Fluctuation moments induced by asymptotically liberating random matrix ensembles

by

Josue Vazquez-Becerra

A thesis submitted to the
Department of Mathematics and Statistics
in conformity with the requirements for
the degree of Doctor of Philosophy

Queen's University
Kingston, Ontario, Canada
September 2020

Abstract

The topics covered in this thesis belong to the theories of free probability and random matrices. Random matrix ensembles formed of independent Haar-unitary random matrices, or independent Haar-orthogonal random matrices, are known to be asymptotically liberating, they give rise to asymptotic free independence when used for conjugation of constant matrices. G. Anderson and B. Farrel showed that certain family of discrete random unitary matrices can actually be used to same end.

We investigate fluctuation moments and higher order moments induced on constant matrices by conjugation with asymptotically liberating random matrix ensembles. We show for the first time that the fluctuation moments associated to 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.

Acknowledgments

First and foremost, I would like to thank my supervisor, Prof. James A. Mingo, for his continuous support through all these years at Queen's University. His understanding of the challenges that have arisen and his constant encouragement to overcome them have been fundamental for my growth as a mathematician and as an individual.

I am grateful for the many wonderful people I have met in Kingston. My friends, my fellow students, the professors and staff at Queen's University, this journey have always relied upon the countless contributions all of you make to my academic and personal life.

I appreciate the examining committee for taking the time to read and examine this work.

I am in debt with the free probability community for all the lectures and discussions that have motivated me to learn more about the subject. I am grateful to Mario Torres-Diaz and Octavio Arizmendi-Echegaray for their friendship and for showing me their always inspiring dedication to mathematics.

I appreciate the financial support from the Mexican National Council of Science and Technology through the project CONACYT ref. 579659/410386.

Last but not least, I thank my family for their love, support, and inspiration. My parents, Maria Becerra-Espiricueta and Candelario Vazquez, whose effort and sacrifice have created a vast and rich life for me. My oldest brother, Miguel Vazquez-Becerra, whose actions have never ceased to show me how to take better care of the ones we love. And my youngest

brother, Mario Vazquez-Becerra, whom I admire for his determination and courage.

Contents

Chapter 1

Introduction

1.1 Background

Random matrices are matrix-valued random variables that were first investigated in mathematical statistics [25] and then in nuclear physics [24]. Over the years, its study has evolved into a theory with applications to pure and applied sciences such as numerical analysis [6], analytic number theory [9], and wireless communications [20], to name some.

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 then those arising from letting N go to infinity. Eigenvalue distributions, eigenvalues spacing, concentration inequalities, large deviation principles, maximal eigenvalues, and central limit theorems are some examples of limiting properties, for a good introduction on these subjects one can consult [2].

Now, introduced by D. Voiculescu in his research on von Neumann algebras in [22], 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 1.1.1. 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 are satisfied:

(AF.1) the limit $\lim_{N\to\infty} \mathbb{E}\left[\mathrm{tr}\left(X_{N,i}^{m}\right)\right]$ exists for each index $i \in I$ and every integer $m \geq 1$, with $\mathrm{tr}(\cdot)$ denoting the normalized trace $\frac{1}{N}\mathrm{Tr}(\cdot)$, and

(AF.2) for all integers $m \geq 1$, all indexes $i_1, i_2, \ldots, i_m \in I$ satisfying $i_1 \neq i_2, i_2 \neq i_3, \ldots, i_{m-2} \neq i_{m-1}, i_{m-1} \neq i_m$, and $i_m \neq i_1$ and all polynomials $\mathrm{p}_1, \mathrm{p}_2, \ldots, \mathrm{p}_m$ in the algebra $\mathbb{C}[\mathrm{x}]$, we have $\lim_{N\to\infty} \mathbb{E}\left[\mathrm{tr}\left(Y_{N,1}Y_{N,2}\cdots Y_{N,m}\right)\right] = 0$ where $Y_{N,k} = \mathrm{p}_k\left(X_{N,i_k}\right) - \mathbb{E}\left[\mathrm{tr}\left(\mathrm{p}_k\left(X_{N,i_k}\right)\right)\right] I_N$.

The first connection between free probability and random matrices was established by D. Voiculescu when he shows in [23] that independent Gaussian Unitary Ensembles converge to free semi-circular 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 [21] and the book [17] have become standard introductions to free probability and the recent monograph [15] 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 [23], and subsequently generalized by other authors, states that conjugation by independent Haar-distributed unitary 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

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

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 [10].

Aiming to enclose all of the 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 1.1.2. 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 $\left\{\{U_{N,i}\}_{i\in I}\right\}_{N=1}^{\infty}$ is *asymptotically liberating* if for all indexes $i_1, i_2, \ldots, i_m \in I$ with $i_1 \neq i_2, i_2 \neq i_3, \ldots, i_{m-1} \neq i_m$, and $i_m \neq i_1$ there exists a constant $C > 0$ depending only on the indexes $i_1, i_2, \ldots, i_m$ such that

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

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

It follows immediately from the definition above 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 asymptotically liberating 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 1.1.1; moreover, if each $Y_{N,k}$ is as in (AF.2) from Definition 1.1.1, 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 $\mathrm{p}_k(D_{N,i_k}) - \mathrm{tr}(\mathrm{p}_k(D_{N,i_k}))I_N$, 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 1.2.3 below.

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

$$\lim_{N\to\infty} \mathbb{E}\left[\mathrm{tr}\left(X_{N,i_1}X_{N,i_2}\cdots X_{N,i_m}\right)\right] \tag{1.2}$$

where at least two of the indexes $i_1, i_2, \ldots, i_m \in I$ are distinct and none of them depend on N. Thus, 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

$$\lim_{N\to\infty} \mathbb{E}\left[\mathrm{tr}\left(X_{N,i_1}^1X_{N,i_2}^4X_{N,i_1}^7X_{N,i_2}^2\right)\right] = \alpha_8^{(i_1)}\alpha_4^{(i_2)}\alpha_2^{(i_2)} + \alpha_6^{(i_2)}\alpha_1^{(i_1)}\alpha_7^{(i_1)} - \alpha_1^{(i_1)}\alpha_4^{(i_2)}\alpha_7^{(i_1)}\alpha_2^{(i_2)}$$

where $\alpha_m^{(i)}$ denotes $\lim_{N\to\infty}\mathbb{E}[\mathrm{tr}(X_{N,i}^m)]$ 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 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

$$\lim_{N\to\infty} N^{n-2}\mathfrak{c}_n[\mathrm{Tr}(\widetilde{X}_{N,1}), \mathrm{Tr}(\widetilde{X}_{N,2}), \ldots, \mathrm{Tr}(\widetilde{X}_{N,n})] \tag{1.3}$$

where $\mathfrak{c}_n[\cdot, \ldots, \cdot]$ denotes the n-th *classical cumulant*, see Section 2.1, and each $\widetilde{X}_{N,k}$ is of the form

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

for some integer $m_k \geq 1$ and some indexes $i_1^{(k)}, i_2^{(k)}, \ldots, i_{m_k}^{(k)} \in I$ 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 $i_1^{(1)}, \ldots, i_{m_1}^{(1)}, i_1^{(2)}, \ldots, i_{m_2}^{(2)}, \ldots, i_1^{(n)}, \ldots, i_{m_n}^{(n)}$ 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

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

for some integers $m_1, m_2 \geq 1$ and indexes $i_1, i_2, \ldots, i_{m_1}, i_{m_1+1}, i_{m_1+2}, \ldots, i_{m_1+m_2} \in I$. A common practice in free probability theory to determine (1.3), or (1.4), combinatorially

is that of calculating limiting moments of products of cyclically alternating and centered random matrices, as in (AF.2) from Definition 1.1.1. For fluctuation moments, this means one must consider limits of the form

$$\lim_{N\to\infty} \mathrm{Cov}\left[\mathrm{Tr}(Y_{N,1}Y_{N,2}\cdots Y_{N,m_1}), \mathrm{Tr}(Z_{N,1}Z_{N,2}\cdots Z_{N,m_2})\right]$$

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

$$Y_{N,k} = \mathrm{p}_k\left(X_{N,i_k}\right) - \mathbb{E}\left[\mathrm{tr}\left(\mathrm{p}_k\left(X_{N,i_k}\right)\right)\right] I_N \text{ and } Z_{N,l} = \mathrm{q}_l\left(X_{N,j_l}\right) - \mathbb{E}\left[\mathrm{tr}\left(\mathrm{q}_l\left(X_{N,j_l}\right)\right)\right] I_N \quad (1.5)$$

for all polynomials $\mathrm{p}_1, \mathrm{p}_2, \ldots, \mathrm{p}_{m_1}, \mathrm{q}_1, \mathrm{q}_2, \ldots, \mathrm{q}_{m_2} \in \mathbb{C}[\mathrm{x}]$ and all indexes $i_1, i_2, \ldots, i_{m_1}, j_1, j_2, \ldots, j_{m_2} \in I$ satisfying the condition

$$i_1 \neq i_2, i_2 \neq i_3, \ldots, i_{m_1-1} \neq i_{m_1}, i_{m_1} \neq i_1, j_1 \neq j_2, j_2 \neq j_3, \ldots, j_{m_2-1} \neq j_{m_2}, j_{m_2} \neq j_1. \quad (1.6)$$

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 [13] the notion of *asymptotic free independence of second order*.

Definition 1.1.3. 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) the limit $\lim_{N\to\infty} \mathrm{Cov}\left[\mathrm{Tr}(X_{N,i}^m), \mathrm{Tr}(X_{N,i}^n)\right]$ exists for each index $i \in I$ and all integers $m, n \geq 1$,

(ASOF.2) for all integers $m_1, m_2 \geq 1$, all indexes $i_1, i_2, \ldots, i_{m_1}, j_1, j_2, \ldots, j_{m_2} \in I$ satisfying (1.6), and all polynomials $\mathrm{p}_1, \mathrm{p}_2, \ldots, \mathrm{p}_{m_1}, \mathrm{q}_1, \mathrm{q}_2, \ldots, \mathrm{q}_{m_2}$ in the algebra $\mathbb{C}[\mathrm{x}]$, if we take $Y_N = Y_{N,1}Y_{N,2}\cdots Y_{N,m_1}$ and $Z_N = Z_{N,1}Z_{N,2}\cdots Z_{N,m_2}$ 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

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

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

(ASOF.3) for ever integer $n \geq 3$, all polynomials $\mathrm{p}_1, \mathrm{p}_2, \ldots, \mathrm{p}_n$ in the algebra of non-commutative polynomials $\mathbb{C}\langle \mathrm{x}_i \mid i \in I\rangle$, letting $Y_{N,k} = \mathrm{p}_k\left(\{X_{N,i}\}_{i\in I}\right)$, we have

$$\lim_{N\to\infty} \mathfrak{c}_n\left[\mathrm{Tr}\left(Y_{N,1}\right), \mathrm{Tr}\left(Y_{N,2}\right), \ldots, \mathrm{Tr}\left(Y_{N,n}\right)\right] = 0$$

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 [13] and [12], 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 [18] 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 1.1.3 but (ASOF.2) has to be replaced by the following:

(ASOF.2') for all integers $m_1, m_2 \geq 1$, all indexes $i_1, i_2, \ldots, i_{m_1}, j_1, j_2, \ldots, j_{m_2} \in I$ satisfying (1.6), and all polynomials $\mathrm{p}_1, \mathrm{p}_2, \ldots, \mathrm{p}_{m_1}, \mathrm{q}_1, \mathrm{q}_2, \ldots, \mathrm{q}_{m_2}$ in the algebra $\mathbb{C}[\mathrm{x}]$, if we take $Y_N = Y_{N,1}Y_{N,2}\cdots Y_{N,m_1}$ and $Z_N = Z_{N,1}Z_{N,2}\cdots Z_{N,m_2}$ 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

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

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 [18], it was showed by J. Mingo and M. Popa in [10] 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 thesis is 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, i.e., more terms are needed, 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 1.1.3, then we can write

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

and

$$Z_N = \left(U_{N,j_1}B_{N,1}U_{N,j_1}^*\right)\left(U_{N,j_2}B_{N,2}U_{N,j_2}^*\right)\cdots\left(U_{N,j_{2m_1}}B_{N,2m_1}U_{N,j_{2m_1}}^*\right)$$

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

$$A_{N,k} = \mathrm{p}_k\left(D_{N,i_k}\right) - \mathrm{tr}\left(\mathrm{p}_k\left(D_{N,i_k}\right)\right)I_N \quad \text{and} \quad B_{N,l} = \mathrm{q}_l\left(D_{N,j_l}\right) - \mathrm{tr}\left(\mathrm{q}_l\left(D_{N,j_l}\right)\right)I_N \tag{1.9}$$

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 1.1.1 and the relation in (1.7) that the covariance $\mathrm{Cov}\left[\mathrm{Tr}(Y_N), \mathrm{Tr}(Z_N)\right]$

converges to

$$\lim_{N\to\infty} \delta_{m_1,m_2} \sum_{l=1}^{m_1} \prod_{k=1}^{2m_2} \mathrm{tr}\left(A_{N,k} B_{N,2l-k}\right) \tag{1.10}$$

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 $\mathrm{Cov}\left[\mathrm{Tr}(Y_N), \mathrm{Tr}(Z_N)\right]$ converges to

$$\lim_{N\to\infty} \delta_{m_1,m_2} \sum_{l=1}^{m_1} \left(\prod_{k=1}^{2m_2} \mathrm{tr}\left(A_{N,k} B_{N,2l-k}\right) + \prod_{k=1}^{2m_2} \mathrm{tr}\left(A_{N,k} B_{N,2l+k}^T\right) \right) \tag{1.11}$$

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 to this thesis, 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 (1.10) and in (1.11).

Theorem 1.2.1. 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). Take $X_{N,1} = U_{N,1} D_{N,2} U_{N,1}^*$ and $X_{N,2} = U_{N,2} D_{N,2} U_{N,2}^*$ where $U_{N,1}$ and $U_{N,2}$ are two 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 $\mathrm{p}_1, \mathrm{p}_2, \ldots, \mathrm{p}_{2m_1}, \mathrm{q}_1, \mathrm{q}_2, \ldots, \mathrm{q}_{2m_2} \in \mathbb{C}[\mathrm{x}]$ and some indexes $i_1, i_2, \ldots, i_{2m_1}, j_1, j_2, \ldots, j_{2m_2} \in \{1, 2\}$ satisfying (1.6) and $i_1 = j_1$, then

the following holds:

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

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

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

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

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

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

with $A_{N,k}$ and $B_{N,l}$ defined as in (1.9), $2l-k$, $2l+k-1$, 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 module $2m_2$.

Evidence of the existence of second order behaviors, other than second order free independence and second order free independence in the real sense, is not new, at least, from an algebraic point of view. We mention in particular the papers [7] and [8] where the authors analyze fluctuation moments of matrices with entries from a possibly non-commutative

unital algebra and obtain different relations from those mentioned above. Now, notice (1.1) alone is not enough to guarantee the existence of limiting second order behaviors in Theorem 1.2.1, in contrast to (1.10) and (1.11). For instance, if we want to take the limit as N goes to infinity in (3) from Theorem 1.2.1, 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 $\lim_{N\to\infty} \operatorname{tr}(D_{N,i_1} D_{N,i_2} \cdots D_{N,i_m})$ exists for all integers $m \geq 1$ and all indexes $i_1, i_2, \ldots, i_m \in \{1, 2\}$. This shows we can not expect a classification for universal products of second order, in the spirit of [16] or [19], encompassing all of the second order behaviors exhibited by random matrices.

Despite the fact that no pair of distinct unitary matrices $U_{N,1}$ and $U_{N,2}$ from the ensemble $\{W_N, H_N W_N/\sqrt{N}, X_N H_N W_N/\sqrt{N}\}$ 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 (1.10). 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 1.2.2. 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 1.1.3. In particular, if Y_N, Z_N, $A_{N,k}$, and $B_{N,l}$ are given as in the previous theorem,

then

$$\mathrm{Cov}\left[\mathrm{Tr}(Y_N), \mathrm{Tr}(Z_N)\right] = \delta_{m_1,m_2} \sum_{l=1}^{m_1} \left(\prod_{k=1}^{2m_1} \mathrm{tr}\left(A_{N,k} B_{N,2l-k}\right) \right) + O\left(N^{-\frac{1}{2}}\right) \tag{1.12}$$

Now, the main result in [1] gives sufficient conditions on a unitary random matrix ensemble to be asymptotically liberating. Using a different approach than that one in [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 1.1.2 to cumulants of any order. More concretely, we have the following lemma.

Lemma 1.2.3. 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 $\mathcal{U} = \{\{U_{N,i}\}_{i\in I}\}_{N=1}^{\infty}$ 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 $\{\mathrm{W}^* U_{N,i_1}^* U_{N,i_2} \mathrm{W}\}_{i_1,i_2\in I}$ are equal in distribution for every N-by-N signed permutation matrix W_N and

(II) for every positive integer m there is a constant C_m independent from N such that

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

for all integers $j_1, j_2 \in \{1, 2, \ldots, N\}$ and indexes $i_1, i_2 \in I$ with $i_1 \neq i_2$,

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

that for

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

with $A_1, A_2, \ldots, A_m \in \mathrm{M}_N(\mathbb{C})$ each of trace zero, we have

$$\left|\mathfrak{c}_n\left[\mathrm{Tr}\left(Y_{N,1}\right), \mathrm{Tr}\left(Y_{N,2}\right), \ldots, \mathrm{Tr}\left(Y_{N,n}\right)\right]\right| \leq C(i_1, i_2, \ldots, i_m)\|A_1\|\|A_2\|\cdots\|A_m\|$$

Thus, the fact that a unitary random matrix ensemble $\{\{U_{N,i}\}_{i\in I}\}_{N=1}^{\infty}$ 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 Definition 3.2.4. 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 1.2.4. 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 $\{\{U_{N,i}\}_{i\in I}\}_{N=1}^{\infty}$ satisfies (I) and (II) from the previous lemma and (1.1) holds. Then the ensemble $\{\{U_{N,i}D_{N,i}U^*_{N,i}\}_{i\in I}\}_{N=1}^{\infty}$ has the *bounded cumulants property*, namely, for all polynomials $\mathrm{p}_1, \mathrm{p}_2, \mathrm{p}_3, \ldots$ in the algebra of non-commutative

polynomials $\mathbb{C}\langle \mathrm{x}_i \mid i \in I\rangle$ taking $Y_{N,k} = \mathrm{p}_k(\{U_{N,i}D_{N,i}U_{N,i}^*\}_{i\in I})$ we have

$$\sup_N \left| \mathfrak{c}_n \left[\mathrm{Tr}\left(Y_{N,1}\right), \mathrm{Tr}\left(Y_{N,2}\right), \ldots, \mathrm{Tr}\left(Y_{N,n}\right) \right] \right| < \infty \tag{1.13}$$

for every integer $n \geq 2$.

The term *bounded cumulants property* is borrowed from [11] 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.

1.3 Organization of this thesis

The rest of this thesis is organized as follows. In Chapter 2, we give some preliminary notation and definitions, concretely, we provide the reader with the definitions and notation for partitions, classical cumulants, non-commutative polynomials, and deterministic matrices. A literature review of free probability and random matrices is presented in Chapter 3 and Chapter 4, anyone familiar with these subjects might choose to skip these two chapters and turn to them only if necessary. Chapter 3 gives an introduction to the main notions in algebraic probability spaces such as algebraic distribution, convergence in distribution, free independence, and asymptotic free independence. In Chapter 4, we describe how the algebraic notions from the previous chapter apply to random matrix ensembles and introduce the notions of second order free independence and asymptotically liberating ensembles. Chapter 5 contains various important results on graph sums of square matrices, a central tool to prove our main results. Roughly speaking, a graph sums 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. In Chapter 6, we prove

our main results, concretely, Lemma 1.2.3 and Theorem 1.2.4 are proved in Section 6.1 and Section 6.1, respectively, whereas Theorem 1.2.1 and Theorem 1.2.2 are proved in Section 6.3. Finally, in Chapter 7, we give some concluding remarks including open questions and further research projects.

Chapter 2

Preliminaries

2.1 Set partitions, Möbius inversion function, and cumulants

A *partition* of 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 blocks 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 $\pi_1 = \{\{-1,-3,-2,2\},\{1,3\}\}$, $\pi_2 = \{\{-1,-2\},\{2\},\{1,-3,3\}\}$, and $\pi_3 = \{\{-1,-3\},\{1,3\},\{-2,2\}\}$ are all partitions of $\{-1,1,2,-2,-3,3\}$. The partitions π_1 and π_3 are both even, but while π_3 is a paring, π_1 is not. The partition π_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 $\{1,2,\ldots,m\}$ and $\{-1,1,-2,2,\ldots,$

$-m, m\}$, respectively. The sets $[m]$ and $[\pm m]$ are used extensively in this thesis, 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 $P_{\text{even}}([\pm m])$.

