) \setminus \hat{P}_\pi(\pm 4m)$. □

Proposition 21 Suppose $\pi \in P(\pm 2m)$ and $\alpha \in P_2(2m)$ and let α_1 and α_2 denote the restrictions of α to the sets $[2m_1]$ and $[2m_1 + 2m_2] \setminus [2m_1]$, respectively. If $\mathfrak{C}_2[\pi, \alpha]$ is given by (5.18), then

$$\mathfrak{C}_2[\pi, \alpha] = \begin{cases} 1 + O(N^{-1}) & \text{if there is a symmetric pairing } \eta \in P(\pm 4m) \\ & \text{satisfying (1) from Proposition 13 and such that } \eta \leq \widehat{\alpha} \sqcup \pi^{\text{odd}}, \\ 1 + O(N^{-1}) & \text{if } \alpha \neq \alpha_1 \sqcup \alpha_2 \text{ and there is a symmetric pairing} \\ & \eta \in P(\pm 4m) \text{ satisfying (3) from Proposition 13} \\ & \text{with } k \text{ and } l \text{ even and such that } \eta \leq \widehat{\alpha} \sqcup \pi^{\text{odd}}, \\ O(N^{-\frac{1}{2}}) & \text{otherwise.} \end{cases}$$

Proof Note that if the polynomial $p_{\widehat{\sigma}^{-1} \circ (\widehat{\alpha} \sqcup \pi^{\text{odd}})}$ is nonzero, then $\mathfrak{C}_2[\pi, \alpha] = O(N^{-1/2})$. Indeed, if $p_{\widehat{\sigma}^{-1} \circ (\widehat{\alpha} \sqcup \pi^{\text{odd}})}$ is a nonzero polynomial, so is $p_{\widehat{\sigma}^{-1} \circ (\widehat{\alpha} \sqcup \pi_1^{\text{odd}} \sqcup \pi_2^{\text{odd}})}$ by Proposition 10, and thus, Corollary 8 implies there is a constant C independent from N such that

$$\left| \sum_{\substack{\mathbf{i}: [\pm 4m] \rightarrow [N] \\ \ker(\mathbf{i}) = \widehat{\sigma}^{-1} \circ (\widehat{\alpha} \sqcup \beta^{\text{odd}})}} \widehat{\mathbf{h}}(\mathbf{i}) \right| = \left| \sum_{\substack{\mathbf{i}: [\pm 4m] \rightarrow [N] \\ \ker(\mathbf{i}) = \widehat{\alpha} \sqcup \beta^{\text{odd}}}} \widehat{\mathbf{h}}(\mathbf{i} \circ \widehat{\sigma}) \right| \leq CN^{m + \#(\beta) - \frac{1}{2}}$$

for $\beta = \pi$ and $\beta = \pi_1 \sqcup \pi_2$. But then, we get that $\mathfrak{C}_2[\pi, \alpha] = O(N^{-1/2})$ since from (2.5), (2.6), and (5.18) we have

$$|\mathfrak{C}_2[\pi, \alpha]| \leq C \cdot \frac{(N - \#(\pi))!}{N!} \cdot N^{\#(\pi) - \frac{1}{2}} + C \cdot \frac{(N - \#(\pi_1))!}{N!} \cdot \frac{(N - \#(\pi_2))!}{N!} \cdot N^{\#(\pi_1) + \#(\pi_2) - \frac{1}{2}}.$$

Assume $p_{\widehat{\sigma}^{-1} \circ (\widehat{\alpha} \sqcup \pi^{\text{odd}})}$ is the zero polynomial. Then, by Proposition 10, there is a symmetric pairing partition $\eta \leq \widehat{\alpha} \sqcup \pi^{\text{odd}}$ such that $p_{\widehat{\sigma}^{-1} \circ \eta}$ is also the zero polynomial, and hence, the partition η must satisfy one of the conditions (1)-(6) from Proposition 13. However, we have $\eta = \eta_{\text{odd}} \sqcup \eta_{\text{even}}$, since $\eta \leq \widehat{\alpha} \sqcup \pi^{\text{odd}}$, and neither $2m_1$ or $2m_2$ is odd, so conditions (2) and (4)-(6) cannot hold. Now, note that if $p_{\widehat{\sigma}^{-1} \circ (\widehat{\alpha} \sqcup \beta^{\text{odd}})}$ is zero polynomial for some partition $\beta \in P(\pm 2m)$, then

$$\sum_{\substack{\mathbf{i}: [\pm 4m] \rightarrow [N] \\ \ker(\mathbf{i}) = \widehat{\alpha} \sqcup \beta^{\text{odd}}}} \widehat{\mathbf{h}}(\mathbf{i} \circ \widehat{\sigma}) = \frac{N!}{(N - \#(\widehat{\alpha} \sqcup \beta^{\text{odd}}) + 1)!} = \frac{N!}{(N - m - \#(\beta) + 1)!}$$

since we would have $\widehat{\mathbf{h}}(\mathbf{i} \circ \widehat{\sigma}) = 1$ for any function $\mathbf{i} : [\pm 4m] \rightarrow [N]$ satisfying $\ker(\mathbf{i}) = \widehat{\alpha} \sqcup \beta^{\text{odd}}$. Hence, if $\alpha_1, \alpha_2, \pi_1,$ and π_2 are all even partitions and the

polynomial $p_{\sigma^{-1} \circ \hat{\alpha} \sqcup \pi_1^{\text{odd}} \sqcup \pi_2^{\text{odd}}}$ is zero, from (2.5), (2.6), and (5.18), we obtain

$$\begin{aligned} & \frac{(N - \#(\pi))!}{N!} \cdot \sum_{\substack{\mathbf{i}: [\pm 4m] \rightarrow [N] \\ \ker(\mathbf{i}) = \hat{\alpha} \sqcup \pi^{\text{odd}}}} \widehat{\mathbf{h}}(\mathbf{i} \circ \widehat{\sigma}) - \frac{(N - \#(\pi_1))!}{N!} \\ & \frac{(N - \#(\pi_2))!}{N!} \cdot \sum_{\substack{\mathbf{i}: [\pm 4m] \rightarrow [N] \\ \ker(\mathbf{i}) = \hat{\alpha} \sqcup \pi_1^{\text{odd}} \sqcup \pi_2^{\text{odd}}}} \widehat{\mathbf{h}}(\mathbf{i} \circ \widehat{\sigma}) \\ & = N^m \mathfrak{C}_2[\pi, \alpha] = O(N^{m-1}) \end{aligned} \tag{5.21}$$

On the other hand, if either α_1 or α_2 is not an even partition, from (2.5) and (5.18), we get

$$\mathfrak{C}_2[\pi, \alpha] = \frac{1}{N^m} \cdot \frac{(N - \#(\pi))!}{N!} \cdot \sum_{\substack{\mathbf{i}: [\pm 4m] \rightarrow [N] \\ \ker(\mathbf{i}) = \hat{\alpha} \sqcup \pi^{\text{odd}}}} \widehat{\mathbf{h}}(\mathbf{i} \circ \widehat{\sigma}) = 1 + O(N^{-1}). \tag{5.22}$$