Every partition $\pi \in P(S)$ defines an *equivalence relation*, denoted by $\sim_\pi$, 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 $\zeta : P(S) \times P(S) \to \{1, 0\}$ 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 $\mu : P(S) \times P(S) \to \mathbb{Z}$ called the *Möbius function* of $P(S)$ which can be explicitly computed, but first, let us establish the convention that whenever we write $\eta = \{B_{i_1}, B_{i_2}, \ldots, B_{i_r}\}$ 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 $\theta = \{B_1, B_2, \ldots, B_r\}$ and $\pi = \{B_{1,1}, B_{1,2}, \ldots, B_{1,m_1}, \ldots, B_{n,m_r}\}$ with $B_k = \cup_{l=1}^{m_k} B_{k,l}$ for each k, and, in this case, we have

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

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 $f, g : P(S) \to \mathbb{C}$, we have the relation

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

The computation of Möbius function, Equation (2.2), and the Möbius inversion formula, Equation (2.3), are well-known and their proofs can be found in [17, Lecture 10].

Classical cumulants

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

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

for random variables $x_1, x_2, x_3, \ldots, x_n \in L^{\infty-}(\Omega, \mathcal{F}, P)$ 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 $\mathfrak{c}_n[x_1, x_2, \ldots, x_n] = 0$.

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 $\mathbf{j} : S_1 \to S_2$, we take $j_k = \mathbf{j}(k)$ for every $k \in S_1$; additionally, if $S_1 = [\pm m]$ for some integer $m \geq 1$, we identify the function $\mathbf{j} : S_1 \to S_2$ with the tuple $(j_{-1}, j_1, j_{-2}, \ldots, j_{-m}, j_m)$. Moreover, the *kernel* of a function $\mathbf{j} : S_1 \to S_2$, 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.,

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

Additionally, if we are given permutations $\sigma_l \in \{f : S_l \to S_l \mid f \text{ is bijective}\}$ for $l = 1, 2$, we let $\mathbf{j} \circ \boldsymbol{\sigma}_1 : S_1 \to S_2$ and $\boldsymbol{\sigma}_2 \circ \mathbf{j} : S_1 \to S_2$ be given by the usual composition of functions, so we have

$$\mathbf{j} \circ \boldsymbol{\sigma}_1(k) = j_{\sigma_1(k)} \quad \text{and} \quad \boldsymbol{\sigma}_2 \circ \mathbf{j}(k) = \sigma_2(j_k) \qquad \forall k \in S_1.$$

Example. The function $\mathbf{j} : [\pm 3] \to [4]$ 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 $\sigma_1 : [\pm 3] \to [\pm 3]$ is given $\sigma_1(k) = -k$ for every $k \in [\pm 3]$ and $\sigma_2 : [4] \to [4]$ is the cyclic permutation $(1, 2, 3, 4)$, then $\mathbf{j} \circ \boldsymbol{\sigma}_1 = (1, 4, 4, 3, 4, 1)$ and $\boldsymbol{\sigma}_2 \circ \mathbf{j} = (1, 2, 4, 1, 2, 1)$.

Now, the group of permutations $\{f : S \to S \mid f \text{ is bijective}\}$ acts on the set of partitions $P(S)$ as follows: given a permutation $\sigma \in \{f : S \to S \mid f \text{ is bijective}\}$ we let $\sigma \circ \pi$ be given by

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

The map $\pi \mapsto \sigma \circ \pi$, preserves order, i.e. for all partition $\pi, \theta \in P(S)$

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

Thus the map $\pi \mapsto \sigma \circ \pi$ is a poset automorphism.

Remark. Note that a partition $\pi \in P(S_1)$ and a function $\mathbf{j} : S_1 \to S_2$ satisfy $\pi \leq \ker(\mathbf{j})$ if 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 permutations $\sigma_1 : S_1 \to S_1$ and $\sigma_2 : S_2 \to S_2$, we have that $\ker(\mathbf{j} \circ \boldsymbol{\sigma}_1) = \sigma_1^{-1} \circ \ker(\mathbf{j})$ and $\ker(\mathbf{j}) = \ker(\boldsymbol{\sigma}_2 \circ \mathbf{j})$.

2.3 Non-commutative polynomials

Let I be a non-empty set. We denote by $\mathbb{C}\langle \mathrm{x}_i \mid i \in I\rangle$ the algebra of non-commutative polynomials on the family of variables $\{\mathrm{x}_i \mid i \in I\}$. Let us recall that $\mathbb{C}\langle \mathrm{x}_i \mid i \in I\rangle$ is the algebra over $\mathbb{C}$ with a basis consisting of all the words in the alphabet $\{\mathrm{x}_i \mid i \in I\}$, 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

$$\mathrm{x}_{i_1}\mathrm{x}_{i_2}\cdots\mathrm{x}_{i_{r-1}}\mathrm{x}_{i_r}$$

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

$$(\mathrm{x}_{i_1}\mathrm{x}_{i_2}\cdots\mathrm{x}_{i_r})(\mathrm{x}_{j_1}\mathrm{x}_{j_2}\cdots\mathrm{x}_{j_s}) = \mathrm{x}_{i_1}\mathrm{x}_{i_2}\cdots\mathrm{x}_{i_r}\mathrm{x}_{j_1}\mathrm{x}_{j_2}\cdots\mathrm{x}_{j_s}.$$

Given polynomials $\mathrm{p}_1, \mathrm{p}_2, \ldots, \mathrm{p}_m$ in the algebra $\mathbb{C}\langle \mathrm{x}_i \mid i \in I\rangle$ and a set $S = \{k_1 < k_2 < \cdots < k_n\} \subset [m]$, we let

$$\prod_{k\in S}^{\rightarrow} \mathrm{p}_k := \mathrm{p}_{k_1}\mathrm{p}_{k_2}\cdots\mathrm{p}_{k_n}.$$

Suppose $\mathcal{A}$ is a unital algebra over $\mathbb{C}$ with multiplicative identity $1_{\mathcal{A}}$ and assume we are given a family of elements $\{a_i\}_{i\in I}$ in $\mathcal{A}$. For each non-commutative polynomial $\mathrm{p} \in \mathbb{C}\langle \mathrm{x}_i \mid i \in I\rangle$, we denote by

$$\mathrm{p}\left(\{a_i\}_{i\in I}\right)$$

the element in $\mathcal{A}$ obtained from replacing each x_i appearing in the polynomial p with a_i for every $i \in I$ and the constant term of p, say λ, with the scalar multiple of the identity matrix $\lambda 1_{\mathcal{A}}$. For instance, if $\mathrm{p}(\mathrm{x}_1, \mathrm{x}_2) = \mathrm{x}_1\mathrm{x}_2 - \mathrm{x}_2^2 + 4$, then $\mathrm{p}(\{a_i\}_{i\in\{1,2\}}) = a_1a_2 - a_2^2 + 41_{\mathcal{A}}$.

2.4 Deterministic matrices

We denote by $\mathrm{Mat}_N(\mathbb{C})$ the set of N-by-N matrices with complex entries for each positive integer N. The identity matrix in $\mathrm{Mat}_N(\mathbb{C})$ is denoted by I_N. Recall that $\mathrm{Mat}_N(\mathbb{C})$ is a unital algebra over $\mathbb{C}$ under the usual matrix operations. Given a matrix $A \in \mathrm{Mat}_N(\mathbb{C})$, we denote by $A(i,j)$ its entry in the i^{th} row and j^{th} column and by A^* its conjugate transpose.

The *operator norm* $\|\cdot\| : \mathrm{Mat}_N(\mathbb{C}) \to [0,\infty)$ is the norms on $\mathrm{Mat}_N(\mathbb{C})$ defined for each

matrix $A \in \mathrm{Mat}_N(\mathbb{C})$ by

$$\|A\| := \sup\{|Ax| : x \in \mathbb{C}^N, |x| = 1\}$$

where $|\cdot|$ denotes the euclidean norm in $\mathbb{C}^N$. Recall that for all matrices $A, B \in \mathrm{Mat}_N(\mathbb{C})$ we have the inequalities

$$\|AB\| \leq \|A\|\|B\|.$$

We always assume that $\mathrm{Mat}_N(\mathbb{C})$ is endowed with such topology.

The *trace* of a matrix $A \in \mathrm{Mat}_N(\mathbb{C})$, denoted $\mathrm{Tr}(A)$, is defined as the sum of its entries on the main diagonal, i.e.,

$$\mathrm{Tr}(A) = \sum_{i=1}^{N} A(i,i).$$

The *normalized trace* of A, denoted $\mathrm{tr}(A)$, is given by the average of its entries on the main diagonal, so we have

$$\mathrm{tr}(A) = \frac{1}{N}\sum_{i=1}^{N} A(i,i) = \frac{1}{N}\mathrm{Tr}(A).$$

A matrix $A \in \mathrm{Mat}_N(\mathbb{C})$ is said to be of *trace zero* if either its trace or its normalized trace equals 0. Notice that for all matrices $A, B \in \mathrm{Mat}_N(\mathbb{C})$, and complex numbers $\lambda \in \mathbb{C}$ we have

$$\mathrm{Tr}(\lambda A + B) = \lambda \mathrm{Tr}(A) + \mathrm{Tr}(B), \quad \mathrm{Tr}(AB) = \mathrm{Tr}(BA), \quad \textit{and} \quad \frac{1}{N}\left|\mathrm{Tr}(A)\right| \leq \|A\| \ .$$

Chapter 3

Algebraic Probability (Literature Review)

This chapter is the first part of the literature review. In this chapter, we start with an introduction to notions of algebraic probability spaces, algebraic distribution, and convergence in algebraic distribution. Then we examine how the notion of independence from classical probability translates to the framework of algebraic probability spaces, so we can identify some similarities and differences with the notions of free independence and asymptotic free independence.

3.1 From classical probability to algebraic probability spaces

Algebraic probability spaces

Let us recall that a *classical probability space* is a triple $(\Omega, \mathcal{F}, P)$ consisting of a non-empty set Ω, a σ-algebra $\mathcal{F}$ of subsets of Ω, and a probability measure $P : \mathcal{F} \to [0, 1]$. Moreover, a *complex-valued random variable* on $(\Omega, \mathcal{F}, P)$ is a function $x : \Omega \to \mathbb{C}$ so that the set $x^{-1}(\mathrm{U}) = \{\omega \in \Omega : x(\omega) \in \mathrm{U}\}$ belongs to the σ-algebra $\mathcal{F}$ for every open set $\mathrm{U} \subset \mathbb{C}$. After identifying complex-valued random variables on $(\Omega, \mathcal{F}, P)$ that are the same function up to a

measurable set of probability zero, the set of complex-valued random variables on $(\Omega, \mathcal{F}, P)$, endowed with point-wise operations, becomes a *complex unital algebra*.

Now, the *k-th moment* of a complex-valued random variable $x : \Omega \to \mathbb{C}$ is defined as the integral

$$\int_{\Omega} [x(\omega)]^k dP(\omega)$$

if such integral exists, and it is not defined otherwise; we denote by $L^{\infty-}(\Omega, \mathcal{F}, P)$ the set of complex-valued random variables on $(\Omega, \mathcal{F}, P)$ that have moments of all orders. The *first moment* of x, denoted $\mathbb{E}[x]$, is also called the *expected value* of x, and it is well-defined if and only if the integral

$$\int_{\Omega} |x(\omega)| dP(\omega)$$

exists. Note the map $x \mapsto \mathbb{E}[x]$ defines a unital linear functional on $L^{\infty-}(\Omega, \mathcal{F}, P)$. Hence, from an algebraic point of view, we might think of $(L^{\infty-}(\Omega, \mathcal{F}, P), \mathbb{E}[\,\cdot\,])$ merely as a pair consisting of a complex unital algebra and a unital linear functional, leading to the following definition.

Definition 3.1.1. An *algebraic probability space* is a pair $(\mathcal{A}, \varphi)$ consisting of a unital algebra $\mathcal{A}$ over $\mathbb{C}$, with multiplicative identity $1_{\mathcal{A}}$, and a linear functional $\varphi : \mathcal{A} \to \mathbb{C}$ such that $\varphi(1_{\mathcal{A}}) = 1$. The elements of $\mathcal{A}$ are called *algebraic random variables*, or simply *random variables*.

Examples. In addition to $(L^{\infty-}(\Omega, \mathcal{F}, P), \mathbb{E}[\,\cdot\,])$, we have the following standard examples of algebraic probability spaces:

(1) $(\mathbb{C}\langle \mathrm{x}_i \mid i \in I\rangle, \mu)$ the algebra of non-commutative polynomials together with any linear functional μ so that $\mu(1) = 1$.

(2) $(M_N(\mathbb{C}), \mathrm{tr}(\cdot))$ the algebra of N-by-N matrices with entries from $\mathbb{C}$ together with the normalized trace $\mathrm{tr}(\cdot) = \frac{1}{N}\mathrm{Tr}(\cdot)$.

(3) $(\mathbb{C}G, \tau_G)$ where $\mathbb{C}G$ denotes the group algebra of a group G and $\tau_G : \mathbb{C}G \to \mathbb{C}$ is defined by $\tau_G\left(\sum_{g\in G} \alpha_g g\right) = \alpha_e$. The group algebra $\mathbb{C}G$ of a group G is defined by

$$\mathbb{C}G := \left\{ \sum_{g\in G} \alpha_g g := (\alpha_g)_{g\in G} \mid \alpha_g \in \mathbb{C} \text{ and } \alpha_g \neq 0 \text{ for finitely many } g \right\}$$

together with point-wise addition and multiplication given by

$$\left(\sum_{g\in G} \alpha_g g\right)\left(\sum_{g\in G} \beta_g g\right) = \sum_{g\in G}\left(\sum_{\substack{h,k\in G \\ hk=g}} \alpha_h \beta_k\right) g.$$

(4) $(B(\mathcal{H}), \tau_\xi)$ where $B(\mathcal{H})$ denotes the algebra of all bounded linear operators on a Hilbert space $\mathcal{H}$ with inner product $\langle\cdot,\cdot\rangle_{\mathcal{H}}$, ξ is a vector in $\mathcal{H}$ of unit norm, and $\tau_\xi : B(\mathcal{H}) \to \mathbb{C}$ is given by $\tau_\xi(T) = \langle T(\xi), \xi\rangle_{\mathcal{H}}$.

In most cases, the unital complex algebras considered in algebraic probability spaces come with underlying additional structure that can be exploited and from which some terminology is borrowed. For instance, an algebraic probability space $(\mathcal{A}, \varphi)$ endowed with an anti-linear operation $\mathcal{A} \ni a \mapsto a^* \in \mathcal{A}$ such that $(a^*)^* = a$, $(ab)^* = b^*a^*$, and $\varphi(a^*a) \geq 0$ for all $a, b \in \mathcal{A}$ is called a $*$-*probability space*. In this framework, a random variable a is called *self-adjoint* if $a = a^*$, *normal* if $aa^* = a^*a$, and *unitary* if $aa^* = a^*a = 1_{\mathcal{A}}$.

Note that the algebraic space $(L^{\infty-}(\Omega, \mathcal{F}, P), \mathbb{E}[\,\cdot\,])$ is a $*$-probability space with the $*$ operation defined by $x^*(\omega) = \overline{x(\omega)}$ for each $x \in L^{\infty-}(\Omega, \mathcal{F}, P)$ and every $\omega \in \Omega$, the complex conjugate of a number $z \in \mathbb{C}$ is denoted by $\overline{z}$. The algebraic probability spaces

$(M_N(\mathbb{C}), \mathrm{tr}(\cdot))$, $(\mathbb{C}G, \tau_G)$, and $(B(\mathcal{H}), \tau_\xi)$ are also $*$-probability space if we take A^* as the conjugate transpose of a matrix $A \in M_N(\mathbb{C})$, $(\sum_{g\in G} \alpha_g g)^* := (\sum_{g\in G} \overline{\alpha_{g^{-1}}} g)$, and T^* as the adjoint of an bounded operator $T \in B(\mathcal{H})$.

Passing from an analytic setting to an algebraic one has certainly shortcomings and virtues. On one hand, algebraic probability spaces only cover random variables with moments of all orders, and even in that case, we might lose some information since moments do not determine random variables in the classical setting. On the other hand, once we establish an appropriate notion of distribution for random variables in algebraic probability spaces, the notion of independence, being that joint distributions can be recovered from individual distributions via universal rules, leads to new types of independence, giving rise to the question of how much of the theory of classical probability still holds or change if we replace classical independence by another type of independence. At the end, the results from algebraic probability theory have exceeded its apparent limitations, in particular, free probability theory, coupled to the notion of free independence, has had outstanding contributions to what once was seemingly unrelated: Operator Algebras and Random Matrix Theory.

Algebraic distribution of first order

A good notion of distribution for algebraic random variables should allow us to compare and analyze families of random variables even if the families come from different probability spaces. In classical probability, if $x_N : \Omega_N \to \mathbb{C}$ is a complex-valued random variable defined on $(\Omega_N, \mathcal{F}_N, P_N)$ for each $N \geq 1$, the distribution of x_N is defined as the push-forward measure μ_N determined by $\mu_N(\mathrm{U}) = P_N(x_N^{-1}(\mathrm{U}))$ for open sets $\mathrm{U} \subset \mathbb{C}$. Moreover, the probability spaces $(\Omega_N, \mathcal{F}_N, P_N)$ might be different from each other but all of the distributions μ_N belong to the set of probability measures on $\mathbb{C}$, so all of the μ_N can be compared with

each other, and hence, the further notions of equality in distribution and convergence in distribution emerge.

Now, in an algebraic probability space $(\mathcal{A}, \varphi)$, the linear functional φ is meant to play the role of the expected value function, so the *k-th moment* of an algebraic random variable $a \in \mathcal{A}$ is defined to be the complex number $\varphi(a^k)$ for every integer $k \geq 1$. It might seem tempting to define the distribution of the random variable a as the sequence of moments $\{\varphi(a^k)\}_{k=1}^{\infty}$, all distributions would be sequences of complex numbers regardless of the ambient probability space, but it is actually more convenient to do so as follows.

Definition 3.1.2. Let a be a random variable in an algebraic probability space $(\mathcal{A}, \varphi)$. The *algebraic distribution* of a is the linear functional $\mu_a : \mathbb{C}[\mathrm{x}] \to \mathbb{C}$ given by $\mu_a(\mathrm{p}) = \varphi(\mathrm{p}(a))$ for every polynomial $\mathrm{p} \in \mathbb{C}[\mathrm{x}]$ where $\mathrm{p}(a) \in \mathcal{A}$ is defined by substituting $\mathrm{x} = a$.

Certainly, the unital linear functional $\mu_a : \mathbb{C}[\mathrm{x}] \to \mathbb{C}$ and the sequence of moments $\{\varphi(a^k)\}_{k=1}^{\infty}$ convey the same information, the distribution of a is completely determined by its moments, and vice versa, but we prefer the former since it has a tidy and natural generalization to several random variables.

Definition 3.1.3. Let $\{a_i\}_{i \in I}$ be a family of random variables in an algebraic probability space $(\mathcal{A}, \varphi)$. The *algebraic joint distribution* of the family $\{a_i\}_{i \in I}$ is the linear functional $\mu : \mathbb{C}\langle \mathrm{x}_i \mid i \in I \rangle \to \mathbb{C}$ given by $\mu(\mathrm{p}) = \varphi(\mathrm{p}(\{a_i\}_{i \in I}))$ for every polynomial $\mathrm{p} \in \mathbb{C}\langle \mathrm{x}_i \mid i \in I \rangle$.

Note that the definition above does achieve the goal of providing us with a notion of distribution that allow us compare families of random variables as long as the random variables in each family are indexed by the same set. Thus, if we are given families of random variables $\{a_i\}_{i \in I}$ and $\{b_i\}_{i \in I}$ from algebraic probability spaces $(\mathcal{A}, \varphi)$ and $(\mathcal{B}, \psi)$, respectively, we say that they are *equal in distribution* if their algebraic joint distributions give the same unital linear functional on the algebra of non-commutative polynomials $\mathbb{C}\langle \mathrm{x}_i \mid i \in I \rangle$.

Remark. Let $\{a_i\}_{i\in I}$ and $\{b_i\}_{i\in I}$ be as above and let $\mu : \mathbb{C}\langle \mathrm{x}_i \mid i \in I\rangle \to \mathbb{C}$ and $\nu : \mathbb{C}\langle \mathrm{x}_i \mid i \in I\rangle \to \mathbb{C}$ be the algebraic joint distributions of $\{a_i\}_{i\in I}$ and $\{b_i\}_{i\in I}$, respectively. Note that if we let $\mathrm{ev}_a : \mathbb{C}\langle \mathrm{x}_i \mid i \in I\rangle \to \mathcal{A}$ and $\mathrm{ev}_b : \mathbb{C}\langle \mathrm{x}_i \mid i \in I\rangle \to \mathcal{B}$ be the unique algebraic homomorphisms such that $\mathrm{ev}_a(\mathrm{x}_i) = a_i$ and $\mathrm{ev}_b(\mathrm{x}_i) = b_i$ for every $i \in I$, then $\mu = \varphi \circ \mathrm{ev}_a$ and $\nu = \psi \circ \mathrm{ev}_b$. Thus, $\{a_i\}_{i\in I}$ and $\{b_i\}_{i\in I}$ are equal in distribution only if the following diagram commutes:

$$\begin{array}{ccc} \mathcal{A} & \xrightarrow{\quad\varphi\quad} & \mathbb{C} \\ {\scriptstyle \mathrm{ev}_a}\uparrow & & \uparrow{\scriptstyle \psi} \\ \mathbb{C}\langle \mathrm{x}_i \mid i \in I\rangle & \xrightarrow[\mathrm{ev}_b]{} & \mathcal{B} \end{array}$$

Equivalently, $\{a_i\}_{i\in I}$ and $\{b_i\}_{i\in I}$ are equal in distribution only if for all integers $m \geq 1$ and indexes $i_1, i_2, \ldots, i_m \in I$ we have $\varphi(a_{i_1}a_{i_2}\cdots a_{i_m}) = \psi(b_{i_1}b_{i_2}\cdots b_{i_m})$.

The collection of *k-th moments* of a family of random variables $\{a_i\}_{i\in I}$ in algebraic probability space $(\mathcal{A}, \varphi)$ is the set $\{\varphi(a_{i_1}a_{i_2}\cdots a_{i_k}) \mid i_1, i_2, \ldots, i_k \in I\}$, this generalizes the notion of k-th moment of an algebraic random variable. Additionally, a moment $\varphi(a_{i_1}a_{i_2}\cdots a_{i_k})$ is called *mixed* if at least two of the indexes $i_1, i_2, \ldots, i_k$ are distinct, and it is called *individual*, otherwise.

It is beneficial, and sometimes even fundamental, to link algebraic random variables to probability measures associated with the corresponding algebraic distributions. Thus, given a normal random variable a in a $*$-probability space $(\mathcal{A}, \varphi)$, we say that a has an *analytic distribution* if there is a measure ν on the set of complex numbers $\mathbb{C}$ so that

$$\varphi(a^k(a^*)^l) = \int_{\mathbb{C}} z^k \overline{z}^l d\nu(z)$$

for all integers $k, l \geq 0$. Note that if a is self-adjoint with analytic distribution ν, then the

support of ν must be a subset of $\mathbb{R}$, so we consider ν as a measure on $\mathbb{R}$ and write

$$\varphi(a^k) = \int_{\mathbb{R}} t^k d\nu(t).$$

Usually, an algebraic random variable with analytic distribution inherits the analytic distribution's name if there is one. For instance, a self-adjoint random variable a in $*$-probability space $(\mathcal{A}, \varphi)$ is called *semi-circular* if it satisfies

$$\varphi(a^k) = \frac{1}{2\pi} \int_{-2}^{2} t^k \sqrt{4 - t^2} dt \qquad \forall\ k \geq 0$$

since the probability density function $f(t) = \frac{\sqrt{4-t^2}}{2\pi}$, if $-2 \leq t \leq 2$, and $f(t) = 0$, otherwise, gives the so-called semi-circular distribution on the real line.

Another example of an algebraic random variable with analytic distribution worth mentioning is the one related to the normalized Lebesgue measure on the unit circle $\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}$, also called *Haar measure*. We say that a unitary random variable u in $*$-probability space $(\mathcal{A}, \varphi)$ is *Haar unitary* if it satisfies

$$\varphi(u^k (u^*)^l) = \int_{\mathbb{T}} z^k \overline{z}^l dz = \frac{1}{2\pi} \int_0^{2\pi} e^{i(k-l)t} dt$$

for all integers $k, l \geq 0$. Note that the random variable u is Haar unitary if and only if

$$\varphi(u^k (u^*)^l) = \begin{cases} 1, & \text{if } k = l, \\ 0, & \text{otherwise.} \end{cases}$$

Convergence in distribution of first order

Once a notion of distribution for algebraic random variables is established, a corresponding notion of convergence in distribution emerge.

Definition 3.1.4. Let $\{a_{N,i}\}_{i\in I}$ be a family of random variables in an algebraic probability space $(\mathcal{A}_N, \varphi_N)$ for each integer $N \geq 1$. We say that the sequence of families of random variables $\{\{a_{N,i}\}_{i\in I}\}_{N=1}^{\infty}$ *converge in distribution* to another family $\{a_i\}_{i\in I}$ of random variables in some algebraic probability space $(\mathcal{A}, \varphi)$ if for every polynomial $\mathrm{p} \in \mathbb{C}\langle \mathrm{x}_i \mid i \in I\rangle$ we have $\mu(\mathrm{p}) = \lim_{N\to\infty} \mu_N(\mathrm{p})$ where $\mu : \mathbb{C}\langle \mathrm{x}_i \mid i \in I\rangle \to \mathbb{C}$ and $\mu_N : \mathbb{C}\langle \mathrm{x}_i \mid i \in I\rangle \to \mathbb{C}$ are the joint algebraic distributions of $\{a_i\}_{i\in I}$ and $\{a_{N,i}\}_{i\in I}$, respectively.

Notice a concrete algebraic probability space $(\mathcal{A}, \varphi)$, and hence, the random variables $\{a_i\}_{i\in I}$, is not crucial for the convergence in distribution of the sequence $\{\{a_{N,i}\}_{i\in I}\}_{N=1}^{\infty}$ in the previous definition. Indeed, let $\mathrm{ev}_N : \mathbb{C}\langle \mathrm{x}_i \mid i \in I\rangle \to \mathcal{A}_N$ be the unital algebraic homomorphism such that $\mathrm{ev}_N(\mathrm{x}_i) = a_{N,i}$ for ever $i \in I$ and note the joint algebraic distribution of $\{a_{N,i}\}_{i\in I}$ satisfies $\mu_N = \varphi_N \circ \mathrm{ev}_N$, i.e., the following diagram

$$\begin{array}{ccc} \mathcal{A}_N & \xrightarrow{\varphi_N} & \mathbb{C} \\ {\scriptstyle \mathrm{ev}_N}\uparrow & \nearrow_{\mu_N} & \\ \mathbb{C}\langle \mathrm{x}_i \mid i \in I\rangle & & \end{array}$$

commutes. Thus, $\lim_{N\to\infty} \varphi_N(a_{N,i_1} a_{N,i_2} \cdots a_{N,i_m})$ exists for all integers $m \geq 1$ and indexes $i_1, i_2, \ldots, i_m \in I$ if and only if $\lim_{N\to\infty} \mu_N(\mathrm{p})$ exists for every polynomial $\mathrm{p} \in \mathbb{C}\langle \mathrm{x}_i \mid i \in I\rangle$, but the latter condition implies $\{\{a_{N,i}\}_{i\in I}\}_{N=1}^{\infty}$ converges in distribution to $\{\mathrm{x}_i\}_{i\in I}$ viewed as a family of random variables in the probability space $(\mathbb{C}\langle \mathrm{x}_i \mid i \in I\rangle, \lim_{N\to\infty} \mu_N)$. Therefore, the sequence $\{\{a_{N,i}\}_{i\in I}\}_{N=1}^{\infty}$ converges in distribution if and only if $\{\mu_N\}_{N=1}^{\infty}$ is a point-wise convergent sequence of unital functionals on $\mathbb{C}\langle \mathrm{x}_i \mid i \in I\rangle$.

In view of the above, it becomes imperative to investigate the point-wise convergence of sequences $\{\mu_N\}_{N=1}^{\infty}$ of linear functionals $\mu_N : \mathcal{A} \to \mathbb{C}$, in particular, if the algebra $\mathcal{A}$ is generated by a family of sub-algebras $\{\mathcal{A}_i\}_{i\in I}$, which is the case when $\mathcal{A}$ is the algebra of non-commutative polynomials $\mathbb{C}\langle \mathrm{x}_i \mid i \in I\rangle$ and each $\mathcal{A}_i$ is the algebra of polynomials $\mathbb{C}[\mathrm{x}_i]$.

Proposition 3.1.5. Let $\mathcal{A}$ be an algebra over $\mathbb{C}$ and let $\mathcal{A}_i \subset \mathcal{A}$ be a sub-algebra for each $i \in I$ so that the family of sub-algebras $\{\mathcal{A}_i\}_{i\in I}$ generate the algebra $\mathcal{A}$. Suppose $\mu_N : \mathcal{A} \to \mathbb{C}$ is linear functional for each $N \geq 1$ such that $\mu[\mathrm{p}] := \lim_{N\to\infty} \mu_N[\mathrm{p}]$ exists for every $\mathrm{p} \in \mathcal{A}_i$ and every $i \in I$. Then $\lim_{N\to\infty} \mu_N[\mathrm{p}]$ exists for every $\mathrm{p} \in \mathcal{A}$ if and only if any of the following conditions hold:

(a) $\lim_{N\to\infty} \mu_N[(\mathrm{p}_1 - \mu[\mathrm{p}_1])(\mathrm{p}_2 - \mu[\mathrm{p}_2])\cdots(\mathrm{p}_m - \mu[\mathrm{p}_m])]$ exists whenever $\mathrm{p}_k \in \mathcal{A}_{i_k}$ with $i_1 \neq i_2, i_2 \neq i_3, \ldots, i_{m-1} \neq i_m$

(b) $\lim_{N\to\infty} \mu_N[(\mathrm{p}_1 - \mu_N[\mathrm{p}_1])(\mathrm{p}_2 - \mu_N[\mathrm{p}_2])\cdots(\mathrm{p}_m - \mu_N[\mathrm{p}_m])]$ exists whenever $\mathrm{p}_k \in \mathcal{A}_{i_k}$ with $i_1 \neq i_2, i_2 \neq i_3, \ldots, i_{m-1} \neq i_m$

Proof. Let J be the set of all positive integers I satisfying the following property: if $\mathrm{p}_1 \in \mathcal{A}_{i_1}$, $\mathrm{p}_2 \in \mathcal{A}_{i_2}$, …, $\mathrm{p}_m \in \mathcal{A}_{i_m}$ with $i_1, i_2, \ldots, i_m \in I$ and $i_1 \neq i_2, i_2 \neq i_3, \ldots, i_{m-1} \neq i_m$, then $\lim_{N\to\infty} \mu_N[\mathrm{p}_1\mathrm{p}_2\cdots\mathrm{p}_m]$ exists. Since the algebras $\mathcal{A}_i$ with $i \in I$ generate $\mathcal{A}$ and each μ_N is linear, then $\lim_{N\to\infty} \mu_N[\mathrm{p}]$ exists for every $\mathrm{p} \in \mathcal{A}$ if the set J contains every positive integer. Now, by hypothesis, 1 belongs to J, so let us assume $1, 2, \ldots, m-1$ belong to J and suppose $\mathrm{p}_1, \mathrm{p}_2, \ldots, \mathrm{p}_m$ are as above. Thus, if $S = \{k_1 < k_2 < \cdots < k_{|S|}\}$ is a strict subset of $[m]$, the limits

$$\lim_{N\to\infty} (-1)^{|S^c|} \prod_{k\in S^c} \mu_N[\mathrm{p}_k]\, \mu_N\left[\vec{\prod_{k\in S}} \mathrm{p}_k\right] \qquad \text{and} \qquad \lim_{N\to\infty} (-1)^{|S^c|} \prod_{k\in S^c} \mu[\mathrm{p}_k]\, \mu_N\left[\vec{\prod_{k\in S}} \mathrm{p}_k\right],$$

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

$$\mu_N\left[(\mathrm{p}_1-\mu_N\left[\mathrm{p}_1\right])\cdots(\mathrm{p}_m-\mu_N\left[\mathrm{p}_m\right])\right]=\mu_N\left[\mathrm{p}_1\cdots\mathrm{p}_m\right]+\sum_{S\subsetneq[m]}(-1)^{|S^c|}\prod_{k\in S^c}\mu_N\left[\mathrm{p}_k\right]\mu_N\left[\vec{\prod_{k\in S}}\mathrm{p}_k\right]$$

implies $\lim_{N\to\infty}\mu_N\left[\mathrm{p}_1\cdots\mathrm{p}_m\right]$ exists. And therefore, J contains every positive integer by induction on I. Similarly, if (a) holds, then $\lim_{N\to\infty}\mu_N\left[\mathrm{p}_1\cdots\mathrm{p}_m\right]$ exists, and hence J contains every positive integer, since each $\mu_N\left[\mathrm{p}_k\right]$ in the equality above can be replaced by $\mu\left[\mathrm{p}_k\right]$.

Let us now show that (a) and (b) are equivalent. Suppose $\mathrm{p}_1\in\mathcal{A}_{i_1},\mathrm{p}_2\in\mathcal{A}_{i_2},\ldots,\mathrm{p}_m\in\mathcal{A}_{i_m}$ with $i_1,i_2,\ldots,i_m\in I$ and $i_1\neq i_2,i_2\neq i_3,\ldots,i_{m-1}\neq i_m$ and take $\mathrm{q}_k=\mathrm{p}_k-\mu\left[\mathrm{p}_k\right]$ for $k=1,2,\ldots,m$. We then have $\lim_{N\to\infty}\mu_N\left[\mathrm{q}_k\right]=0$ and the equality

$$\begin{aligned}\mu_N\left[(\mathrm{p}_1-\mu_N\left[\mathrm{p}_1\right])\cdots(\mathrm{p}_m-\mu_N\left[\mathrm{p}_m\right])\right]=&\mu_N\left[\mathrm{q}_1\cdots\mathrm{q}_m\right]+\sum_{S\subsetneq[m]}(-1)^{|S^c|}\prod_{k\in S^c}\mu_N\left[\mathrm{q}_k\right]\mu_N\left[\vec{\prod_{k\in S}}\mathrm{q}_k\right]\\=&\mu_N\left[(\mathrm{q}_1-\mu_N\left[\mathrm{q}_1\right])\cdots(\mathrm{q}_m-\mu_N\left[\mathrm{q}_m\right])\right]\end{aligned}$$

Thus, if condition (a) holds, then $\lim_{N\to\infty}\mu_N\left[\mathrm{p}\right]$ exists for every $\mathrm{p}\in\mathcal{A}$, and hence

$$0=\lim_{N\to\infty}(-1)^{|S^c|}\prod_{k\in S^c}\mu_N\left[\mathrm{q}_k\right]\mu_N\left[\vec{\prod_{k\in S}}\mathrm{q}_k\right]\qquad\forall\ S\subsetneq[m];$$

additionally, we have $\lim_{N\to\infty}\mu_N\left[(\mathrm{p}_1-\mu\left[\mathrm{p}_1\right])\cdots(\mathrm{p}_m-\mu\left[\mathrm{p}_m\right])\right]=\lim_{N\to\infty}\mu_N\left[\mathrm{q}_1\cdots\mathrm{q}_m\right]$ exists. Thus, we obtain the limit $\lim_{N\to\infty}\mu_N\left[(\mathrm{p}_1-\mu_N\left[\mathrm{p}_1\right])\cdots(\mathrm{p}_m-\mu_N\left[\mathrm{p}_m\right])\right]$ also exists. This shows that (a) implies (b). A similar proof shows that (b) implies (a). □

3.2 Free independence

Before we give the definition of free independence, it is convenient to examine how the notion of independence from classical probability theory translates to the framework of algebraic probability spaces, so we can identify some of the similarities and differences between these two notions of independences.

Suppose we are given two complex-valued random variables $x, y : \Omega \to \mathbb{C}$ on a probability space $(\Omega, \mathcal{F}, P)$. Recall that x and y are said to be *independent* if for any pair of open sets $\mathrm{U}, \mathrm{V} \subset \mathbb{C}$ we have

$$P\left(x^{-1}(U) \cap y^{-1}(V)\right) = P\left(x^{-1}(U)\right) P\left(y^{-1}(V)\right). \tag{3.1}$$

The notion of independence from classical probability theory can be stated as *the joint distribution of independent random variables is the product of the individual distributions.* Now, if we think of x and y as algebraic random variables in $(L^{\infty-}(\Omega, \mathcal{F}, P), \mathbb{E}[\,\cdot\,])$, then their algebraic joint distribution is determined by the map

$$z_1 z_2 \cdots z_m \;\mapsto\; \mathbb{E}\left[z_1 z_2 \cdots z_m\right] \tag{3.2}$$

where $m \geq 1$ and $z_1, z_2, \ldots, z_m \in \{x, y\}$, and hence, the independence of x and y given by (3.1) translates to the framework of algebraic probability spaces as

$$\mathbb{E}\left[z_1 z_2 \cdots z_m\right] = \mathbb{E}\left[x^k\right] \mathbb{E}\left[y^l\right] \tag{3.3}$$

whenever x and y appear exactly k and l times, respectively, in the expression $z_1 z_2 \cdots z_m$. We can consider an arbitrary number of random variables, say $x_i : \Omega \to \mathbb{C}$ is a complex-valued

random variable for each index $i \in I$, and their algebraic joint distribution is also determined by the map (3.2), but now each z_k belongs to the set $\{x_i \mid i \in I\}$, moreover, their mutual classical independence translates to the framework of algebraic probability spaces as

$$\mathbb{E}\left[z_1 z_2 \cdots z_m\right] = \prod_{B \in \pi} \mathbb{E}\left[\prod_{k \in B} z_k\right] = \prod_{B \in \pi} \mathbb{E}\left[\prod_{k \in B} x_{i_k}\right] \tag{3.4}$$

whenever $z_1 z_2 \cdots z_m = x_{i_1} x_{i_2} \cdots x_{i_m}$ with $i_1, i_2, \ldots, i_m \in I$ and $\pi = \ker(\mathbf{i})$, using the kernel notation from Section 2.2. For instance, if $I = [4]$ and $z_1 z_2 z_3 z_4 z_5 = x_4 x_1 x_3 x_1 x_2$, then (3.4) gives $\mathbb{E}\left[z_1 z_2 \cdots z_5\right] = \mathbb{E}\left[z_1\right]\mathbb{E}\left[z_2 z_4\right]\mathbb{E}\left[z_3\right]\mathbb{E}\left[z_5\right] = \mathbb{E}\left[x_4\right]\mathbb{E}\left[x_1 x_1\right]\mathbb{E}\left[x_3\right]\mathbb{E}\left[x_2\right]$. The relation (3.4) holds even if each x_i is replaced with a family $\{x_{i,j}\}_{j \in J_i}$, we would only have to consider x_{i_k, j_k} instead of x_{i_k}, since random variables in $L^{\infty-}(\Omega, \mathcal{F}, P)$ always commute, but commutativity does not hold true in arbitrary algebraic probability spaces. Nonetheless, the relation (3.4) can be used to produce a notion of classical independence in the framework of algebraic probability spaces that considers random variables that do not necessarily commute.

Definition 3.2.1. Let $(\mathcal{A}, \varphi)$ be an algebraic probability space. A collection $\{\mathcal{A}_i\}_{i \in I}$ of unital sub-algebras of $\mathcal{A}$ is *classically independent*, also called *tensor independent*, with respect to φ if for all integers $m \geq 0$ and random variables $a_1 \in \mathcal{A}_{i_1}$, $a_2 \in \mathcal{A}_{i_2}$, …, and $a_m \in \mathcal{A}_{i_m}$ with $i_1, i_2, \ldots, i_m \in I$ satisfying $\ker(\mathbf{i}) = \pi$, we have

$$\varphi(a_1 a_2 \cdots a_m) = \prod_{B \in \pi} \varphi\left(\vec{\prod_{k \in B}} a_k\right). \tag{3.5}$$

The product $\vec{\prod}_{k \in B} a_k$ in the previous definition is the ordered product of the random variables a_k with respect to k, namely, we denote by $\vec{\prod}_{k \in B} a_k$ the product $a_{k_1} a_{k_2} \cdots a_{k_n}$

provided $B = \{k_1 < k_2 < \cdots < k_n\}$. Thus, the only difference between the relations (3.4) and (3.5) is that the latter specifies the order in which the random variables a_k are to be multiplied to take into account their possibly non-commutativity. Now, defining tensor independence for collections of sub-algebras, instead of defining it merely for collections of random variables, is the appropriate way of doing so in an algebraic setting, the independence of random variables in the sense of (3.1) is such a strong condition that it implies the independence of the algebras generated by the corresponding random variables, i.e., for any polynomials $\mathrm{p}, \mathrm{q} \in \mathbb{C}[\mathrm{x}]$ we have that $\mathrm{p}(x)$ and $\mathrm{q}(y)$ are independent provided (3.1) holds. Consequently, a collection of families of random variables $\{\{a_{i,j}\}_{j\in J_i}\}_{i\in I}$ in an algebraic probability space $(\mathcal{A}, \varphi)$ is said to be *tensor independent* if the collection of sub-algebras $\{\mathcal{A}_i\}_{i\in I}$ is tensor independent where each $\mathcal{A}_i$ is the unital sub-algebra generated by $\{a_{i,j}\}_{j\in J_i}$.

It is fundamental to the theory of probability that we are able to construct a "product space" containing independent copies of any given collection of algebraic probability spaces. This product space should be the algebraic analogue of constructing product measurable spaces and product measures, and hence, it would be what would allow us to talk about independent and identically distributed random variables, or, more generally, independent random variables with predetermined distributions.