Suppose η satisfies (3) from Proposition 13 and let $1 \leq k \leq 4m_1$ and $4m_1 + 1 \leq l \leq 4m_1 + 4m_2$ such that $\eta = \{ \{ \widehat{\sigma}^{t_1}(-k), \widehat{\sigma}^{-t_1}(k) \}, \{ \widehat{\sigma}^{t_2}(-l), \widehat{\sigma}^{-t_2}(l) \} \mid t_2, t_2 \geq 0 \}$. We need to consider three cases: k and l are both odd, $k + l$ is odd, and k and l are both even. First, if k and l are both odd, then $p_{\sigma^{-1} \circ \hat{\alpha} \sqcup \pi_1^{\text{odd}} \sqcup \pi_2^{\text{odd}}}$ is also the zero polynomial, π_1 and π_2 are both even partitions, and $\alpha = \alpha_1 \sqcup \alpha_2$, so (5.21) holds. Second, if $k + l$ is odd, then $\alpha = \alpha_1 \sqcup \alpha_2$ and $\pi = \pi_1 \sqcup \pi_2$, but then (5.21) holds too. Third, if k and l are both even, then $\pi = \pi_1 \sqcup \pi_2$ and either $\alpha = \alpha_1 \sqcup \alpha_2$ or $\alpha \neq \alpha_1 \sqcup \alpha_2$. However, if $\alpha = \alpha_1 \sqcup \alpha_2$, we already know that $\mathfrak{C}_2[\pi, \alpha] = O(N^{-1})$ from (5.21), and if $\alpha \neq \alpha_1 \sqcup \alpha_2$, then α_1 and α_2 are not even partitions, so (5.22) holds. Finally, if η satisfies (1) from Proposition 13, we must have $\alpha \neq \alpha_1 \sqcup \alpha_2$, so we obtain $\mathfrak{C}_2[\pi, \alpha] = 1 + O(N^{-1})$. \square

Proof of (3) from Proposition 17 Fix an even partition $\pi \in P(\pm 2m)$ such that $\pi \leq \theta$ for some partition $\theta \in P_{\chi\chi}(\pm 2m)$ and let $\mathfrak{C}_2[\pi, \alpha]$ be given by (5.18) for each pairing partition $\alpha \in P_2(2m)$. By Proposition 21, we have that

$$\sum_{\alpha \in P_2(2m)} \mathfrak{C}_2[\pi, \alpha] = |E_\pi| + |F_\pi| - |E_\pi \cap F_\pi| + O(N^{-1/2})$$

where E_π and F_π are the subsets of $P_2(2m)$ given by

$$E_\pi = \left\{ \alpha \in P_2(2m) \mid \eta \leq \widehat{\alpha} \sqcup \pi^{\text{odd}} \text{ for some symmetric pairing } \eta \in P(\pm 4m) \text{ satisfying (1) from Proposition 13} \right\}$$

and

$$F_\pi = \left\{ \alpha \in P_2(2m) \mid \alpha \neq \alpha_1 \sqcup \alpha_2 \text{ and } \eta \leq \widehat{\alpha} \sqcup \pi^{\text{odd}} \text{ for some symmetric pairing } \eta \in P(\pm 4m) \text{ satisfying (3) from Proposition 13 with } k \text{ and } l \text{ even} \right\}.$$

Thus, by Proposition 20, we only need to show that $E_\pi \neq \emptyset$ implies $|E_\pi| = 1$, $F_\pi \neq \emptyset$ implies $|F_\pi| = 2$, and $E_\pi \cap F_\pi$ is empty.

Let α and β be pairing partitions in $P_2(2m)$ and suppose there are symmetric pairings $\eta_\alpha, \eta_\beta \in P(\pm 4m)$ satisfying (1) from Proposition 13, $\eta_\alpha \leq \widehat{\alpha} \sqcup \pi^{\text{odd}}$, and $\eta_\beta \leq \widehat{\beta} \sqcup \pi^{\text{odd}}$. Then, there are integers $2m_1 + 1 \leq l_\alpha, l_\beta \leq 2m_1 + 2m_2$ so that

$$\widehat{\sigma}^{-t}(2l_\alpha - 1) \sim_{\eta_\alpha} \widehat{\sigma}^t(-1) \sim_{\eta_\beta} \widehat{\sigma}^{-t}(2l_\beta - 1) \quad \forall t \geq 0$$

where $\widehat{\sigma}$ is the permutation given by

$$\begin{aligned} \widehat{\sigma} &= (-1, 1, -2, 2, \dots, -4m_1, 4m_1) \\ &\quad (-4m_1 - 1, 4m_1 + 1, -4m_1 - 2, \dots, -4m_1 - 4m_2, 4m_1 + 4m_2). \end{aligned}$$