More specifically, suppose we are given two algebraic probability spaces $(\mathcal{A}_1, \varphi_1)$ and $(\mathcal{A}_2, \varphi_2)$, which might or might not be the same space. We would like to find an algebraic probability space $(\mathcal{A}, \varphi)$ and injective unital algebra homomorphisms $\psi_1 : \mathcal{A}_1 \to \mathcal{A}$ and $\psi_2 : \mathcal{A}_2 \to \mathcal{A}$ so that the diagram

$$\begin{array}{ccccc} \mathcal{A}_1 & \xrightarrow{\psi_1} & \mathcal{A} & \xleftarrow{\psi_2} & \mathcal{A}_2 \\ & \searrow^{\varphi_1} & \downarrow{\scriptstyle \varphi} & \swarrow_{\varphi_2} & \\ & & \mathbb{C} & & \end{array} \tag{3.6}$$

commutes, i.e., $\varphi_1 = \varphi \circ \psi_1$ and $\varphi_2 = \varphi \circ \psi_2$, and the sub-algebras $\psi_1(\mathcal{A}_1)$ and $\psi_2(\mathcal{A}_2)$ are independent with respect to φ. Note that given an algebra $\mathcal{A}$ and homomorphisms $\psi_i : \mathcal{A}_i \to \mathcal{A}$, the sub-algebras $\psi_1(\mathcal{A}_1)$ and $\psi_2(\mathcal{A}_2)$ are tensor independent with respect to a linear functional $\varphi : \mathcal{A} \to \mathbb{C}$ that makes the diagram (3.6) commute only if

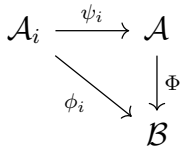
$$\varphi(b_1 b_2 \cdots b_m) = \prod_{B \in \pi} \varphi \left(\vec{\prod_{k \in B}} \psi_{i_k}(a_k) \right) = \prod_{B \in \pi} \varphi \circ \psi_{i_B} \left(\vec{\prod_{k \in B}} a_k \right) = \prod_{B \in \pi} \varphi_{i_B} \left(\vec{\prod_{k \in B}} a_k \right) \tag{3.7}$$

whenever $b_k = \psi_{i_k}(a_k)$ with $a_k \in \mathcal{A}_{i_k}$, the indexes $i_1, i_2, \ldots, i_m \in \{1, 2\}$ satisfy $\pi = \ker(\mathbf{i})$, and $i_B := i_k$ provided $k \in B \in \ker(\mathbf{i})$. Therefore, finding a probability space $(\mathcal{A}, \varphi)$ containing tensor independent copies of $(\mathcal{A}_1, \varphi_1)$ and $(\mathcal{A}_2, \varphi_2)$ relies primarily on choosing a suitable algebra $\mathcal{A}$ and the corresponding algebra homomorphisms $\psi_i : \mathcal{A}_i \to \mathcal{A}$.

Now, for illustration, let us assume $\mathcal{A}_i = \mathbb{C}[\mathrm{x}_i]$ the algebra of commutative polynomials on the indeterminate x_i, so every unital linear functional $\varphi_i : \mathcal{A}_i \to \mathbb{C}$ is determined by a corresponding moment sequence $\{\varphi_i(\mathrm{x}_i^k)\}_{k=1}^{\infty}$. We can then easily think of various candidates for a unital algebra $\mathcal{A}$ that makes the diagram (3.6) commute. For instance, we could take $\mathcal{A} = \mathbb{C}[\mathrm{x}_1, \mathrm{x}_2]$, the algebra of commutative polynomials on the indeterminates x_1 and x_2, or $\mathcal{A} = \mathbb{C}\langle \mathrm{x}_1, \mathrm{x}_2 \rangle$, the algebra of non-commutative polynomials on the indeterminates x_1 and x_2, together with the canonical algebra homomorphisms $\psi_i : \mathcal{A}_i \to \mathcal{A}$ defined by $\psi_i(\mathrm{x}_i) = \mathrm{x}_i$. Although both choices above for $\mathcal{A}$ are plausible, it is the non-commutative setting the one that ultimately offers enough room for other independences to emerge, so we resolve to take the algebra $\mathcal{A}$ as the free product of $\mathcal{A}_1 = \mathbb{C}[\mathrm{x}_1]$ and $\mathcal{A}_2 = \mathbb{C}[\mathrm{x}_2]$ with identification of the identities, namely, $\mathcal{A} = \mathbb{C}\langle \mathrm{x}_1, \mathrm{x}_2 \rangle$.

More generally, a unital algebra $\mathcal{A}$ is said to be the *free product with identification of the identity* of a collection of unital algebras $\{\mathcal{A}_i\}_{i \in I}$ if there are unital algebra homomorphism $\psi_i : \mathcal{A}_i \to \mathcal{A}$ satisfying the following universal property: *if $\mathcal{B}$ is any unital algebra and*

$\phi_i : \mathcal{A}_i \to \mathcal{B}$ is a unital algebra homomorphism for each $i \in I$, then there is a unique unital algebra homomorphism $\Phi : \mathcal{A} \to \mathcal{B}$ so that $\phi_i = \Phi \circ \psi_i$ for all $i \in I$, i.e., the following diagram commutes:



Due to its defining universal property, the free product with identification of the identity of a collection of unital algebras $\{\mathcal{A}_i\}_{i\in I}$ is unique up to isomorphism provided it exists, and, if that is the case, we denote it by $*_{i\in I}\mathcal{A}_i$. Roughly speaking, the free product $*_{i\in I}\mathcal{A}_i$ is the smallest algebra containing copies of each $\mathcal{A}_i$ so that elements from distinct algebras do not commute except for the multiplicative identities $1_{\mathcal{A}_i}$, which are to be considered the same element. It is not hard to show that $\mathbb{C}\langle \mathrm{x}_1, \mathrm{x}_2\rangle$ is indeed the free product with identification of the identities of $\mathbb{C}[\mathrm{x}_1]$ and $\mathbb{C}[\mathrm{x}_2]$.

Let us now return to the particular case of finding a probability space $(\mathcal{A}, \varphi)$ containing tensor independent copies of $(\mathcal{A}_1, \varphi_1)$ and $(\mathcal{A}_2, \varphi_2)$ when $\mathcal{A}_1 = \mathbb{C}[\mathrm{x}_1]$ and $\mathcal{A}_2 = \mathbb{C}[\mathrm{x}_2]$. We have already resolved to take $\mathcal{A} = \mathcal{A}_1 * \mathcal{A}_2 = \mathbb{C}\langle \mathrm{x}_1, \mathrm{x}_2\rangle$, together with the algebra homomorphisms $\psi_i : \mathcal{A}_i \to \mathcal{A}$ defined by $\psi_i(\mathrm{x}_i) = \mathrm{x}_i$, since the non-commutative setting offers great generality. Strictly speaking, the algebra $\mathcal{A}$ contains copies of $\mathcal{A}_1$ and $\mathcal{A}_2$ via the homomorphisms $\psi_i : \mathcal{A}_i \to \mathcal{A}$, however, there is no harm if we think of $\mathcal{A}_1$ and $\mathcal{A}_2$ simply as unital sub-algebras of $\mathcal{A}$. And thus, it remains to define a linear functional $\varphi : \mathcal{A} \to \mathbb{C}$ under which $\mathcal{A}_1$ and $\mathcal{A}_2$ are tensor independent and so that $\varphi|_{\mathcal{A}_i} = \varphi_i$ for $i = 1, 2$. To do so, we just need to define the linear functional $\varphi : \mathbb{C}\langle \mathrm{x}_1, \mathrm{x}_2\rangle \to \mathbb{C}$ on basis elements of the form $\mathrm{x}_{i_1}\mathrm{x}_{i_2}\cdots\mathrm{x}_{i_m}$ with $i_k \in \{1, 2\}$ and abide by the relation (3.7). For instance, if we consider $\mathrm{x}_{i_1}\mathrm{x}_{i_2}\mathrm{x}_{i_3}\mathrm{x}_{i_4} = \mathrm{x}_1\mathrm{x}_2\mathrm{x}_1\mathrm{x}_2$, which is a basis element of $\mathbb{C}\langle \mathrm{x}_1, \mathrm{x}_2\rangle$, then $\ker(\mathbf{i}) = \{\{1, 3\}, \{2, 4\}\}$ since $i_1 = i_3 = 1$ and $i_2 = i_4 = 2$, and hence, the relation (3.7) forces $\varphi(\mathrm{x}_{i_1}\mathrm{x}_{i_2}\mathrm{x}_{i_3}\mathrm{x}_{i_4})$ to be

given by

$$\varphi(\mathrm{x}_{i_1}\mathrm{x}_{i_2}\mathrm{x}_{i_3}\mathrm{x}_{i_4}) = \varphi_1(\mathrm{x}_{i_1}\mathrm{x}_{i_3})\varphi_2(\mathrm{x}_{i_2}\mathrm{x}_{i_4}) = \varphi_1(\mathrm{x}_1^2)\varphi_2(\mathrm{x}_2^2). \tag{3.8}$$

The general case is conceptually not different. If $(\mathcal{A}_i, \varphi_i)$ is an algebraic probability space for each $i \in I$, then the probability space $(\mathcal{A}, \varphi)$ where $\mathcal{A}$ is the free product $*_{i\in I}\mathcal{A}_i$ and φ is determined by (3.7) contains tensor independent copies of each $(\mathcal{A}_i, \varphi_i)$.

So far, in this section, we have examined how the notion of independence from classical probability translates to the framework of algebraic probability spaces, where it is called tensor independence, and how we can construct product spaces containing tensor independent copies of any given collection of algebraic probability spaces. In the algebraic framework, a notion of independence should be understood as a set of universal rules to compute mixed moments out of individual ones, for tensor independence such universal rules are encapsulated in (3.5) and (3.7) and exemplified in (3.8). Hence, it is natural to ask if the relation (3.7) can be replaced with some other relation that gives rise to a distinct notion of independence. An answer to this question is given in [19] under the requirement that mixed moments be expressed as "linear combinations" of "lower degree" individual moments.

In [19], each notion of independence is linked to a collection of coefficients $\lambda(\pi, \theta)$ where π and θ are partitions in $P(m)$ satisfying $\pi \leq \theta$. Essentially, if we are given a collection $\{(\mathcal{A}_i, \varphi_i)\}_{i\in I}$ of algebraic probability spaces, the coefficients $\lambda(\pi, \theta)$ are used to define a unital linear functional $\varphi : *_{i\in I}\mathcal{A} \to \mathbb{C}$ under which $\{\mathcal{A}_i\}_{i\in I}$, viewed as a collection of unital sub-algebras of the free product $*_{i\in I}\mathcal{A}$, is independent. More specifically, if we take indexes $i_1, i_2, \ldots, i_m \in I$ and random variables $a_1 \in \mathcal{A}_{i_1}, a_2 \in \mathcal{A}_{i_2}, \ldots, a_m \in \mathcal{A}_{i_m}$, then the linear

functional φ evaluated at $a_1a_2\cdots a_m \in *_{i\in I}\mathcal{A}$ must be given by

$$\varphi(a_1a_2\cdots a_m) = \sum_{\substack{\pi\in P(m)\\ \pi\leq\theta}} \lambda(\pi,\theta)\prod_{B\in\pi}\varphi_{i_B}\left(\prod_{k\in B}^{\rightarrow} a_k\right) \tag{3.9}$$

where $\ker(\mathbf{i}) = \theta$ and $i_B := i_k$ provided $k \in B \in \ker(\mathbf{i})$. For instance, suppose $a_1, a_3 \in \mathcal{A}_1$ and $a_2, a_4 \in \mathcal{A}_2$, so we obtain $(i_1, i_2, i_3, i_4) = (1, 2, 1, 2)$, and hence, $\theta = \ker(\mathbf{i}) = \{\{1, 3\}, \{2, 4\}\}$. Thus, since we have

$$\{\pi \in P(4) \mid \pi \leq \ker(\mathbf{i})\} = \left\{ \begin{array}{ccc} \pi_1 = \{\{1,3\},\{2,4\}\} & , & \pi_2 = \{\{1,3\},\{2\},\{4\}\} \\ \pi_3 = \{\{1\},\{3\},\{2,4\}\} & , & \pi_4 = \{\{1\},\{3\},\{2\},\{4\}\} \end{array} \right\},$$

the relation (3.9) produces

$$\begin{aligned}\varphi(a_1a_2a_3a_4) =& \lambda(\pi_1,\theta)\varphi_1(a_1a_3)\varphi_2(a_2a_4) + \lambda(\pi_2,\theta)\varphi_1(a_1a_3)\varphi_2(a_2)\varphi_2(a_4) + \\ & \lambda(\pi_3,\theta)\varphi_1(a_1)\varphi_1(a_3)\varphi_2(a_2a_4) + \lambda(\pi_4,\theta)\varphi_1(a_1)\varphi_1(a_3)\varphi_2(a_2)\varphi_2(a_4).\end{aligned} \tag{3.10}$$

For tensor independence, the collection of coefficients $\lambda(\pi, \theta)$ is given by

$$\lambda(\pi,\theta) = \left\{ \begin{array}{ll} 1, & \text{if } \pi = \theta, \\ 0, & \text{otherwise.} \end{array} \right. \tag{3.11}$$

The coefficients $\lambda(\pi, \theta)$ are universal in the sense that they do not depend at all on the family $\{(\mathcal{A}_i, \varphi_i)\}_{i\in I}$. It is shown in [19] that if we require notions of independence to be commutative and associative, meaning that they are independent from re-indexing and grouping of the probability spaces $(\mathcal{A}_i, \varphi_i)$, respecively, then there exists only one more notion of independence, called *free independence*; more concretely, other than (3.11), there exists only

one more collection of coefficients $\lambda(\pi, \theta)$ so that (3.9) always gives a well-defined unital functional.

Definition 3.2.2. Let $(\mathcal{A}, \varphi)$ be an algebraicraic probability space. A family $\{\mathcal{A}_i\}_{i\in I}$ of unital sub-algebras of $\mathcal{A}$ is *freely independent*, or simply *free*, with respect to φ if for all positive integers $m \geq 1$, indexes $i_1, i_2, \ldots, i_m \in I$ with $i_1 \neq i_2, \ldots, i_{m-1} \neq i_m$, and random variables $a_k \in \mathcal{A}_{i_k}$ with $\varphi(a_k) = 0$ for $1 \leq k \leq m$ we have $\varphi(a_1 a_2 \cdots a_m) = 0$.

Similar to tensor independence, a collection of families of random variables $\{\{a_{i,j}\}_{j\in J_i}\}_{i\in I}$ in an algebraic probability space $(\mathcal{A}, \varphi)$ is said to be *free independent* if the collection of sub-algebras $\{\mathcal{A}_i\}_{i\in I}$ is free independent where each $\mathcal{A}_i$ is the unital sub-algebra generated by $\{a_{i,j}\}_{j\in J_i}$.

One might rightfully complain that tensor independence and free independence have been defined in different ways: while tensor independence relies on explicit rules for computing mixed moments out of individual ones, combining (3.9) and (3.11) to obtain (3.5), free independence is determined by the *free independence condition*, namely, $\varphi(a_1 a_2 \cdots a_m) = 0$ whenever $a_k \in \mathcal{A}_{i_k}$ with $\varphi(a_k) = 0$ for $k = 1, 2, \ldots, m$ and the indexes $i_1, i_2, \ldots, i_m \in I$ satisfy $i_1 \neq i_2, \ldots, i_{m-1} \neq i_m$. The reason behind such difference is that the coefficients $\lambda(\pi, \theta)$ coupled to free independence are not as straightforward as the ones for tensor independence and the free independence condition actually defines the corresponding set of rules for computing mixed moments.

Let us examine what the free independence condition means for the computation of mixed moments by looking at a few examples. Suppose $\mathcal{A}_1$ and $\mathcal{A}_2$ are freely independent unital sub-algebras of an algebraic probability space $(\mathcal{A}, \varphi)$. The free independence condition implies the following three rules for mixed moments:

(i) $\varphi(b_1 c_1) = \varphi(b_1)\varphi(c_1)$

(ii) $\varphi(b_1c_1b_2) = \varphi(b_1b_2)\varphi(c_1)$

(iii) $\varphi(b_1c_1b_2c_2) = \varphi(b_1b_2)\varphi(c_1)\varphi(c_2) + \varphi(b_1)\varphi(b_2)\varphi(c_1c_2) - \varphi(b_1)\varphi(b_2)\varphi(c_1)\varphi(c_2)$

for all random variables $b_1, b_2 \in \mathcal{A}_1$ and $c_1, c_2 \in \mathcal{A}_2$. Notice that (i) and (ii) are the same relations we would have if $\mathcal{A}_1$ and $\mathcal{A}_2$ were tensor independent but (iii) is not, if $\mathcal{A}_1$ and $\mathcal{A}_2$ were tensor independent we would have $\varphi(b_1c_1b_2c_2) = \varphi(b_1b_2)\varphi(c_1c_2)$. We describe how (i)-(iii) are obtained next. By the free independence condition, we have

$$0 = \varphi(a_1a_2) = \varphi(a_1a_2a_3) = \varphi(a_1a_2a_3a_4)$$

where $a_{2k-1} = b_k - \varphi(b_k)1_{\mathcal{A}} \in \mathcal{A}_1$ and $a_{2k} = c_k - \varphi(c_k)1_{\mathcal{A}} \in \mathcal{A}_2$. But, we also have

$$a_1a_2 = b_1c_1 - b_1\varphi(c_1) - \varphi(b_1)c_1 + \varphi(b_1)\varphi(c_1)1_{\mathcal{A}}$$

and hence, by linearity of φ, we obtain

$$\varphi(a_1a_2) = \varphi(b_1c_1) - \varphi(b_1)\varphi(c_1) - \varphi(b_1)\varphi(c_1) + \varphi(b_1)\varphi(c_1) = 0.$$

Thus, we get $\varphi(b_1c_1) = \varphi(b_1)\varphi(c_1)$. Similarly, since we have

$$\begin{aligned} a_1a_2a_3 =& b_1c_1b_2 - b_1\varphi(c_1)b_2 - \varphi(b_1)c_1b_2 + \varphi(b_1)\varphi(c_1)b_2 \\ & - b_1c_1\varphi(b_2) + b_1\varphi(c_1)\varphi(b_2) + \varphi(b_1)c_1\varphi(b_2) - \varphi(b_1)\varphi(c_1)\varphi(b_2)1_{\mathcal{A}}, \end{aligned}$$

the freeness condition, the linearity of φ, and (i) above imply $\varphi(b_1c_1b_2) = \varphi(b_1b_2)\varphi(c_1)$.

Finally, (iii) follows from the freeness condition, the linearity of φ, (i), (ii), and the relation

$$\begin{aligned}
a_1a_2a_3a_4 = {} & b_1c_1b_2c_2 - b_1\varphi(c_1)b_2c_2 - \varphi(b_1)c_1b_2c_2 + \varphi(b_1)\varphi(c_1)b_2c_2 \\
& - b_1c_1\varphi(b_2)c_2 + b_1\varphi(c_1)\varphi(b_2)c_2 + \varphi(b_1)c_1\varphi(b_2)c_2 - \varphi(b_1)\varphi(c_1)\varphi(b_2)c_2 \\
& + b_1c_1b_2\varphi(c_2) - b_1\varphi(c_1)b_2\varphi(c_2) - \varphi(b_1)c_1b_2\varphi(c_2) + \varphi(b_1)\varphi(c_1)b_2\varphi(c_2) \\
& - b_1c_1\varphi(b_2)\varphi(c_2) + b_1\varphi(c_1)\varphi(b_2)\varphi(c_2) + \varphi(b_1)c_1\varphi(b_2)\varphi(c_2) - \varphi(b_1)\varphi(c_1)\varphi(b_2)\varphi(c_2)1_{\mathcal{A}}.
\end{aligned}$$

From the above, we can infer that free independence does determine a set of rules for computing mixed moments and such rules are derived recursively from the free independence condition.

Proposition 3.2.3. Let $(\mathcal{A}, \varphi)$ be an algebraic probability space and let $\{\mathcal{A}_i\}_{i\in I}$ be a family of unital sub-algebras of $\mathcal{A}$ be freely independent with respect to φ. If $\mathcal{A}$ is generated as an algebra by the family $\{\mathcal{A}_i\}_{i\in I}$, then φ is uniquely determined by the restrictions $\varphi|_{\mathcal{A}_i}$ and by the free independence condition.

To prove the previous proposition, since the algebra $\mathcal{A}$ is assumed to be generated by the family of sub-algebras $\{\mathcal{A}_i\}_{i\in I}$, it is enough to show that the following holds: *for any indexes $i_1, i_2, \ldots, i_m \in I$ and random variables $b_1 \in \mathcal{A}_{i_1}, b_2 \in \mathcal{A}_{i_2}, \ldots, b_m \in \mathcal{A}_{i_m}$, the value $\varphi(b_1b_2\cdots b_m)$ is uniquely determined by the restrictions $\varphi|_{\mathcal{A}_i}$ and by the free independence condition.* Suppose $i_1, i_2, \ldots, i_m$ and $b_1, b_2, \ldots, b_m$ are as above. Without loss of generality, we can assume $i_1 \neq i_2$, $i_2 \neq i_3$, ..., and $i_{m-1} \neq i_m$, otherwise, we recursively group b_k and b_{k+1} if $i_k = i_{k+1}$. Now, taking $a_k = b_k - \varphi(b_k)1_{\mathcal{A}}$ for $1 \leq k \leq m$, the free independence condition implies $\varphi(a_1a_2\cdots a_m) = 0$, but, we also have

$$a_1a_2\cdots a_m = b_1b_2\cdots b_m + \sum_{K\subsetneq[m]} (-1)^{m-|K|} \prod_{k\in[m]\setminus K} \varphi(b_k) \cdot \vec{\prod_{k\in K}} b_k$$

where $|K|$ denotes the cardinality of the set K. Thus, by linearity of φ, we obtain

$$\varphi(b_1 b_2 \cdots b_m) = -\sum_{K \subsetneq [m]} (-1)^{m-|K|} \prod_{k \in [m]\setminus K} \varphi(b_k) \cdot \varphi\left(\vec{\prod_{k\in K}} b_k\right) \tag{3.12}$$

By induction on $|K|$, each term in the sum in the left-hand side of (3.12) is uniquely determined by the restrictions $\varphi|_{\mathcal{A}_i}$ and by the free independence condition, and so is $\varphi(b_1 b_2 \cdots b_m)$.