But then, we must have

$$\widehat{\sigma}^{-t}(2l_\alpha - 1) \sim_{\widehat{\alpha} \sqcup \pi^{\text{odd}}} \widehat{\sigma}^t(-1) \sim_{\widehat{\beta} \sqcup \pi^{\text{odd}}} \widehat{\sigma}^{-t}(2l_\beta - 1) \quad \forall t \geq 0 \tag{5.23}$$

since $\eta_\alpha \leq \widehat{\alpha} \sqcup \pi^{\text{odd}}$ and $\eta_\beta \leq \widehat{\beta} \sqcup \pi^{\text{odd}}$, and thus, we get that

$$\sigma^{-t}(l_\alpha) \sim_\pi \sigma^t(-1) \sim_\pi \sigma^{-t}(l_\beta) \quad \forall t \geq 0$$

where σ is the permutation given by

$$\begin{aligned} \sigma &= (-1, 1, -2, 2, \dots, -2m_1, 2m_1) \\ &\quad (-2m_1 - 1, 2m_1 + 1, -2m_1 - 2, \dots, -2m_1 - 2m_2, 2m_1 + 2m_2). \end{aligned}$$

In particular, for $t = 0$, we obtain $l_\alpha \sim_\pi -1 \sim_\pi l_\beta$, and thus, we have $l_\alpha = l_\beta$ since π is an even partition with only blocks of the form $\{-k, +k, -l, l\}$ and $\{+k, -l\}$. Therefore, it follows from (5.23) that $\widehat{\alpha} = \widehat{\beta}$, or, equivalently, $\alpha = \beta$. This shows that $E_\pi \neq \emptyset$ implies $|E_\pi| = 1$.

Suppose now there are symmetric pairings $\eta_\alpha, \eta_\beta \in P(\pm 4m)$ satisfying (3) from Proposition 13 with k and l even, $\eta_\alpha \leq \widehat{\alpha} \sqcup \pi^{\text{odd}}$, and $\eta_\beta \leq \widehat{\beta} \sqcup \pi^{\text{odd}}$. Then, there exist integers $1 \leq k_\alpha \leq k_\beta \leq 2m_1$ so that

$$\widehat{\sigma}^t(-2k_\alpha) \sim_{\eta_\alpha} \widehat{\sigma}^{-t}(2k_\alpha) \quad \text{and} \quad \widehat{\sigma}^t(-2k_\beta) \sim_{\eta_\beta} \widehat{\sigma}^{-t}(2k_\beta) \quad \forall t \geq 0,$$

and hence, we get

$$\widehat{\sigma}^t(-2k_\alpha) \sim_{\widehat{\alpha} \sqcup \pi^{\text{odd}}} \widehat{\sigma}^{-t}(2k_\alpha) \quad \text{and} \quad \widehat{\sigma}^t(-2k_\beta) \sim_{\widehat{\beta} \sqcup \pi^{\text{odd}}} \widehat{\sigma}^{-t}(2k_\beta) \quad \forall t \geq 0 \tag{5.24}$$

since $\eta_\alpha \leq \widehat{\alpha} \sqcup \pi^{\text{odd}}$ and $\eta_\beta \leq \widehat{\beta} \sqcup \pi^{\text{odd}}$; in particular, we must have

$$\widehat{\sigma}^{4t}(2k_\alpha) \sim_{\widehat{\alpha}} \widehat{\sigma}^{-4t}(-2k_\alpha) \quad \text{and} \quad \widehat{\sigma}^{4t}(2k_\beta) \sim_{\widehat{\beta}} \widehat{\sigma}^{-4t}(-2k_\beta) \quad \forall t \geq 0.$$

Now, since α and β are pairing partitions of $[2m_1+2m_2]$, $\widehat{\alpha} = \{\{+2k, -2k, +2l, -2l\} \mid \{k, l\} \in \alpha\}$, and $\widehat{\beta} = \{\{+2k, -2k, +2l, -2l\} \mid \{k, l\} \in \beta\}$, we get

$$\sigma^{2t}(k_\alpha) \sim_\alpha \sigma^{-2t}(k_\alpha) \quad \text{and} \quad \sigma^{2t}(k_\beta) \sim_\beta \sigma^{-2t}(k_\beta) \quad \forall t \geq 0,$$