Remark. Even though it is not evident from the definition of free independence, the free independence condition characterizes the product spaces containing free independent copies of any given collection of algebraic probability spaces. Indeed, suppose $(\mathcal{A}_i, \varphi_i)$ is an algebraic probability space for each $i \in I$. Since $\varphi_i : \mathcal{A}_i \to \mathbb{C}$ is a unital linear functional, each algebra $\mathcal{A}_i$ can be written as a direct sum of vector spaces

$$\mathcal{A}_i = \mathbb{C}1_{\mathcal{A}_i} \oplus \mathring{\mathcal{A}}_i$$

where $\mathring{\mathcal{A}}_i = \ker(\varphi_i) := \{a \in \mathcal{A}_i \mid \varphi_i(a) = 0\}$ and $\mathbb{C}1_{\mathcal{A}_i} = \{\lambda 1_{\mathcal{A}_i} \in \mathcal{A}_i \mid \lambda \in \mathbb{C}\}$. Moreover, it can be shown that the free product $*_{i\in I}\mathcal{A}_i$ exists and is given by

$$*_{i\in I}\mathcal{A}_i = \mathbb{C}1_{\mathcal{A}} \oplus \bigoplus_{m=1}^{\infty} \bigoplus_{\substack{i_1,i_2,\ldots,i_m \in I \\ i_1 \neq i_2,\ldots,i_{m-1}\neq i_m}} \mathring{\mathcal{A}}_{i_1} \otimes \mathring{\mathcal{A}}_{i_2} \otimes \cdots \otimes \mathring{\mathcal{A}}_{i_m}$$

with multiplication on tensors $a_1 \otimes a_2 \otimes \cdots \otimes a_m \in \mathring{\mathcal{A}}_{i_1} \otimes \mathring{\mathcal{A}}_{i_2} \otimes \cdots \otimes \mathring{\mathcal{A}}_{i_m}$ and $b_1 \otimes b_2 \otimes \cdots \otimes b_m \in$

$\overset{\circ}{\mathcal{A}}_{j_1} \otimes \overset{\circ}{\mathcal{A}}_{j_2} \otimes \cdots \otimes \overset{\circ}{\mathcal{A}}_{j_n}$ determined by

$$(a_1 \otimes \cdots \otimes a_m)(b_1 \otimes \cdots \otimes b_n) = \begin{cases} a_1 \otimes \cdots \otimes a_m \otimes b_1 \otimes \cdots \otimes b_n & , \text{if } i_m \neq j_1 \\ a_1 \otimes \cdots \otimes a_{m-1} \otimes \widehat{a_m} \otimes b_2 \otimes \cdots \otimes b_n + & \\ \varphi_{i_m}(a_m b_1)(a_1 \otimes \cdots \otimes a_{m-1})(b_2 \otimes \cdots \otimes b_n) & , \text{otherwise,} \end{cases}$$

where $\widehat{a_m} = a_m b_1 - \varphi(a_m b_1) 1_{\mathcal{A}_{i_m}}$. Taking $\mathcal{A}$ as the free product $*_{i \in I} \mathcal{A}_i$ above, we can consider each $\mathcal{A}_i$ as a unital sub-algebra of $\mathcal{A}$, although, strictly speaking, the algebra $\mathcal{A}$ contains the sub-algebra $\mathbb{C}1_{\mathcal{A}} \oplus \overset{\circ}{\mathcal{A}}_i$ which is canonically isomorphic to $\mathcal{A}_i$. Thus, to obtain a probability space $(\mathcal{A}, \varphi)$ containing free independent copies of each $(\mathcal{A}_i, \varphi_i)$, we just need to find a unital linear functional $\varphi : \mathcal{A} \to \mathbb{C}$ satisfying the free independence condition for $\{\mathcal{A}_i\}_{i \in I}$, viewed as a collection of sub-algebras of $\mathcal{A}$, and $\varphi_i = \varphi|_{\mathcal{A}_i}$ for every $i \in I$. But, a unital linear functional $\varphi : \mathcal{A} \to \mathbb{C}$ satisfies the free independence condition for the collection $\{\mathcal{A}_i\}_{i \in I}$ if and only if its kernel is given by

$$\ker(\varphi) = \bigoplus_{m=1}^{\infty} \bigoplus_{\substack{i_1, i_2, \ldots, i_m \in I \\ i_1 \neq i_2, \ldots, i_{m-1} \neq i_m}} \overset{\circ}{\mathcal{A}}_{i_1} \otimes \overset{\circ}{\mathcal{A}}_{i_2} \otimes \cdots \otimes \overset{\circ}{\mathcal{A}}_{i_m}. \tag{3.13}$$

Thus, letting $\mathcal{B}$ denote the direct sum in right-hand side of (3.13), we have $\mathcal{A} = \mathbb{C}1_{\mathcal{A}} \oplus \mathcal{B}$ and the map

$$\mathbb{C}1_{\mathcal{A}} \oplus \mathcal{B} \ni \lambda 1_{\mathcal{A}} \oplus b \;\mapsto\; \varphi(\lambda 1_{\mathcal{A}} \oplus b) := \lambda \in \mathbb{C}$$

is a well-defined unital linear functional $\varphi : \mathcal{A} \to \mathbb{C}$ satisfying the free independence condition for $\{\mathcal{A}_i\}_{i \in I}$. Finally, the condition $\varphi_i = \varphi|_{\mathcal{A}_i}$ is an immediate consequence of the definition of φ since every random variable $a \in \mathcal{A}_i$ can be written as $a = \varphi_i(a) 1_{\mathcal{A}} \oplus (a - \varphi_i(a) 1_{\mathcal{A}_i})$ with $a - \varphi_i(a) 1_{\mathcal{A}_i} \in \overset{\circ}{\mathcal{A}}_i \subset \mathcal{B}$.

Asymptotic free independence

In some cases, as we state for several random matrix ensembles in the next chapter, a sequence of families of algebraic random variables converge to a free family of random variables, so free independence arises as a limiting property.

Definition 3.2.4. Let I be a non-empty set. Assume $\{a_{N,i}\}_{i\in I}$ is a family of random variables from an algebraic probability space $(\mathcal{A}_N, \varphi_N)$ for each integer $N \geq 1$. We say that the sequence $\{\{a_{N,i}\}_{i\in I}\}_{N=1}^{\infty}$ of families of random variables is *asymptotically freely independent*, or simply *asymptotically free*, if it converges in distribution to a family $\{a_i\}_{i\in I}$ of free random variables in some algebraic probability space $(\mathcal{A}, \varphi)$.

Similar to convergence in distribution, the ambient probability space $(\mathcal{A}, \varphi)$ is not determining for the asymptotic free independence of the sequence $\{\{a_{N,i}\}_{i\in I}\}_{N=1}^{\infty}$ in the previous definition. Indeed, given a family $\{a_i\}_{i\in I}$ of random variables in some algebraic probability $(\mathcal{A}, \varphi)$, if we let $\mu : \mathbb{C}\langle \mathrm{x}_i \mid i \in I\rangle \to \mathbb{C}$ be the algebraic distribution of $\{a_i\}_{i\in I}$ and $\mathrm{ev} : \mathbb{C}\langle \mathrm{x}_i \mid i \in I\rangle \to \mathcal{A}$ be the unital algebraic homomorphism such that $\mathrm{ev}(\mathrm{x}_i) = a_i$ for ever $i \in I$, the diagram

$$\begin{array}{ccc} \mathcal{A} & \xrightarrow{\ \varphi\ } & \mathbb{C} \\ {\scriptstyle \mathrm{ev}}\uparrow & \nearrow_{\mu} & \\ \mathbb{C}\langle \mathrm{x}_i \mid i \in I\rangle & & \end{array}$$

commutes, and hence, the family $\{a_i\}_{i\in I}$ is free independent with respect to φ if and only if the family of unital sub-algebras $\{\mathbb{C}[\mathrm{x}_i] \subset \mathbb{C}\langle \mathrm{x}_i \mid i \in I\rangle\}_{i\in I}$ is free independent with respect to μ. Moreover, if $\mu_N : \mathbb{C}\langle \mathrm{x}_i \mid i \in I\rangle \to \mathbb{C}$ is the algebraic distribution of $\{a_{N,i}\}_{i\in I}$ for each integer $N \geq 1$, then the sequence $\{\{a_{N,i}\}_{i\in I}\}_{N=1}^{\infty}$ converges in distribution if and only if $\lim_{N\to\infty} \mu_N(\mathrm{p})$ exists for every polynomial $\mathrm{p} \in \mathbb{C}\langle \mathrm{x}_i \mid i \in I\rangle$. Therefore, the sequence

$\{\{a_{N,i}\}_{i\in I}$ is asymptotic free independent if and only if $\lim_{N\to\infty}\mu_N[\mathrm{p}]$ exists for every polynomial $\mathrm{p}\in\mathbb{C}\langle \mathrm{x}_i \mid i\in I\rangle$ and the family of unital sub-algebras $\{\mathbb{C}[\mathrm{x}_i]\subset\mathbb{C}\langle \mathrm{x}_i \mid i\in I\rangle\}_{i\in I}$ is free independent with respect to $\lim_{N\to\infty}\mu_N$. There is no reference to a particular space $(\mathcal{A},\varphi)$ in the latter condition for the asymptotic free independence of $\{\{a_{N,i}\}_{i\in I}$.

Let us recall that Proposition 3.1.5 provide us with a couple of equivalent conditions for the point-wise convergence of a sequence $\{\mu_N\}_{N=1}^{\infty}$ of linear functionals $\mu_N:\mathcal{A}\to\mathbb{C}$ defined on a complex algebra $\mathcal{A}$ which is generated by a family of sub-algebras $\{\mathcal{A}_i\}_{i\in I}$. But this is exactly the setting we have for the asymptotic free independence of $\{\{a_{N,i}\}_{i\in I}$ if we let $\mathcal{A}=\mathbb{C}\langle \mathrm{x}_i \mid i\in I\rangle$ and $\mathcal{A}_i=\mathbb{C}[\mathrm{x}_i]$ for each index $i\in I$. Hence, following the same steps as in the proof of Proposition 3.1.5, we obtain some equivalent conditions for the asymptotic free independence of a family of unital sub-algebras.

Corollary 3.2.5. Let $\mathcal{A}$ be an algebra over $\mathbb{C}$ and let $\mathcal{A}_i\subset\mathcal{A}$ be a sub-algebra for each $i\in I$ so that the family of sub-algebras $\{\mathcal{A}_i\}_{i\in I}$ generate the algebra $\mathcal{A}$. Suppose $\mu_N:\mathcal{A}\to\mathbb{C}$ is linear functional for each $N\geq 1$ such that $\mu[\mathrm{p}]:=\lim_{N\to\infty}\mu_N[\mathrm{p}]$ exists for every $\mathrm{p}\in\mathcal{A}_i$ and every $i\in I$. Then the following two conditions are equivalent:

(a) $\lim\limits_{N\to\infty}\mu_N[\mathrm{p}]$ exists for every $\mathrm{p}\in\mathcal{A}$ and the family of unital sub-algebras $\{\mathcal{A}_i\}_{i\in I}$ is free independent with respect to $\mu:=\lim\limits_{N\to\infty}\mu_N$

(b) $\lim\limits_{N\to\infty}\mu_N[(\mathrm{p}_1-\mu_N[\mathrm{p}_1])(\mathrm{p}_2-\mu_N[\mathrm{p}_2])\cdots(\mathrm{p}_m-\mu_N[\mathrm{p}_m])]=0$ whenever $\mathrm{p}_k\in\mathcal{A}_{i_k}$ with $i_1\neq i_2, i_2\neq i_3,\ldots,i_{m-1}\neq i_m$

Chapter 4

Free Probability and Random Matrices (Literature Review)

This chapter is the second and last part of the literature review. First, we present some fundamental definitions from random matrix theory and set the framework under which random matrices are regarded as algebraic random variables. Second, we state what asymptotic free independence means for random matrix ensembles and give some known results on this matter. Lastly, we introduce the notions of second order free independence, the bounded cumulants property, and asymptotically liberating ensembles and state some results relevant to this thesis.

4.1 Random matrices as algebraic random variables

Definition 4.1.1. Let $(\Omega, \mathcal{F}, P)$ be a classical probability space. An *N-by-N random matrix* on $(\Omega, \mathcal{F}, P)$ is a matrix $X = (x_{i,j})_{1 \leq i,j \leq N}$ having complex random variables on $(\Omega, \mathcal{F}, P)$ as entries. The (i, j)-entry of X is also denoted by $X(i, j)$.

Note that an N-by-N random matrix X on a classical probability space $(\Omega, \mathcal{F}, P)$ is simply a matrix-valued random variable on $(\Omega, \mathcal{F}, P)$, i.e., X is a function $X : \Omega \to \mathrm{Mat}_N(\mathbb{C})$

so that the set $X^{-1}(\mathrm{U}) = \{\omega \in \Omega : X(\omega) \in \mathrm{U}\}$ belongs to the σ-algebra $\mathcal{F}$ for every open set $\mathrm{U} \subset \mathrm{Mat}_N(\mathbb{C})$.

Although random matrices are interesting in their own, many of their most studied properties arise as the matrix dimension goes to infinity. Thus, we are led to consider sequences, or sequences of families, of size-increasing random matrices, known as *ensembles*.

Definition 4.1.2. Let I be and index set. Suppose $(\Omega_N, \mathcal{F}_N, P_N)$ is a classical probability space for each integer $N \geq 1$. A sequence of families $\{\{X_{N,i}\}_{i\in I}\}_{N=1}^{\infty}$ where each $X_{N,i}$ is an N-by-N random matrix on $(\Omega_N, \mathcal{F}_N, P_N)$ is called a *random matrix ensemble*. If the index set I is just a singleton $\{i\}$, we simply write $\{X_{N,i}\}_{N=1}^{\infty}$ or $\{X_N\}_{N=1}^{\infty}$.

Remark. Since entries from random matrices of distinct dimension are never used in the same mathematical expression in this thesis, with out loss of generality, all of the random matrices $X_{N,i}$ in a random matrix ensemble $\{\{X_{N,i}\}_{i\in I}\}_{N=1}^{\infty}$ can be assumed to be defined on the same probability space $(\Omega, \mathcal{F}, P)$, say, by letting $(\Omega, \mathcal{F}, P)$ be product space of the $(\Omega_N, \mathcal{F}_N, P_N)$.

Let us now address the question of finding an algebraic probability space where random matrices can be regarded as algebraic random variables. Suppose we are given a classical probability space $(\Omega, \mathcal{F}, P)$. In Section 3.1, we consider the algebraic probability spaces:

1. $(L^{\infty-}(\Omega, \mathcal{F}, P), \mathbb{E}[\,\cdot\,])$ where $\mathbb{E}[\cdot]$ is the expected value on $(\Omega, \mathcal{F}, P)$ and $L^{\infty-}(\Omega, \mathcal{F}, P)$ is the set of complex-valued random variables on $(\Omega, \mathcal{F}, P)$ that have moments of all orders modulo the following relation: complex-valued random variables on $(\Omega, \mathcal{F}, P)$ that are the same function up to a measurable set of probability zero are considered the same random variable.

2. $(\mathrm{Mat}_N(\mathbb{C}), \mathrm{tr}(\cdot))$ where $\mathrm{Mat}_N(\mathbb{C})$ is the algebra of N-by-N matrices with entries from $\mathbb{C}$ and $\mathrm{tr}(\cdot)$ denotes the normalized trace $\frac{1}{N}\mathrm{Tr}(\cdot)$.

It turns out that if we combine the above, we obtain an algebraic probability space whose algebraic random variables are precisely random matrices with entries having finite moments of all orders. More specifically, letting $\mathrm{Mat}_N\left(L^{\infty-}\right)$ denote the set of N-by-N matrices with entries from $L^{\infty-}(\Omega, \mathcal{F}, P)$, the pair $\left(\mathrm{Mat}_N\left(L^{\infty-}\right), \mathbb{E}[\mathrm{tr}(\ \cdot\ )]\right)$ is an algebraic probability space. Indeed, random matrices are endowed with the usual matrix operations of addition, multiplication, and multiplication by scalars: given any two random matrices $X = (x_{i,j})_{1\leq i,j\leq N}$ and $Y = (y_{i,j})_{1\leq i,j\leq N}$ and a complex number $\lambda \in \mathbb{C}$, we have

$$X + \lambda Y := \left(x_{i,j} + \lambda y_{i,j}\right)_{1\leq i,j\leq N} \qquad \text{and} \qquad XY := \left(\textstyle\sum_{k=1}^{N} x_{i,k}y_{k,j}\right)_{1\leq i,j\leq N}.$$

Moreover, we can identify $\mathrm{Mat}_N(\mathbb{C})$ with the subset of $\mathrm{Mat}_N(L^{\infty-})$ consisting of constant random matrices, and hence, $\mathrm{Mat}_N(L^{\infty-})$ is a unital algebra over the complex numbers with multiplicative identity I_N. Now, generalizing the notions of trace and normalized trace from $\mathrm{Mat}_N(\mathbb{C})$, the *trace* and the *normalized trace* of a random matrix $X \in \mathrm{Mat}_N(L^{\infty-})$, denoted $\mathrm{Tr}(X)$ and $\mathrm{tr}(X)$, respectively, are given by

$$\mathrm{Tr}(X) = \sum_{i=1}^{N} X(i,i) \qquad \text{and} \qquad \mathrm{tr}(X) = \frac{1}{N}\sum_{i=1}^{N} X(i,i) = \frac{1}{N}\mathrm{Tr}(X).$$

Both maps $X \mapsto \mathrm{Tr}(X)$ and $X \mapsto \mathrm{tr}(X)$ are well-defined linear functionals from $\mathrm{Mat}_N(L^{\infty-})$ to $L^{\infty-}(\Omega, \mathcal{F}, P)$ and the latter is also unital, in the sense that the multiplicative identity in $\mathrm{Mat}_N(L^{\infty-})$ is mapped to the multiplicative identity in $L^{\infty-}(\Omega, \mathcal{F}, P)$. Therefore, the expected value of the normalized trace $\mathbb{E}[\mathrm{tr}(\cdot)] : \mathrm{Mat}_N(L^{\infty-}) \to \mathbb{C}$ is a unital linear functional and the pair $\left(\mathrm{Mat}_N\left(L^{\infty-}\right), \mathbb{E}[\mathrm{tr}(\ \cdot\ )]\right)$ is an algebraic probability space.

Remark. Through the entire thesis, we examine random matrices primarily as algebraic random variables. Thus, unless otherwise stated, it is assumed that random matrices are taken from algebraic probability spaces $(\mathrm{Mat}_N(L^{\infty-}), \mathbb{E}[\mathrm{tr}(\,\cdot\,)])$. It is always under this assumption that we make use of the results and terminology from algebraic probability spaces when dealing with random matrices.

Regarding random matrices as algebraic random variables enables us to analyze random matrix ensembles as sequences of families of algebraic random variables. This is particularly important since many random matrix ensembles have been shown to exhibit asymptotic free independence. Before we present some well-known results on asymptotic free independence of random matrix ensembles, we need to provide the reader with some more notation and terminology, as well as the definition of certain random matrices pertinent to this thesis.

As matrix-valued random variables, random matrices inherit the terminology and notation from matrices in $\mathrm{Mat}_N(\mathbb{C})$. Hence, for a random matrix $X \in \mathrm{Mat}_N(L^{\infty-})$ we have the following:

- The *transpose* of X is the unique random matrix $X^T \in \mathrm{Mat}_N(L^{\infty-})$ such that $X^T(i,j) = X(j,i)$. We call X *orthogonal* if it satisfies $X^TX = XX^T = I_N$.

- The *conjugate transpose* of X is the unique random matrix $X^* \in \mathrm{Mat}_N(L^{\infty-})$ such that $X^*(i,j) = \overline{X(j,i)}$ where $\overline{X(j,i)}$ denotes the complex conjugate of $X(j,i)$. The matrix X is called *normal* if we have $X^*X = XX^*$ and is said to be *self-adjoint*, or *Hermitian*, if $X = X^*$. We call X *unitary* if it satisfies $X^*X = XX^* = I_N$.

Additionally, a random matrix ensemble $\{\{X_{N,i}\}_{i\in I}\}_{N=1}^{\infty}$ is called *orthogonal*, *self-adjoint*, or *unitary* if every $X_{N,i}$ is orthogonal, self-adjoint, or unitary, respectively.