where σ is the permutation defined above; hence, we obtain

$$\alpha_1 = \{\{k_\alpha\}, \{k_\alpha + 1, k_\alpha - 1\}, \dots, \{k_\alpha + m_1 - 1, k_\alpha - m_1 + 1\}, \{k_\alpha + m_1\}\}$$

and

$$\beta_1 = \{\{k_\beta\}, \{k_\beta + 1, k_\beta - 1\}, \dots, \{k_\beta + m_1 - 1, k_\beta - m_1 + 1\}, \{k_\beta + m_1\}\}$$

where α_1 and β_1 denote the restrictions of α and β , respectively, to the set $[\pm 2m_1]$. Let us show that $\alpha_1 = \beta_1$. From (5.24), we also have that

$$\begin{aligned} \widehat{\sigma}^{4t}(-2k_\alpha - 1) &\sim_{\pi^{\text{odd}}} \widehat{\sigma}^{-4t}(2k_\alpha - 1), & \widehat{\sigma}^{4t}(2k_\alpha + 1) &\sim_{\pi^{\text{odd}}} \widehat{\sigma}^{-4t}(-2k_\alpha + 1), \\ \widehat{\sigma}^{4t}(-2k_\beta - 1) &\sim_{\pi^{\text{odd}}} \widehat{\sigma}^{-4t}(2k_\beta - 1), & \text{and} & \widehat{\sigma}^{4t}(2k_\beta + 1) \sim_{\pi^{\text{odd}}} \widehat{\sigma}^{-4t}(-2k_\beta + 1) \end{aligned}$$

for every integer $t \geq 0$, and thus, since $\pi^{\text{odd}} = \{\{2k - \text{sign}(k) \mid k \in B\} \mid B \in \pi\}$, we obtain

$$\begin{aligned} \sigma^{t+1}(k_\alpha) &= \sigma^t(-k_\alpha - 1) \sim_\pi \sigma^{-t}(k_\alpha) \quad \text{and} \\ \sigma^{t+1}(k_\beta) &= \sigma^t(-k_\beta - 1) \sim_\pi \sigma^{-t}(k_\beta) \quad \forall t \geq 0. \end{aligned}$$

Let $t = k_\beta - k_\alpha$ and note that

$$\sigma^{2t}(k_\alpha) \sim_\pi \sigma^{-2t+1}(k_\alpha) \sim_\pi \sigma^{2t+1}(k_\alpha)$$

since

$$k_\beta = \sigma^{2t}(k_\alpha) \sim_\pi \sigma^{-2t+1}(k_\alpha) \quad \text{and} \quad \sigma^{2t+1}(k_\alpha) = \sigma(k_\beta) \sim_\pi k_\beta;$$

moreover, since $\sigma^{2t}(k_\alpha) > 0$, $\sigma^{-2t+1}(k_\alpha), \sigma^{2t+1}(k_\alpha) < 0$, and π is a partition with only blocks of the form $\{-k, +k, -l, l\}$ and $\{+k, -l\}$ with $k, l > 0$, we must have

$$\sigma^{2t}(k_\alpha) = -\sigma^{-2t+1}(k_\alpha), \quad \sigma^{2t}(k_\alpha) = -\sigma^{2t+1}(k_\alpha), \quad \text{or} \quad \sigma^{-2t+1}(k_\alpha) = \sigma^{2t+1}(k_\alpha),$$

or, equivalently,

$$\sigma^{4t-2}(k_\alpha) = k_\alpha, \quad \sigma^{-2}(k_\alpha) = k_\alpha, \quad \text{or} \quad \sigma^{-4t}(k_\alpha) = k_\alpha.$$

But the equality $\sigma^s(k_\alpha) = k_\alpha$ holds if only if $s \equiv 0 \pmod{4m_1}$, so only $\sigma^{-4t}(k_\alpha) = k_\alpha$ can hold, and thus, we get $k_\alpha = k_\beta$ or $k_\beta = k_\alpha + m_1$ since $0 \leq t = k_\beta - k_\alpha \leq 2m_1 - 1$.

Therefore, $\alpha_1 = \beta_1$ and there is an integer $1 \leq k = k_\alpha \leq 2m_1$ so that

$$\begin{aligned} \alpha_1 &= \{\{k\}, \{k + 1, k - 1\}, \dots, \{k + m_1 - 1, k - m_1 + 1\}, \{k + m_1\}\} = \beta_1 \\ &= \{\{\sigma^{2t}(k), \sigma^{-2t}(k)\} \mid 0 \leq t \leq m_1\}. \end{aligned}$$

Similarly, letting α_2 and β_2 denote the restrictions of α and β , respectively, to the set $[\pm(2m_1 + 2m_2)] \setminus [\pm 2m_1]$, we have $\alpha_2 = \beta_2$ and there is an integer $2m_1 + 1 \leq l \leq 2m_1 + 2m_2$ so that

$$\begin{aligned} \alpha_2 &= \{\{l\}, \{l + 1, l - 1\}, \dots, \{l + m_2 - 1, l - m_2 + 1\}, \{l + m_2\}\} = \beta_2 \\ &= \{\{\sigma^{2t}(l), \sigma^{-2t}(l)\} \mid 0 \leq t \leq m_2\}. \end{aligned}$$

This shows that $|F_\pi| = 2$ provided $F_\pi \neq \emptyset$ since $\gamma \in F_\pi$ implies

$$\gamma = \{\{k, l\}, \{k + m_1, l + m_2\}\} \cup \tilde{\alpha} \quad \text{or} \quad \gamma = \{\{k, l + m_2\}, \{k + m_1, l\}\} \cup \tilde{\alpha}$$

where $\tilde{\alpha} = \{\{\sigma^{2t}(k), \sigma^{-2t}(k)\} \mid 1 \leq t \leq m_1 - 1\} \cup \{\{\sigma^{2t}(l), \sigma^{-2t}(l)\} \mid 1 \leq t \leq m_2 - 1\}$.

Finally, $E_\pi \cap F_\pi$ is empty since $E_\pi \neq \emptyset$ implies $\pi \neq \pi_1 \sqcup \pi_2$, and, on the other hand, $F_\pi \neq \emptyset$ implies $\pi = \pi_1 \sqcup \pi_2$. □

6 Concluding Remarks

(1) The exponent $-1/2$ in the remainder terms $O(N^{-1/2})$ essentially comes from the $-1/2$ in Proposition 7 and can be upgraded to -1 as follows. One first shows that for all partitions $\pi = \{B_1, \dots, B_r\}$ appearing in (5.3) and having at least one through block—i.e., a block intersecting both $[\pm 2m_1]$ and $[\pm 2m] \setminus [\pm 2m_1]$ —the polynomial $p_{\sigma^{-1} \circ \pi}(x_1, \dots, x_r) = \sum_{1 \leq t \leq s \leq r} a_{t,s} x_t x_s$ satisfies exactly one of the following:

- (a) $p_{\sigma^{-1} \circ \pi}$ is the zero polynomial, or
- (b) there exists $t \in [r]$ so that $a_{t,t} = 0$ and $a_{t,s} \neq 0$ or $a_{s,t} \neq 0$ for some $s \in [r]$.

For polynomials $p_{\sigma^{-1} \circ \pi}$ satisfying (b) above, the last part of Proposition 7’s proof shows that

$$\left| \sum_{j_1, j_2, \dots, j_r=0}^{N-1} e^{-\frac{2\pi\sqrt{-1}}{N} p_{\sigma^{-1} \circ \pi}(j_1, j_2, \dots, j_r)} \right| \leq C_{p_{\sigma^{-1} \circ \pi}} N^{r-1} \tag{6.1}$$

for some constant $C_{p_{\sigma^{-1} \circ \pi}}$ independent of N . Then, carefully carrying the -1 from (6.1) through the computations of $\mathfrak{C}_2[\pi]$ and $\mathfrak{C}_2[\pi, \alpha]$, one can replace $-1/2$ by -1 in the remainder terms $O(N^{-1/2})$, first in Proposition 17 and Lemma 18, and then in Theorems 1 and 2.