Some random matrices and their distributions

Given a random matrix $X \in \mathrm{Mat}_N(L^{\infty-})$, there are three mathematical objects that are referred as distribution of X: the matrix distribution of X, the algebraic distribution of the entries of X, and the algebraic distribution of X. The *matrix distribution* of X is defined as the push-forward measure μ_X on $\mathrm{Mat}_N(\mathbb{C})$ determined by

$$\mu_X(\mathrm{U}) = P(X^{-1}(\mathrm{U})) = P(\{\omega \in \Omega \mid X(\omega) \in \mathrm{U}\})$$

for every open set $\mathrm{U} \subset \mathrm{Mat}_N(\mathbb{C})$. A non-trivial problem related to the matrix distribution of X is that of computing matrix integrals. A *matrix integral* of X is a integral of the form

$$\int_{\mathrm{Mat}_N(\mathbb{C})} f(\mathrm{M}) d\mu_X(\mathrm{M}) = \int_\Omega f(X(\omega)) dP(\omega) = \int_\Omega f \circ X(\omega) dP(\omega)$$

where $f : \mathrm{Mat}_N(\mathbb{C}) \to \mathbb{C}$ is a measurable function, often a polynomial function on the entries of X and their complex conjugates. Now, regarding the entries of X, $\{X(i,j) \mid 1 \leq i,j \leq N\}$, as algebraic random variables in $(L^{\infty-}(\Omega, \mathcal{F}, P), \mathbb{E}[\,\cdot\,])$, the *algebraic distribution of the entries* of X is the unital linear functional $\mu : \mathbb{C}\langle \mathrm{x}_{i,j} \mid 1 \leq i,j \leq N\rangle \to \mathbb{C}$ given by

$$\mu(\mathrm{x}_{i_1,j_1}\mathrm{x}_{i_2,j_2}\cdots\mathrm{x}_{i_m,j_m}) = \mathbb{E}[X(i_1,j_1)X(i_2,j_2)\cdots X(i_m,j_m)]$$

for all integers $m \geq 1$ and $1 \leq i_k, j_k \leq N$ for $k = 1, 2, \ldots, m$. Two families $\{X_i\}_{i\in I}$ and $\{Y_i\}_{i\in I}$ of N-by-N random matrices from $\mathrm{Mat}_N(L^{\infty-})$ are said to be *equal in distribution of their entries*, or simply *equal in distribution*, if they satisfy

$$\mathbb{E}\left[\prod_{k=1}^{m} X_{i_k}(j_{-k}, j_k)\right] = \mathbb{E}\left[\prod_{k=1}^{m} Y_{i_k}(j_{-k}, j_k)\right] \tag{4.1}$$

for all integers $m \geq 1$, indexes $i_1, i_2, \ldots, i_m \in I$, and functions $\mathbf{j} : [\pm m] \to [N]$. Finally, the *algebraic distribution* of X, regarded as an element of the algebraic probability space $(\mathrm{Mat}_N(L^{\infty-}), \mathbb{E}[\mathrm{tr}(\,\cdot\,)])$, is the unital linear functional $\mu : \mathbb{C}[\mathrm{x}] \to \mathbb{C}$ determined by

$$\mu(\mathrm{x}^m) = \mathbb{E}\left[\mathrm{tr}\left(X^m\right)\right] = \frac{1}{N} \sum_{j_1, j_2, \ldots, j_k = 1}^{N} \mathbb{E}\left[X(j_1, j_2) X(j_2, j_3) \cdots X(j_m, j_1)\right]$$

for all integers $m \geq 1$ and functions $\mathbf{j} : [m] \to [N]$.

We end this section with a list of some random matrices and the joint distribution of their entries relevant to this thesis.

Real Wigner matrix. A self-adjoint N-by-N random matrix $X_N = (\frac{1}{\sqrt{N}} x_{i,j})_{1 \leq i \leq j \leq N}$ is a *real Wigner matrix* if $x_{1,2}$ has unit variance and $\{x_{i,j} \mid 1 \leq i < j \leq N\}$ and $\{x_{i,i} \mid 1 \leq i \leq N\}$ form two independent families of independent and identically distributed real-valued random variables with zero mean and finite p-norms of all orders. If $x_{1,1}$ and $x_{1,2}$ are Gaussian distributed, we say X_N is a *Gaussian Wigner matrix*; additionally, $x_{1,1}$ has variance 2, the sequence $\{X_N\}_{N=1}^{\infty}$ is called *Gaussian Orthogonal Ensemble*.

Complex Wigner matrix. A self-adjoint N-by-N random matrix $Z_N = (\frac{1}{\sqrt{N}} z_{i,j})_{1 \leq i \leq j \leq N}$ is an *Hermitian Wigner matrix* if $z_{1,2}$ has zero second moment, $|z_{1,2}|$ has unit second moment and $\{z_{i,j} \mid 1 \leq i < j \leq N\}$ and $\{z_{i,i} \mid 1 \leq i \leq N\}$ form two independent families of independent and identically distributed complex-valued random variables with zero mean and finite p-norms of all orders. If $z_{1,1}$ is Gaussian distributed and $z_{1,2}$ is complex-Gaussian distributed, we say that Z_N is a *Gaussian Hermitian Wigner matrix*; additionally, $z_{1,1}$ has variance 1, we call the sequence $\{Z_N\}_{N=1}^{\infty}$ a *Gaussian Unitary Ensemble*.

Haar-unitary random matrix. An N-by-N random matrix Z_N is a *Haar-unitary random matrix* if it is unitary and its matrix distribution μ_{Z_N} gives the Haar-measure on the unitary

group $\mathcal{U}_N(\mathbb{C}) = \{\mathrm{U} \in \mathrm{Mat}_N(\mathbb{C}) \mid \mathrm{U}^*\mathrm{U} = \mathrm{U}\mathrm{U}^* = I_N\}$.

Haar-orthogonal random matrix. An N-by-N random matrix Z_N is a *Haar-orthogonal random matrix* if it is orthogonal and its matrix distribution μ_{Z_N} gives the Haar-measure on the orthogonal group $\mathcal{O}_N(\mathbb{C}) = \{\mathrm{O} \in \mathrm{Mat}_N(\mathbb{C}) \mid \mathrm{O}^T\mathrm{O} = \mathrm{O}\mathrm{O}^T = I_N\}$.

Uniformly distributed signature matrix. 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.

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

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

If X is an N-by-N uniformly distributed signature matrix, then for all functions $\mathbf{i}, \mathbf{j} : S \to [N]$ we have

$$\mathbb{E}\left[\prod_{k \in S} X(i_k, j_k)\right] = \begin{cases} 1, & \text{if } \mathbf{i} = \mathbf{j} \text{ and } \ker(\mathbf{i}) \text{ is an even partition} \\ 0, & \text{otherwise} \end{cases} \tag{4.2}$$

Uniformly distributed signed permutation matrix. 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.

A matrix $\mathrm{W} \in \mathrm{Mat}_N(\mathbb{C})$ is a *signed permutation matrix* if there exists signs $\epsilon_1, \ldots, \epsilon_N \in \{-1, 1\}$ and a permutation $\sigma \in \{f : [N] \to [N] : f \text{ is bijective}\}$ such that

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

If W is an N-by-N uniformly distributed signed permutation matrix, then for all functions $\mathbf{i}, \mathbf{j} : S \to [N]$ we get

$$\mathbb{E}\left[\prod_{s\in S} W(i_s, j_s)\right] = \begin{cases} \frac{(N-\#(\pi))!}{N!} & \text{, if } \pi = \ker(\mathbf{i}) = \ker(\mathbf{j}) \in P_{\text{even}}(S) \\ 0 & \text{, otherwise} \end{cases} \tag{4.3}$$

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 $\{\mathrm{W}^* V_i \mathrm{W}\}_{i\in I}$ are equal in distribution, in the sense of (4.1), for every signed permutation matrix W. Then, for all integers $m \geq 1$, indexes $i_1, i_2, \ldots, i_m \in I$, and functions $\mathbf{j} : [\pm m] \to [N]$, we have

$$\mathbb{E}\left[\prod_{k=1}^{m} V_{i_k}(j_{-k}, j_k)\right] = \prod_{k=1}^{m} \epsilon_{\sigma(j_{-k})}\epsilon_{\sigma(j_k)} \mathbb{E}\left[\prod_{k=1}^{m} V_{i_k}(\sigma(j_{-k}), \sigma(j_k))\right] \tag{4.4}$$

for all signs $\epsilon_1, \ldots, \epsilon_N \in \{-1, 1\}$ and permutations $\sigma \in \{f : [N] \to [N] : f \text{ is bijective}\}$.

4.2 Asymptotic free independence

Let I be an index set. Suppose we are given a random matrix ensemble $\{X_{N,i}\}_{N=1}^{\infty}$ for each index $i \in I$. Formally, the *joint (algebraic) distribution* of each family $\{X_{N,i}\}_{i\in I}$ is the unital linear functional $\mu_N : \mathbb{C}\langle \mathrm{x}_i \mid i \in I\rangle \to \mathbb{C}$ defined by

$$\mu_N(\mathrm{p}) := \mathbb{E}\left[\mathrm{tr}\left(\mathrm{p}\left(\{X_{N,i}\}_{i\in I}\right)\right)\right]$$

for every polynomial $\mathrm{p} \in \mathbb{C}\langle \mathrm{x}_i \mid i \in I\rangle$. Moreover, the convergence in distribution of the ensembles $\{X_{N,i}\}_{N=1}^{\infty}$ with $i \in I$, as well as their asymptotic free independence, is defined as a condition on the linear functionals μ_N resulting from taking N going to infinity. However, the

notions of convergence in distribution and asymptotic free independence for random matrix ensembles can be stated without referring to the functionals μ_N explicitly. For instance, Corollary 3.2.5 implies that the ensembles $\{X_{N,i}\}_{N=1}^{\infty}$ with $i \in I$ are *asymptotically freely independent* if and only if the following conditions hold:

(AF.1) $\lim_{N\to\infty} \mathbb{E}\left[\mathrm{tr}\left(X_{N,i}^k\right)\right]$ exists each integer $k \geq 1$ and each index $i \in I$, and

(AF.2) for all integers $m \geq 1$, all indexes $i_1, i_2, \ldots, i_m \in I$ satisfying $i_1 \neq i_2, i_2 \neq i_3, \ldots, i_{m-2} \neq i_{m-1}, i_{m-1} \neq i_m$ and all polynomials $\mathrm{p}_1, \mathrm{p}_2, \ldots, \mathrm{p}_m$ in the algebra $\mathbb{C}[\mathrm{x}]$, we have $\lim_{N\to\infty} \mathbb{E}\left[\mathrm{tr}\left(Y_{N,1}Y_{N,2}\cdots Y_{N,m}\right)\right] = 0$ where $Y_{N,k} = \mathrm{p}_k\left(X_{N,i_k}\right) - \mathbb{E}\left[\mathrm{tr}\left(\mathrm{p}_k\left(X_{N,i_k}\right)\right)\right] I_N$.

The first result about random matrix ensembles exhibiting asymptotic free independence is due to D. Voiculescu in [23]. He showed that independent Gaussian Unitary Ensembles converge in distribution to free semi-circular random variables. This result has been extended by many authors since then, here we present it as formulated in [2, Chapter 5].

Theorem 4.2.1. Let $\{X_{N,i}\}_{i\in I}$ be a family of independent N-by-N complex (real) Wigner matrices for every integer $N \geq 1$. Suppose the following two conditions hold:

(a) $\mathbb{E}\left[|X_{N,i}(j_1, j_2)|^2\right] = \frac{1}{\sqrt{N}}$ for all integers $1 \leq j_1, j_2 \leq N$ and indexes $i \in I$,

(b) $\sup_{N\geq 1} \max_{1\leq j_1, j_2 \leq N} \sqrt{N}\|X_{N,i}(j_1, j_2)\|_p < \infty$ for every integer $p \geq 1$ and ever index $i \in I$.

Then the random matrix ensembles $\{X_{N,i}\}_{N=1}^{\infty}$ with $i \in I$ are asymptotically free.

It turns out that Wigner matrix ensembles are also asymptotically freely independent from any ensemble composed of deterministic matrices that has a limiting distribution of first order, see [2, Chapter 5]. A random matrix ensemble $\{\{D_{N,i}\}_{i\in I}\}_{N=1}^{\infty}$ has a *first order limiting distribution* if the limit

$$\lim_{N\to\infty} \mathbb{E}\left[\mathrm{tr}\left(D_{N,i_1} D_{N,i_2} \cdots D_{N,i_m}\right)\right]$$

exist for all integers $m \geq 1$ and indexes $i_1, i_2, \ldots, i_m$. If every $D_{N,i}$ is a deterministic matrix from $\mathrm{Mat}_N(\mathbb{C})$, the limit above can be simply taken without the expected value.

Theorem 4.2.2. Let $\{\{X_{N,i}\}_{i\in I}\}$ be a as in the previous theorem. Suppose $\{D_{N,i}\}_{i\in I}$ is a family of deterministic matrices in $\mathrm{Mat}_N(\mathbb{C}) \subset \mathrm{Mat}_N(L^{\infty-})$ for each integer $N \geq 1$. If the ensemble $\{\{D_{N,i}\}_{i\in I}\}_{N=1}^{\infty}$ has a first order limiting distribution, then $\{\{X_{N,i}\}_{i\in I}\}_{N=1}^{\infty}$ and $\{\{D_{N,i}\}_{i\in I}\}_{N=1}^{\infty}$ are asymptotically free.

It was first noted by D. Voiculescu in [23] that the previous two theorems hold if each $\{X_{N,i}\}_{i\in I}$ is replaced by a family of independent Haar-unitary random matrices. In general, an ensemble $\{\{D_{N,i}\}_{i\in I}\}_{N=1}^{\infty}$ with a first order limiting distribution and an unitarily (orthogonally) invariant random matrix ensemble $\{\{X_{N,i}\}_{i\in I}\}_{N=1}^{\infty}$ are asymptotically free, see [11]. A random matrix ensemble $\{\{X_{N,i}\}_{i\in I}\}_{N=1}^{\infty}$ is said to be *unitarily (orthogonally) invariant* if the distribution of each $\{X_{N,i}\}_{i\in I}$ is invariant under conjugation by unitary (orthogonal) matrices, i.e., $\{X_{N,i}\}_{i\in I}$ and $\{\mathrm{U}_N^* X_{N,i} \mathrm{U}_N\}_{i\in I}$ are equal in distribution of their entries for any unitary matrix $\mathrm{U}_N \in \mathrm{Mat}_N(\mathbb{C})$

Theorem 4.2.3. Suppose $\{X_{N,i}\}_{i\in I}$ is a family of independent N-by-N unitarily (orthogonally) invariant random matrix for every integer $N \geq 1$. Then $\{\{X_{N,i}\}_{i\in I}\}_{N=1}^{\infty}$ is asymptotically free. Additionally, if the sequence $\{\{D_{N,i}\}_{i\in I}\}_{N=1}^{\infty}$ has a first order limiting distribution, then $\{\{X_{N,i}\}_{i\in I}\}_{N=1}^{\infty}$ and $\{\{D_{N,i}\}_{i\in I}\}_{N=1}^{\infty}$ are asymptotically free.

Unitarily invariant ensembles include: Gaussian Unitary Ensembles, complex Wishart ensembles, and Haar-unitary ensembles. Similarly, Gaussian Orthogonal Ensembles, real Wishart ensembles, and Haar-orthogonal ensembles are orthogonally invariant. As a consequence of Theorem 4.2.3 we have that conjugation of deterministic matrices by independent Haar-unitary (Haar-orthogonal) random matrices gives rise to asymptotic free independence.

Corollary 4.2.4. Suppose $\{U_{N,i}\}_{i\in I}$ is a family of independent N-by-N Haar-unitary (Haar-orthogonal) random matrices for each integer $N \geq 1$. If $\{\{D_{N,i}\}_{i\in I}\}_{N=1}^{\infty}$ has a first order limiting distribution, then $\{U_{N,i}D_{N,i}U_{N,i}^*\}_{N=1}^{\infty}$ with $i \in I$ are asymptotically free.

The assumption of $\{\{D_{N,i}\}_{i\in I}\}_{N=1}^{\infty}$ having a first order limiting distribution is crucial for the conclusion in Corollary 4.2.4. However, this assumption can be weaken if we require each ensemble of constant matrices $\{D_{N,i}\}_{N=1}^{\infty}$ to be uniformly bounded with respect to the operator norm.

4.3 Asymptotic free independence of second order

A main topic of independences of second order is the behavior of $\mathrm{cov}[\mathrm{Tr}(Y_N), \mathrm{Tr}(Z_N)]$ as the size of random matrices Y_N and Z_N goes to infinity. As in the case of asymptotic free independence, an independence of second order for random matrix ensembles $\{X_{N,1}\}_{N=1}^{\infty}$ and $\{X_{N,2}\}_{N=1}^{\infty}$ should allows us to compute

$$\lim_{N\to\infty} \mathrm{cov}\left[\mathrm{Tr}\left(X_{N,i_1}X_{N,i_2}\cdots X_{N,i_m}\right), \mathrm{Tr}\left(X_{N,i_{m+1}}X_{N,i_{m+2}}\cdots X_{N,i_{m+n}}\right)\right], \tag{4.5}$$

known as *fluctuation moments*, for all integers $m, n \geq 1$ and indexes $i_1, i_2, \ldots, i_{m+n} \in \{1, 2\}$ in terms of individual second order moments: $\lim_{N\to\infty} \mathrm{cov}\left[\mathrm{Tr}(X_{N,1}^k), \mathrm{Tr}(X_{N,1}^l)\right]$ and $\lim_{N\to\infty} \mathrm{cov}\left[\mathrm{Tr}(X_{N,2}^k), \mathrm{Tr}(X_{N,2}^l)\right]$. In general, the computation of (4.5) also involves individual first order moments $\lim_{N\to\infty} \mathbb{E}\left[\mathrm{tr}(X_{N,1}^k)\right]$ and $\lim_{N\to\infty} \mathbb{E}\left[\mathrm{tr}(X_{N,2}^k)\right]$.

Complex case

The *Lindeberg trick*, used for deriving universal or limit laws, consists in considering Gaussian distributed random variables as a case study to infer what might hold true for general random

variables. For instance, Wigner's semicircular law was first established for Gaussian Unitary Ensembles, Wigner matrices with standard Gaussian random variables as entries, and then for general Wigner matrices. Analyzing the fluctuation moments of independent Gaussian Unitary Ensembles, J. Mingo and R. Speicher found a relation between fluctuation moments and individual moments of first and second order in [13].

Theorem 4.3.1. Suppose $\{\{X_{N,i}\}_{N=1}^{\infty}\}_{i\in I}$ is a family of independent Gaussian Unitary Ensembles. Then the fluctuation moments of $\{\{X_{N,i}\}_{i\in I}\}_{N=1}^{\infty}$ are determined by the following property: for any given integers $m_1, m_2 \geq 1$, polynomials $\mathrm{p}_1, \mathrm{p}_2, \ldots, \mathrm{p}_{m_1}, \mathrm{q}_1, \mathrm{q}_2, \ldots, \mathrm{q}_{m_2} \in \mathbb{C}[\mathrm{x}]$ and indexes $i_1, i_2, \ldots, i_{m_1}, j_1, j_2, \ldots, j_{m_2} \in I$, if we take $Y_{N,k}$ and $Z_{N,l}$ given by

$$Y_{N,k} = \mathrm{p}_k\left(X_{N,i_k}\right) - \mathbb{E}\left[\mathrm{tr}\left(\mathrm{p}_k\left(X_{N,i_k}\right)\right)\right] I_N \quad \text{and } Z_{N,l} = \mathrm{q}_l\left(X_{N,j_l}\right) - \mathbb{E}\left[\mathrm{tr}\left(\mathrm{q}_l\left(X_{N,j_l}\right)\right)\right] I_N \tag{4.6}$$

for $1 \leq k \leq m_1$ and $1 \leq l \leq m_2$, then

$$\lim_{N\to\infty} \mathrm{cov}\Big[\mathrm{Tr}\left(Y_{N,1}Y_{N,2}\cdots Y_{N,m_1}\right), \mathrm{Tr}\left(Z_{N,1}Z_{N,2}\cdots Z_{N,m_2}\right)\Big] = \delta_{m_1,m_2} \lim_{N\to\infty} \sum_{l=1}^{m_2}\prod_{k=1}^{m_1} \mathbb{E}\left[\mathrm{tr}\left(Y_{N,k}Z_{N,l-k}\right)\right]$$

provided $i_1 \neq i_2, i_2 \neq i_3, \ldots, i_{m_1-1} \neq i_{m_1}, i_{m_1} \neq i_1$ and $j_1 \neq j_2, \ldots, j_{m_2-1} \neq j_{m_2}, j_{m_2} \neq j_1$.