- (2) The random matrix ensemble $\{W_{N,1}, H_N W_{N,2}\}_{N=1}^\infty$ satisfies the hypothesis in Lemma 3, and hence, Theorem 2 is proved once we show (1.14) holds. To that end, we first define appropriate versions of the functions $\mathbf{w}(\mathbf{i}, \mathbf{j})$, $\mathbf{w}_1(\mathbf{i}, \mathbf{j})$, $\mathbf{w}_2(\mathbf{i}, \mathbf{j})$ and show that (5.10) still holds in this case. Then, following similar steps to those in the proof of Proposition 17 and Lemma 18 and letting $U_{N,i_1}^* U_{N,i_2} = \frac{1}{\sqrt{N}} W_{N,1}^* H_N W_{N,2}$, we conclude

$$\begin{aligned} & \sum_{\substack{\pi \in P_{\text{even}}(\pm 2m) \\ \pi \leq \theta}} N^m c_2[\pi] \mu(\pi, \theta) \\ &= \begin{cases} 1 + O(N^{-1/2}) & \text{if } \theta \text{ is a pairing partition satisfying (1)} \\ & \text{from Proposition 13,} \\ O(N^{-1/2}) & \text{otherwise.} \end{cases} \end{aligned}$$

- (3) One can replace the discrete Fourier transform H_N in the unitary random matrix ensemble $\{W_N, H_N W_N / \sqrt{N}, X_N H_N W_N / \sqrt{N}\}_{N=1}^\infty$ by any Hadamard matrix H'_N and still get an asymptotically liberating ensemble, see [1]. Moreover, key equations in this paper involving H_N still hold when we replace H_N by a general Hadamard matrix H'_N , for instance, (3.8), (3.10), and (3.12). Thus, to determine the corresponding induced fluctuations moments, one needs to compute graph sums of H'_N and obtain similar results to those from Sect. 3.2. However, the results for graph sums of H_N were possible thanks to the reciprocity theorem for generalized Gauss sums and it is not immediate what tools could be used for a general H'_N .
- (4) Although Proposition 15 and Corollary 16 give equivalent conditions only for point-wise uniform boundedness, similar statements and proofs provide us with corresponding conditions for the point-wise convergence of a sequence of multilinear functionals. These conditions together with bounds for graph sums can be exploited to study higher-order moments. In particular, the relations (4.4) and (5.3) can be used to determine the higher-order moments induced by Haar-unitary and Haar-orthogonal via the Weingarten Calculus from [4] and [5].

Acknowledgements The author would like to thank James A. Mingo for invaluable discussions during the preparation of this paper. The author also thanks the anonymous referees for their insightful suggestions and comments, all of which improved the presentation of this material. Research was partially supported by The Mexican National Council of Science and Technology (CONACYT) ref. 579659/410386.

Data Availability Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

Declarations

Conflict of interest Research was partially supported by The Mexican National Council of Science and Technology (CONACYT) ref. 579659/410386.