From an algebraic point of view, the previous theorem can be read as follows. For each integer $N \geq 1$, we have a unital linear functional $\mu_N : \mathbb{C}\langle \mathrm{x}_i \mid i \in I\rangle \to \mathbb{C}$ and a bi-linear functional $\rho_N : \mathbb{C}\langle \mathrm{x}_i \mid i \in I\rangle \times \mathbb{C}\langle \mathrm{x}_i \mid i \in I\rangle \to \mathbb{C}$ so that the following conditions holds

$$\begin{aligned}\lim_{N\to\infty} \rho_N\left[\left(\mathrm{p}_1 - \mu_N(\mathrm{p}_1)\right)\cdots\left(\mathrm{p}_{m_1} - \mu_N(\mathrm{p}_{m_1})\right), \left(\mathrm{q}_1 - \mu_N(\mathrm{q}_1)\right)\cdots\left(\mathrm{q}_{m_1} - \mu_N(\mathrm{q}_{m_2})\right)\right] = \\ \delta_{m_1,m_2} \lim_{N\to\infty} \sum_{l=1}^{m_2}\prod_{k=1}^{m_1} \mu_N\left[\left(\mathrm{p}_k - \mu_N(\mathrm{p}_k)\right)\left(\mathrm{q}_{l-k} - \mu_N(\mathrm{q}_{l-k})\right)\right]\end{aligned} \tag{4.7}$$

whenever $\mathrm{p}_k \in \mathbb{C}[\mathrm{x}_{i_k}]$ and $\mathrm{q}_l \in \mathbb{C}[\mathrm{x}_{j_l}]$ for $1 \leq k \leq m_1$ and $1 \leq l \leq m_2$ and the indexes $i_1, i_2, \ldots, i_{m_1}, j_1, j_2, \ldots, j_{m_2} \in I$ satisfy $i_1 \neq i_2, i_2 \neq i_3, \ldots, i_{m_1-1} \neq i_{m_1}, i_{m_1} \neq i_1$ and $j_1 \neq j_2, \ldots, j_{m_2-1} \neq j_{m_2}, j_{m_2} \neq j_1$. The unital linear functional μ_N and the bi-linear functional ρ_N paired with the previous theorem are the ones defined by

$$\mu_N(\mathrm{p}) = \mathbb{E}\left[\mathrm{tr}\left(\mathrm{p}\left(\{X_{N,i}\}_{i\in I}\right)\right)\right] \tag{4.8}$$

and

$$\rho_N(\mathrm{p},\mathrm{q}) = \mathrm{cov}\left[\mathrm{Tr}\left(\mathrm{p}(\{X_{N,i}\}_{i\in I})\right), \mathrm{Tr}\left(\mathrm{q}(\{X_{N,i}\}_{i\in I})\right)\right] \tag{4.9}$$

for all polynomials $\mathrm{p}, \mathrm{q} \in \mathbb{C}\langle \mathrm{x}_i \mid i \in I\rangle$ and the conclusion is that both limits in (4.7) exists and are equal if $\{X_{N,i}\}_{N=1}^{\infty}$ with $i \in I$ are independent Gaussian Unitary Ensembles. The same conclusion holds if $\{X_{N,i}\}_{N=1}^{\infty}$ with $i \in I$ are independent complex Wishart random matrix ensembles.

Motivated by their findings, J. Mingo and R. Speicher introduce in [13] the notions of second order probability space and free independence of second order, providing an abstract framework that captures the main algebraic aspects of what had being observed for some random matrix ensembles.

Definition 4.3.2. A *complex second order probability space* is a triple $(\mathcal{A}, \varphi, \psi)$ consisting of a tracial algebraic probability space $(\mathcal{A}, \varphi)$ and a symmetric bi-linear functional $\psi : \mathcal{A}\times\mathcal{A} \to \mathbb{C}$ tracial in each coordinate such that $\psi(a, 1_{\mathcal{A}}) = \psi(1_{\mathcal{A}}, a) = 0$ for all random variables $a \in \mathcal{A}$.

Note that the triple $(\mathrm{Mat}_N(L^{\infty-}), \mathbb{E}[\mathrm{tr}(\,\cdot\,)], \mathrm{cov}[\mathrm{Tr}(\,\cdot\,), \mathrm{Tr}(\,\cdot\,)])$ is a complex second order probability space. Indeed, for all random matrices $X, Y, Z \in \mathrm{Mat}_N(L^{\infty-})$ and any complex

number $\lambda \in \mathbb{C}$ we have:

$$\begin{aligned}
&(1) && \mathbb{E}[\mathrm{tr}(XY)] &&= && \mathbb{E}[\mathrm{tr}(YX)] && \textit{(traciality)}\\
&(2) && \mathrm{cov}[\mathrm{Tr}(X), \mathrm{Tr}(Y)] &&= && \mathrm{cov}[\mathrm{Tr}(Y), \mathrm{Tr}(X)] && \textit{(symmetry)}\\
&(3) && \mathrm{cov}[\mathrm{Tr}(X + \lambda Y), \mathrm{Tr}(Z)] &&= && \mathrm{cov}[\mathrm{Tr}(X), \mathrm{Tr}(Z)] + \lambda \cdot \mathrm{cov}[\mathrm{Tr}(Y), \mathrm{Tr}(Z)] && \textit{(linearity)}\\
&(4) && \mathrm{cov}[\mathrm{Tr}(XY), \mathrm{Tr}(Z)] &&= && \mathrm{cov}[\mathrm{Tr}(YX), \mathrm{Tr}(Z)] && \textit{(traciality)}
\end{aligned}$$

Definition 4.3.3. Let $(\mathcal{A}, \varphi, \psi)$ be a second order algebraic probability space. A collection $\{\mathcal{A}_i\}_{i\in I}$ of unital sub-algebras of $\mathcal{A}$ is *complex second order free* with respect to (φ, ψ) if

(i) the family $\{\mathcal{A}_i\}_{i\in I}$ is free with respect to φ and

(ii) for all integers $m, n \geq 1$, indexes $i_1, i_2, \ldots, i_m, j_1, j_2, \ldots, j_n \in I$ with $i_1 \neq i_2, \ldots, i_{m-1} \neq i_m, i_m \neq i_1$ and $j_1 \neq j_2, \ldots, j_{n-1} \neq j_n, j_n \neq j_1$, and random variables $a_k \in \mathcal{A}_{i_k}$ and $b_l \in A_{j_l}$ with $\varphi(a_k) = \varphi(b_m) = 0$ for $1 \leq k \leq m$ and $1 \leq l \leq n$, we have

$$\psi(a_1 a_2 \cdots a_m, b_1 b_2 \cdots b_n) = \delta_{m,n} \sum_{l=1}^{n} \prod_{k=1}^{m} \varphi(a_k b_{l-k})$$

where $l - k$ is taken modulo n; additionally, if $m = n = 1$ and $i_1 \neq j_1$, we require $\psi(a_1, b_1) = 0$.

A collection of families of random variables $\{\{a_{i,j}\}_{j\in J_i}\}_{i\in I}$ is called *complex second order free* if the collection of sub-algebras $\{\mathcal{A}_i\}_{i\in I}$ is complex second order free where each $\mathcal{A}_i$ is the unital sub-algebra generated by $\{a_{i,j}\}_{j\in J_i}$.

Complex free independence of second order determines a set of rules to compute mixed moments in terms of individual moments. But in a complex second order probability space $(\mathcal{A}, \varphi, \psi)$ we have to consider two types of moments, one type corresponding to the linear

functional φ and another type corresponding to the bi-linear functional ψ. For a random variable $a \in \mathcal{A}$, the set $\{\varphi(a^k) \mid k \geq 1\}$ is the collection of *moments of first order* of a and the set $\{\psi(a^k, a^l) \mid k, l \geq 1\}$ is the collection of *moments of second order*. More generally, the collection of *moments of first order* of a family of random variables $\{a_i\}_{i \in I} \subset \mathcal{A}$ is the set

$$\{\varphi(a_{i_1} a_{i_2} \cdots a_{i_m}) \mid m \geq 1 \text{ and } i_1, i_2, \ldots, i_m \in I\}$$

and the collection of *moments of second order* of $\{a_i\}_{i \in I} \subset \mathcal{A}$ is the set

$$\{\psi(a_{i_1} a_{i_2} \cdots a_{i_m}, a_{j_1} a_{j_2} \cdots a_{j_n}) \mid m, n \geq 1 \text{ and } i_1, i_2, \ldots, i_m, j_1, j_2, \ldots, j_n \in I\}.$$

A moment of first order $\varphi(a_{i_1} a_{i_2} \cdots a_{i_m})$ is said to be *mixed* if at least two of the indexes $i_1, i_2, \ldots, i_m \in I$ are distinct, otherwise, it is said to be *individual*. Similarly, a moment of second order $\psi(a_{i_1} \cdots a_{i_m}, a_{j_1} \cdots a_{j_n})$ is said to be *mixed* if at least two of the indexes $i_1, \ldots, i_m, j_1, \ldots, j_n \in I$ are distinct, and *individual*, otherwise.

Under the presence of free independence, the rules to compute mixed moments of first order are determined by the free independence condition, see Proposition 3.2.3. On the other hand, under the presence of complex free independence of second order, the computation of mixed moments of second order is determined by the free independence condition and by the *free independence condition of second order*, namely,

$$\psi(a_1 a_2 \cdots a_m, b_1 b_2 \cdots b_n) = \delta_{m,n} \sum_{l=1}^{n} \prod_{k=1}^{m} \varphi(a_k b_{l-k})$$

whenever $a_k \in \mathcal{A}_{i_k}$ and $b_l \in A_{j_l}$ with $\varphi(a_k) = \varphi(b_m) = 0$ for $1 \leq k \leq m$ and $1 \leq l \leq n$ and the indexes $i_1, i_2, \ldots, i_m, j_1, j_2, \ldots, j_n \in I$ satisfy $i_1 \neq i_2, \ldots, i_{m-1} \neq i_m, i_m \neq i_1$ and

$j_1 \neq j_2, \ldots, j_{n-1} \neq j_n, j_n \neq j_1$.

Proposition 4.3.4. Let $(\mathcal{A}, \varphi, \psi)$ be a complex second order probability space and let $\{\mathcal{A}_i\}_{i\in I}$ be a family of unital sub-algebras of $\mathcal{A}$ second order free independent with respect to (φ, ψ). If $\mathcal{A}$ is generated as an algebra by the family $\{\mathcal{A}_i\}_{i\in I}$, then ψ is uniquely determined by the restrictions $\varphi|_{\mathcal{A}_i}$ and $\psi|_{\mathcal{A}_i\times\mathcal{A}_i}$ and by the complex second order free independence condition.

Proof. Suppose $c_k \in \mathcal{A}_{i_k}$ and $d_l \in A_{j_l}$ for $1 \leq k \leq m$ and $1 \leq l \leq n$ and some indexes $i_1, i_2, \ldots, i_m, j_1, j_2, \ldots, j_n \in I$. Without loss of generality, we can assume with $i_1 \neq i_2, \ldots, i_{m-1} \neq i_m, i_m \neq i_1$ and $j_1 \neq j_2, \ldots, j_{n-1} \neq j_n, j_n \neq j_1$, otherwise, we recursively group c_k and c_{k+1} if $i_k = i_{k+1}$ or d_l and d_{l+1} if $i_l = i_{l+1}$. Now, taking $a_k = b_k - \varphi(b_k)1_{\mathcal{A}}$ for $1 \leq k \leq m$ and $b_l = d_l - \varphi(d_l)1_{\mathcal{A}}$ for $1 \leq l \leq n$, we have

$$a_1a_2\cdots a_m = c_1c_2\cdots c_m + \sum_{K\subsetneq[m]} (-1)^{m-|K|} \prod_{k\in[m]\setminus K} \varphi(c_k) \cdot \vec{\prod_{k\in K}} c_k$$

and

$$b_1b_2\cdots b_n = d_1d_2\cdots d_n + \sum_{L\subsetneq[n]} (-1)^{n-|L|} \prod_{l\in[n]\setminus L} \varphi(d_l) \cdot \vec{\prod_{l\in L}} d_l.$$

Thus, by bi-linearity of ψ, we get

$$\psi[a_1a_2\cdots a_m, b_1b_2\cdots b_n] - \sum_{K\subsetneq[m]} \sum_{L\subsetneq[n]} (-1)^{m+n-|K|-|L|} \prod_{k\in[m]\setminus K} \varphi(c_k) \prod_{l\in[n]\setminus L} \varphi(d_l)\ \psi\left[\vec{\prod_{k\in K}} c_k, \vec{\prod_{l\in L}} d_l\right]$$

$$= \psi[c_1c_2\cdots c_m, d_1d_2\cdots d_n]$$

Moreover, the free independence condition of second order implies

$$\psi[a_1a_2\cdots a_m, b_1b_2\cdots b_n] = \delta_{m,n}\sum_{l=1}^{n}\prod_{k=1}^{m}\varphi(a_kb_{l-k}),$$

and hence, we obtain

$$\delta_{m,n}\sum_{l=1}^{n}\prod_{k=1}^{m}\varphi(a_kb_{l-k}) - \sum_{K\subsetneq[m]}\sum_{L\subsetneq[n]}(-1)^{m+n-|K|-|L|}\prod_{k\in[m]\setminus K}\varphi(c_k)\prod_{l\in[n]\setminus L}\varphi(d_l)\ \psi\left[\prod_{k\in K}^{\vec{}}c_k, \prod_{l\in L}^{\vec{}}d_l\right] \tag{4.10}$$

$$= \psi[c_1c_2\cdots c_m, d_1d_2\cdots d_n]$$

By induction on $|K|+|L|$, each term in the sum in ‘ (4.10) is uniquely determined by the restrictions $\varphi|_{\mathcal{A}_i}$ and $\psi|_{\mathcal{A}_i\times\mathcal{A}_i}$ and by the complex second order free independence condition, and so is $\psi[c_1c_2\cdots c_m, d_1d_2\cdots d_n]$. □

Following along with the line of algebraic probability spaces and free independence, we obtain the corresponding notions of distribution, convergence in distribution, and asymptotic independence for second order probability spaces and free independence of second order. The *distribution of first and second order* of a family of random variables $\{a_i\}_{i\in I}$ in a second order probability space $(\mathcal{A},\varphi,\psi)$ is the pair (μ,ρ) where $\mu:\mathbb{C}\langle \mathrm{x}_i \mid i\in I\rangle\to\mathbb{C}$ is the unital linear functional defined by

$$\mu(\mathrm{p}) = \varphi(\mathrm{p}(\{a_i\}_{i\in I}))$$

for all polynomial $\mathrm{p}\in\mathbb{C}\langle \mathrm{x}_i \mid i\in I\rangle$ and $\rho:\mathbb{C}\langle \mathrm{x}_i \mid i\in I\rangle\times\mathbb{C}\langle \mathrm{x}_i \mid i\in I\rangle\to\mathbb{C}$ is the bi-linear functional given by

$$\rho(\mathrm{p},\mathrm{q}) = \psi\left(\mathrm{p}(\{a_i\}_{i\in I}), \mathrm{q}(\{a_i\}_{i\in I})\right)$$

for all polynomial $\mathrm{p}, \mathrm{q} \in \mathbb{C}\langle \mathrm{x}_i \mid i \in I\rangle$. Moreover, if $\{a_{N,i}\}_{i\in I}$ is a family of random variables from a complex probability space of second order $(\mathcal{A}_N, \varphi_N, \psi_N)$ for each integer $N \geq 1$, we say that the sequence $\{\{a_{N,i}\}_{i\in I}\}_{N=1}^{\infty}$ *converge in distribution of first and second order* to the family $\{a_i\}_{i\in I}$ if for all positive integers $m, n \geq 1$ and indexes $i_1, i_2, \ldots, i_m, j_1, j_2, \ldots, j_n \in I$ we have

$$\lim_{N\to\infty} \varphi_N\left(a_{N,i_1} a_{N,i_2} \cdots a_{N,i_m}\right) = \varphi\left(a_{i_1} a_{i_2} \cdots a_{i_m}\right)$$

and

$$\lim_{N\to\infty} \psi_N\left(a_{N,i_1} a_{N,i_2} \cdots a_{N,i_m}, a_{N,j_1} a_{N,j_2} \cdots a_{N,j_N}\right) = \psi\left(a_{i_1} a_{i_2} \cdots a_{i_m}, a_{j_1} a_{j_2} \cdots a_{j_m}\right).$$

Finally, if the sequence $\{\{a_{N,i}\}_{i\in I}\}_{N=1}^{\infty}$ converge in distribution of first and second order to the family $\{a_i\}_{i\in I}$ and the family $\{a_i\}_{i\in I}$ is complex second order free with respect to (φ, ψ), we say that the sequence $\{\{a_{N,i}\}_{i\in I}\}_{N=1}^{\infty}$ is *asymptotically freely independent of second order*, or simply, *asymptotically second order free*.

As it might be expected, an specific limiting probability space is not needed for convergence in distribution of first and second order. Indeed, suppose (μ_N, ρ_N) is the distribution of first and second order of family of random variables $\{a_{N,i}\}_{i\in I}$ from a complex probability space of second order $(\mathcal{A}_N, \varphi_N, \psi_N)$ for each integer $N \geq 1$. The sequence $\{\{a_{N,i}\}_{i\in I}\}_{N=1}^{\infty}$ converge in distribution of first and second order if and only if $\lim_{N\to\infty} \mu_N[\mathrm{p}]$ and $\lim_{N\to\infty} \rho_N[\mathrm{p}, \mathrm{q}]$ exist for all polynomials $\mathrm{p}, \mathrm{q} \in \mathbb{C}\langle \mathrm{x}_i \mid i \in I\rangle$. For random matrix ensembles, convergence in distribution of first and second order is referred as having a second order limiting distribution and takes the following form.

Definition 4.3.5. We say that a random matrix ensemble $\{\{X_{N,i}\}_{i\in I}\}_{N=1}^{\infty}$ has a *second order limiting distribution* if for all polynomials $\mathrm{p}_1, \mathrm{p}_2, \mathrm{p}_3, \ldots$ from the algebra $\mathbb{C}\langle \mathrm{x}_i \mid i \in I\rangle$,

letting $Y_{N,k} = \mathrm{p}_k(\{X_{N,i}\}_{i\in I})$ for $k = 1, 2, \ldots$, we have:

(i) $\lim_{N\to\infty} \mathbb{E}\left[\mathrm{tr}\left(Y_{N,1}\right)\right]$ exists,

(ii) $\lim_{N\to\infty} \mathrm{cov}\left[\mathrm{Tr}\left(Y_{N,1}\right), \mathrm{Tr}\left(Y_{N,2}\right)\right]$ exists, and

(iii) $\lim_{N\to\infty} \mathfrak{c}_n\left[\mathrm{Tr}\left(Y_{N,1}\right), \mathrm{Tr}\left(Y_{N,2}\right), \ldots, \mathrm{Tr}\left(Y_{N,r}\right)\right] = 0$ for $n \geq 3$.

Rigorously, condition (iii) above is not required for the convergence in distribution of first and second order of a random matrix ensemble $\{\{X_{N,i}\}_{i\in I}\}_{N=1}^{\infty}$. Each family of random matrices $\{X_{N,i}\}_{i\in I}$ is being regarded as a family of random variables in the complex second order probability space $(\mathrm{Mat}_N(L^{\infty-}), \mathbb{E}[\mathrm{tr}(\,\cdot\,)], \mathrm{cov}[\mathrm{Tr}(\,\cdot\,), \mathrm{Tr}(\,\cdot\,)])$, and hence, the convergence in distribution of first and second order of the ensemble $\{\{X_{N,i}\}_{i\in I}\}_{N=1}^{\infty}$ depends only on (i) and (ii) above. However, as pointed out in [10] and [11], condition (iii) is needed to ensure the convergence of mixed fluctuation moments in results such as Theorem 4.3.8 and Corollary 4.3.9 bellow, so it is just convenient to include it in the notion of second order limiting distribution of random matrix ensembles.

Now, an specific limiting probability space is also not essential for asymptotic free independence of second order. Note that if (μ_N, ρ_N) and $\{a_{N,i}\}_{i\in I}$ are as above for each integer $N \geq 1$, the sequence $\{\{a_{N,i}\}_{i\in I}\}_{N=1}^{\infty}$ is asymptotically second order free if and only if $\lim_{N\to\infty} \mu_N[\mathrm{p}]$ and $\lim_{N\to\infty} \rho_N[\mathrm{p}, \mathrm{q}]$ exists for all $\mathrm{p}, \mathrm{q} \in \mathbb{C}\langle \mathrm{x}_i \mid i \in I\rangle$ and the family of unital sub-algebras $\{\mathbb{C}[\mathrm{x}_i]\}_{i\in I}$ is complex second order free independent with respect to $\mu := \lim_{N\to\infty} \mu_N$ and $\rho := \lim_{N\to\infty} \rho_N$. Following similar arguments to those in Proposition 3.1.5 and Proposition 4.3.18, we obtain the next result.

Proposition 4.3.6. Suppose $\mu_N : \mathbb{C}\langle \mathrm{x}_i \mid i \in I\rangle \to \mathbb{C}$ is a linear functional and assume $\rho_N : \mathbb{C}\langle \mathrm{x}_i \mid i \in I\rangle \times \mathbb{C}\langle \mathrm{x}_i \mid i \in I\rangle \to \mathbb{C}$ is a bi-linear functional for each integer $N \geq 1$.