References

1. Anderson, G.W., Farrell, B.: Asymptotically liberating sequences of random unitary matrices. *Adv. Math.* **255**, 381–413 (2014)
2. Anderson, G.W., Guionnet, A., Zeitouni, O.: *An Introduction to Random Matrices*. Cambridge University Press, Cambridge (2010)
3. Berndt, B.C., Evans, R.J., Williams, K.S.: *Gauss and Jacobi Sums*. Wiley, New York (1998)
4. Collins, B.: Moments and cumulants of polynomial random variables on unitary groups, the Itzykson-Zuber integral, and free probability. *Int. Math. Res. Not.* **8**, 953–982 (2003)
5. Collins, B., Śniady, P.: Integration with respect to the Haar measure on unitary, orthogonal and symplectic group. *Commun. Math. Phys.* **264**, 773–795 (2006)
6. Edelman, A., Rao, N.R.: Random matrix theory. *Acta Numer.* **14**, 233–297 (2005)
7. Gabriel, F.: Combinatorial theory of permutation-invariant random matrices I: Partitions, geometry and renormalization, (2015). Preprint at [arXiv:1503.02792](https://arxiv.org/abs/1503.02792)
8. Hao, Z., Popa, M.: A combinatorial result on asymptotic independence relations for random matrices with non-commutative entries. *J. Oper. Theory* **80**, 47–76 (2018)
9. Jiao, Y., Popa, M.: On fluctuations of traces of large matrices over a non-commutative algebra. *J. Oper. Theory* **73**, 71–90 (2015)
10. Keating, J.: The Riemann zeta-function and quantum chaos. In: Casati, G., Guarneri, I., Smilansky, U. (eds.) *Quantum Chaos*, pp. 145–185. North-Holland Publishing Co., Amsterdam (1993)
11. Male, C.: Traffic distributions and independence: permutation invariant random matrices and the three notions of independence. *Mem. Am. Math. Soc.* **267**, 850 (2020)
12. Male, C., Mingo, J.A., Péché, S., Speicher, R.: Joint global fluctuations of complex wigner and deterministic matrices. *Random Matrices Theory Appl.* **11**, 2250015 (2022)
13. Mingo, J.A., Popa, M.: Real second order freeness and Haar orthogonal matrices. *J. Math. Phys.* **54**, 051701 (2013)
14. Mingo, J.A., Popa, M.: Freeness and the transposes of unitarily invariant random matrices. *J. Funct. Anal.* **271**, 883–921 (2016)
15. Mingo, J.A., Śniady, P., Speicher, R.: Second order freeness and fluctuations of random matrices. II. Unitary random matrices. *Adv. Math.* **209**, 212–240 (2007)
16. Mingo, J.A., Speicher, R.: Second order freeness and fluctuations of random matrices. I. Gaussian and Wishart matrices and cyclic Fock spaces. *J. Funct. Anal.* **235**, 226–270 (2006)
17. Mingo, J.A., Speicher, R.: Sharp bounds for sums associated to graphs of matrices. *J. Funct. Anal.* **262**, 2272–2288 (2012)
18. Mingo, J.A., Speicher, R.: *Free Probability and Random Matrices*. Springer, New York (2017)
19. Muraki, N.: The five independences as natural products. *Infin. Dimens. Anal. Quantum Probab. Relat. Top.* **6**, 337–371 (2003)
20. Nica, A., Speicher, R.: *Lectures on the Combinatorics of Free Probability*. Cambridge University Press, Cambridge (2006)
21. Redelmeier, C.E.I.: Real second-order freeness and the asymptotic real second-order freeness of several real matrix models. *Int. Math. Res. Not. IMRN* **3353–3395**, 2012 (2014)
22. Redelmeier, C.E.I.: Quaternionic second-order freeness and the fluctuations of large symplectically invariant random matrices. *Random Matrices Theory Appl.* **10**, 2150017 (2021)
23. Speicher, R.: On universal products. In: Voiculescu, D.-V. (ed.) *Free probability theory*, pp. 257–266. Amer. Math. Soc, Providence, RI (1997)
24. Tulino, A.M., Verdú, S.: Random matrix theory and wireless communications. *Commun. Inf. Theory* **1**, 1–182 (2004)
25. Voiculescu, D.: Symmetries of some reduced free product C^* -algebras. In H. Araki, C. C. Moore, Ş. V. Stratila, and D. V. Voiculescu, editors, *Operator Algebras and their Connections with Topology and Ergodic Theory*, vol. 1132, pp. 556–588 (1985). Springer Berlin
26. Voiculescu, D.: Limit laws for random matrices and free products. *Invent. Math.* **104**, 201–220 (1991)
27. Voiculescu, D.V., Dykema, K.J., Nica, A.: *Free Random Variables*. American Mathematical Society, Providence (1992)
28. Wigner, E.P.: Characteristic vectors of bordered matrices with infinite dimensions. *Ann. Math.* **2**(62), 548–564 (1955)
29. Wishart, J.: The generalised product moment distribution in samples from a normal multivariate population. *Biometrika* **20A**(1/2), 32–52 (1928)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.