The family of unital sub-algebras $\{\mathbb{C}[\mathrm{x}_i]\}_{i\in I}$ is complex second order free independent with respect to $(\lim_{N\to\infty}\mu_N, \lim_{N\to\infty}\rho_N)$ if and only if the following three conditions hold:

(1) $\lim\limits_{N\to\infty}\mu_N[\mathrm{p}]$ exists for every polynomial $\mathrm{p}\in\mathbb{C}\langle \mathrm{x}_i \mid i\in I\rangle\to\mathbb{C}$ and the family of unital sub-algebras $\{\mathbb{C}[\mathrm{x}_i]\}_{i\in I}$ is order free independent with respect to $\mu := \lim\limits_{N\to\infty}\mu_N$,

(2) $\lim\limits_{N\to\infty}\rho_N[\mathrm{p},\mathrm{q}]$ exist for all polynomials $\mathrm{p}\in\mathbb{C}[\mathrm{x}_i]$ and $\mathrm{q}\in\mathbb{C}[\mathrm{x}_j]$ and indexes $i,j\in I$,

(3) for all integers $m_1, m_2 \geq 1$ and indexes $i_1, i_2, \ldots, i_{m_1}, j_1, j_2, \ldots, j_{m_2} \in I$ with $i_1 \neq i_2, \ldots, i_{m_1-1} \neq i_{m_1}, i_{m_1} \neq i_1$ and $j_1 \neq j_2, \ldots, j_{m_2-1} \neq j_{m_2}, j_{m_2} \neq j_1$, if we take $\mathrm{p}_k \in \mathbb{C}[\mathrm{x}_{i_k}]$ and $\mathrm{q}_l \in \mathbb{C}[\mathrm{x}_{j_l}]$ for $1\leq k\leq m_1$ and $1\leq l\leq m_2$, then

$$\lim_{N\to\infty}\rho_N\left[(\mathrm{p}_1-\mu_N(\mathrm{p}_1))\cdots\left(\mathrm{p}_{m_1}-\mu_N(\mathrm{p}_{m_1})\right),(\mathrm{q}_1-\mu_N(\mathrm{q}_1))\cdots\left(\mathrm{q}_{m_1}-\mu_N(\mathrm{q}_{m_2})\right)\right] = \delta_{m_1,m_2}\lim_{N\to\infty}\sum_{l=1}^{m_2}\prod_{k=1}^{m_1}\mu_N\left[(\mathrm{p}_k-\mu_N(\mathrm{p}_k))(\mathrm{q}_{l-k}-\mu_N(\mathrm{q}_{l-k}))\right]$$

where $l-k$ is taken modulo m_2; moreover, if $m_1 = m_2 = 1$ and $i_1 \neq j_1$, we require

$$\lim_{N\to\infty}\rho_N\left[(\mathrm{p}_1-\mu_N(\mathrm{p}_1)),(\mathrm{q}_1-\mu_N(\mathrm{q}_1))\right] = 0.$$

Having a second order limiting distribution, in the sense of Definition 4.3.5, is required in the most common definition of asymptotic free independence of second order for random matrix ensembles. More concretely, random matrix ensembles $\{X_{N,i}\}_{N=1}^{\infty}$ with $i\in I$ are said to be *asymptotically freely independent of second order*, or simply, *asymptotically second order free*, if the ensemble $\{\{X_{N,i}\}_{i\in I}\}_{N=1}^{\infty}$ has a second order limiting distribution and converges in distribution of first and second order to a complex second order free family of random variables $\{a_i\}_{i\in I}$. As a result of Proposition 4.3.6, we are able to reformulate the notion of asymptotic free independence of second order as follows.

Definition 4.3.7. We say that the random matrix ensembles $\{X_{N,i}\}_{N=1}^{\infty}$ with $i \in I$ are *asymptotically freely independent of second order*, or simply, *asymptotically second order free*, if they are asymptotically freely independent and the following three conditions are satisfied:

(ASOF.1) $\lim_{N\to\infty} \mathrm{Cov}\left[\mathrm{Tr}(X_{N,i}^m), \mathrm{Tr}(X_{N,i}^n)\right]$ exists for each index $i \in I$ and all integers $m, n \geq 1$,

(ASOF.2) for all integers $m_1, m_2 \geq 1$, indexes $i_1, i_2, \ldots, i_{m_1}, j_1, j_2, \ldots, j_{m_2} \in I$ satisfying $i_1 \neq i_2, \ldots, i_{m_1-1} \neq i_{m_1}, i_{m_1} \neq i_1$ and $j_1 \neq j_2, \ldots, j_{m_2-1} \neq j_{m_2}, j_{m_2} \neq j_1$, and polynomials $\mathrm{p}_1, \mathrm{p}_2, \ldots, \mathrm{p}_{m_1}, \mathrm{q}_1, \mathrm{q}_2, \ldots, \mathrm{q}_{m_2}$ in the algebra $\mathbb{C}[\mathrm{x}]$, if we take $Y_N = Y_{N,1}Y_{N,2}\cdots Y_{N,m_1}$ and $Z_N = Z_{N,1}Z_{N,2}\cdots Z_{N,m_2}$ with $Y_{N,k}$ and $Z_{N,l}$ given by (4.6) for $1 \leq k \leq m_1$ and $1 \leq l \leq m_2$, we have

$$\lim_{N\to\infty} \mathrm{Cov}\left[\mathrm{Tr}(Y_N), \mathrm{Tr}(Z_N)\right] = \delta_{m_1,m_2} \lim_{N\to\infty} \sum_{l=1}^{m_1} \prod_{k=1}^{m_2} \mathbb{E}\left[\mathrm{tr}\left(Y_{N,k}Z_{N,l-k}\right)\right] \tag{4.11}$$

where $l-k$ is taken modulo m_2; moreover, if $m_1 = m_2 = 1$ and $i_1 \neq j_1$, we require

$$\lim_{N\to\infty} \mathrm{cov}\left[\mathrm{Tr}\left(Y_{N,1}\right), \mathrm{Tr}\left(Z_{N,1}\right)\right] = 0,$$

(ASOF.3) for ever integer $n \geq 3$, all polynomials $\mathrm{p}_1, \mathrm{p}_2, \ldots, \mathrm{p}_n$ in the algebra of non-commutative polynomials $\mathbb{C}\langle \mathrm{x}_i \mid i \in I\rangle$, letting $Y_{N,k} = \mathrm{p}_k\left(\{X_{N,i}\}_{i\in I}\right)$, we have

$$\lim_{N\to\infty} \mathfrak{c}_n\left[\mathrm{Tr}\left(Y_{N,1}\right), \mathrm{Tr}\left(Y_{N,2}\right), \ldots, \mathrm{Tr}\left(Y_{N,n}\right)\right] = 0$$

Independent Gaussian Unitary Ensembles, independent Haar-unitary ensembles, and independent complex Wishart ensembles are among those ensembles known to exhibit asymptotic second order free independence, see [13, 12]. All of the above ensembles are unitarily-invariant, in the sense that their matrix-distribution is invariant under conjugation by unitary matrices, and the fact that they are asymptotically second order free can be seen as a particular case of the following general theorem from [11].

Theorem 4.3.8. Suppose $\{X_{N,i}\}_{i\in I}$ is a family of independent N-by-N unitarily invariant random matrix for every integer $N \geq 1$. Then $\{\{X_{N,i}\}_{i\in I}\}_{N=1}^{\infty}$ is asymptotically second order free. Additionally, if an ensemble $\{\{D_{N,i}\}_{i\in I}\}_{N=1}^{\infty}$ has a second order limiting distribution and is independent from $\{\{X_{N,i}\}_{i\in I}\}_{N=1}^{\infty}$, then $\{\{X_{N,i}\}_{i\in I}\}_{N=1}^{\infty}$ and $\{\{D_{N,i}\}_{i\in I}\}_{N=1}^{\infty}$ are asymptotically second order free.

As a consequence, conjugation by independent Haar-unitary random matrices gives rise to asymptotic free independence of second order.

Corollary 4.3.9. Suppose $\{U_{N,i}\}_{i\in I}$ are independent N-by-N Haar-distributed random unitary matrices for each integer $N \geq 1$. If $\{\{D_{N,i}\}_{i\in I}\}_{N=1}^{\infty}$ has a second order limiting distribution, then $\{\{U_{N,i}D_{N,i}U_{N,i}^*\}_{i\in I}\}_{N=1}^{\infty}$ is asymptotically second order free.

Note that conjugation by unitary matrices does not change individual distributions in the sense that for all random matrices D_N and U_N from $\mathrm{Mat}_N(L^{\infty-})$ with U_N unitary, we have $\mathbb{E}\left[\mathrm{tr}((U_N^*D_NU_N)^m)\right] = \mathbb{E}\left[\mathrm{tr}(D_N^m)\right]$ and $\mathrm{cov}\left[\mathrm{Tr}\left((U_N^*D_NU_N)^m\right), \mathrm{Tr}\left((U_N^*D_NU_N)^n\right)\right] = \mathrm{cov}\left[\mathrm{Tr}\left(D_N^m\right), \mathrm{Tr}\left(D_N^n\right)\right]$. Thus, conjugation by Haar-unitary random ensembles allows us to construct asymptotically second order free random matrices with arbitrary distributions of first and second order.

Real case

Although independent Gaussian Unitary Ensembles and independent Gaussian Orthogonal Ensembles exhibit the same asymptotic behavior of first order, both of them are asymptotically free by Theorem 4.2.1, they display distinct behavior of second order. This distinction was first noted by E. Redelmeier in [18] where the fluctuation moments of independent Gaussian Unitary Ensembles are computed.

Theorem 4.3.10. Suppose $\{\{X_{N,i}\}_{N=1}^{\infty}\}_{i\in I}$ is a family of independent Gaussian Orthogonal Ensembles. Then the fluctuation moments of $\{\{X_{N,i}\}_{i\in I}\}_{N=1}^{\infty}$ are determined by the following condition: given integers $m_1, m_2 \geq 1$, polynomials $\mathrm{p}_1, \mathrm{p}_2, \ldots, \mathrm{p}_{m_1}, \mathrm{q}_1, \mathrm{q}_2, \ldots, \mathrm{q}_{m_2} \in \mathbb{C}[\mathrm{x}]$ and indexes $i_1, i_2, \ldots, i_{m_1}, j_1, j_2, \ldots, j_{m_2} \in I$, if we take

$$Y_{N,k} = \mathrm{p}_k\left(X_{N,i_k}\right) - \mathbb{E}\left[\mathrm{tr}\left(\mathrm{p}_k\left(X_{N,i_k}\right)\right)\right] I_N \text{ and } Z_{N,l} = \mathrm{q}_l\left(X_{N,j_l}\right) - \mathbb{E}\left[\mathrm{tr}\left(\mathrm{q}_l\left(X_{N,j_l}\right)\right)\right] I_N$$

for $1 \leq k \leq m_1$ and $1 \leq l \leq m_2$, then

$$\begin{aligned} &\lim_{N\to\infty} \mathrm{cov}\Big[\mathrm{Tr}\left(Y_{N,1}Y_{N,2}\cdots Y_{N,m_1}\right), \mathrm{Tr}\left(Z_{N,1}Z_{N,2}\cdots Z_{N,m_2}\right)\Big] = \\ &\delta_{m_1,m_2} \lim_{N\to\infty} \sum_{l=1}^{m_2} \left(\prod_{k=1}^{m_1} \mathbb{E}\left[\mathrm{tr}\left(Y_{N,k}Z_{N,l-k}\right)\right] + \prod_{k=1}^{m_1} \mathbb{E}\left[\mathrm{tr}\left(Y_{N,k}Z_{N,l+k}^{T}\right)\right]\right) \end{aligned} \tag{4.12}$$

provided $i_1 \neq i_2, i_2 \neq i_3, \ldots, i_{m_1-1} \neq i_{m_1}, i_{m_1} \neq i_1, j_1 \neq j_2, \ldots, j_{m_2-1} \neq j_{m_2}, j_{m_2} \neq j_1$.

It was also proved by E. Redelmeier in [18] that independent real Ginibre ensembles and independent real Wishart ensembles exhibit the same fluctuation moments as independent Gaussian Orthogonal Ensembles. The appearance of (4.12) in several random matrix ensembles led E. Redelmeier to introduce the notions of real second order probability space and real second order free independence.

Definition 4.3.11. A *real second order probability space* is a quadruple $(\mathcal{A}, \varphi, \rho, t)$ consisting of a second order algebraic probability space $(\mathcal{A}, \varphi, \rho)$ and an involution $t : \mathcal{A} \to \mathcal{A}$, called *transpose*, such that $(ab)^t = b^t a^t$, $\varphi(a) = \varphi(a^t)$, and $\rho(a, b) = \rho(a^t, b) = \rho(a, b^t)$ for all random variables $a, b \in \mathcal{A}$.

Definition 4.3.12. Let $(\mathcal{A}, \varphi, \rho, t)$ be a real second order probability space. A family $\{\mathcal{A}_i\}_{i\in I}$ of unital sub-algebras of $\mathcal{A}$, invariant under $a \mapsto a^t$, is said to be *real second order free* with respect to (φ, ρ) if

i) the family $\{\mathcal{A}_i\}_{i\in I}$ is free with respect to φ, and

ii) for all positive integers $m, n \geq 1$, indexes $i_1, i_2, \ldots, i_m, j_1, j_2, \ldots, i_n \in I$ with $i_1 \neq i_2, \ldots, i_{m-1} \neq i_m, i_m \neq i_1$ and $j_1 \neq j_2, \ldots, j_{n-1} \neq j_n, j_n \neq j_1$, and random variables $a_k \in \mathcal{A}_{i_k}$ and $b_l \in A_{j_l}$ with $\varphi(a_k) = \varphi(b_m) = 0$ for $1 \leq k \leq m$ and $1 \leq l \leq n$ we have

$$\rho(a_1 a_2 \cdots a_m, b_1 b_2 \cdots b_n) = \delta_{m,n} \sum_{l=1}^{N} \left(\prod_{k=1}^{m} \varphi(a_k b_{l-k}) + \prod_{k=1}^{m} \varphi(a_k b_{l+k}^t) \right)$$

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

We could perform a similar analysis than the one we did for complex second order probability spaces and define the notions of t-distribution, convergence in t-distribution, and asymptotic real second order free independence in purely algebraic terms. However, since both analysis would be very similar and our main focus is on random matrices, we simply present these notions in terms of random matrices ensembles. Note that if $T : \mathrm{Mat}_N(L^{\infty-}) \to \mathrm{Mat}_N(L^{\infty-})$ is the function that maps a matrix to its transpose, then $(\mathrm{Mat}_N(L^{\infty-}), \mathbb{E}[\mathrm{tr}(\,\cdot\,)], \mathrm{cov}[\mathrm{Tr}(\,\cdot\,), \mathrm{Tr}(\,\cdot\,)], T)$ is a real second order probability space.

Definition 4.3.13. We say that a random matrix ensemble $\{\{X_{N,i}\}_{i\in I}\}_{N=1}^{\infty}$ has a *second order limiting t-distribution* if $\{\{X_{N,i}, X_{N,i}^T\}_{i\in I}\}_{N=1}^{\infty}$ has a second order limiting distribution.

Definition 4.3.14. We say that the random matrix ensembles $\{X_{N,i}\}_{N=1}^{\infty}$ with $i \in I$ are *asymptotically real second order free* if $\{\{X_{N,i}, X_{N,i}^T\}_{i\in I}\}_{N=1}^{\infty}$ is asymptotically freely independent and the following three conditions are satisfied:

(ASOF.1) $\lim_{N\to\infty} \mathrm{Cov}\left[\mathrm{Tr}(\mathrm{p}(X_{N,i}, X_{N,i}^T)), \mathrm{Tr}(\mathrm{q}(X_{N,i}, X_{N,i}^T))\right]$ exists for each index $i \in I$ and all polynomials $\mathrm{p}, \mathrm{q} \in \mathbb{C}\langle \mathrm{x}, \mathrm{x}^T\rangle$,

(ASOF.2) for all integers $m_1, m_2 \geq 1$, all indexes $i_1, i_2, \ldots, i_{m_1}, j_1, j_2, \ldots, j_{m_2} \in I$ with $i_1 \neq i_2, i_2 \neq i_3, \ldots, i_{m_1-1} \neq i_{m_1}, i_{m_1} \neq i_1, j_1 \neq j_2, \ldots, j_{m_2-1} \neq j_{m_2}, j_{m_2} \neq j_1$, and all polynomials $\mathrm{p}_1, \mathrm{p}_2, \ldots, \mathrm{p}_{m_1}, \mathrm{q}_1, \mathrm{q}_2, \ldots, \mathrm{q}_{m_2}$ in the algebra $\mathbb{C}\langle \mathrm{x}, \mathrm{x}^T\rangle$, if we take

$$Y_{N,k} = \mathrm{p}_k\left(X_{N,i_k}, X_{N,i_k}^T\right) - \mathbb{E}\left[\mathrm{tr}\left(\mathrm{p}_k\left(X_{N,i_k}, X_{N,i_k}^T\right)\right)\right] I_N$$

and

$$Z_{N,l} = \mathrm{q}_l\left(X_{N,j_l}, X_{N,j_l}^T\right) - \mathbb{E}\left[\mathrm{tr}\left(\mathrm{q}_l\left(X_{N,j_l}, X_{N,j_l}^T\right)\right)\right] I_N$$

for $1 \leq k \leq m_1$ and $1 \leq l \leq m_2$, then

$$\lim_{N\to\infty} \mathrm{cov}\Big[\mathrm{Tr}\left(Y_{N,1}Y_{N,2}\cdots Y_{N,m_1}\right), \mathrm{Tr}\left(Z_{N,1}Z_{N,2}\cdots Z_{N,m_2}\right)\Big] = \delta_{m_1,m_2} \lim_{N\to\infty} \sum_{l=1}^{m_2} \left(\prod_{k=1}^{m_1} \mathbb{E}\left[\mathrm{tr}\left(Y_{N,k}Z_{N,l-k}\right)\right] + \prod_{k=1}^{m_1} \mathbb{E}\left[\mathrm{tr}\left(Y_{N,k}Z_{N,l+k}^T\right)\right]\right)$$

where $l-k$ is taken modulo m_2; additionally, if $m_1 = m_2 = 1$ and $i_1 \neq j_1$, we require

$$\lim_{N\to\infty} \mathrm{cov}\left[\mathrm{Tr}\left(Y_{N,1}\right), \mathrm{Tr}\left(Z_{N,1}\right)\right] = 0,$$

(ASOF.3) for ever integer $n \geq 3$, all polynomials $\mathrm{p}_1, \mathrm{p}_2, \ldots, \mathrm{p}_n$ in the algebra of non-commutative polynomials $\mathbb{C}\left\langle \mathrm{x}_i, \mathrm{x}_i^T \mid i \in I\right\rangle$, letting $Y_{N,k} = \mathrm{p}_k\left(\{X_{N,i}, X_{N,i}^T\}_{i\in I}\right)$,

we have

$$\lim_{N\to\infty} \mathfrak{c}_n \left[\mathrm{Tr}\left(Y_{N,1}\right), \mathrm{Tr}\left(Y_{N,2}\right), \ldots, \mathrm{Tr}\left(Y_{N,n}\right)\right] = 0$$

The random matrix ensembles analyzed by E. Redelmeier in [18] are orthogonally-invariant, their matrix-distribution is invariant under conjugation by orthogonal matrices. It was showed by J. Mingo and M. Popa [11] that orthogonal invariance leads to asymptotic real second order free independence, just as unitary invariance leads to asymptotic complex second order free independence. Specifically, J. Mingo and M. Popa showed the following.

Theorem 4.3.15. Suppose $\{X_{N,i}\}_{i\in I}$ is a family of independent N-by-N orthogonally invariant random matrix for every integer $N \geq 1$. Then $\{\{X_{N,i}\}_{i\in I}\}_{N=1}^{\infty}$ is asymptotically real second order free. Additionally, if the sequence $\{\{D_{N,i}\}_{i\in I}\}_{N=1}^{\infty}$ has a second order limiting t-distribution, then $\{\{X_{N,i}\}_{i\in I}\}_{N=1}^{\infty}$ and $\{\{D_{N,i}\}_{i\in I}\}_{N=1}^{\infty}$ are asymptotically real second order free.

Corollary 4.3.16. Suppose $\{U_{N,i}\}_{i\in I}$ are independent N-by-N Haar-distributed random orthogonal matrices for each integer $N \geq 1$. If $\{\{D_{N,i}\}_{i\in I}\}_{N=1}^{\infty}$ has a second order limiting t-distribution, then $\{\{U_{N,i}D_{N,i}U_{N,i}^*\}_{i\in I}\}_{N=1}^{\infty}$ is asymptotically real second order free.

The bounded cumulants property

As mentioned earlier, condition (iii) from Definition 4.3.5 is not needed for the convergence in distribution of first and second order of a random matrix ensemble $\{\{X_{N,i}\}_{i\in I}\}_{N=1}^{\infty}$, it is only needed to ensure the convergence of mixed fluctuation moments. In most cases, see [10, 11], this condition can be replaced with the bounded cumulants property.

Definition 4.3.17. A random matrix ensemble $\{\{X_{N,i}\}_{i\in I}\}_{N=1}^{\infty}$ is said to have the *bounded cumulants property* if for all polynomials $\mathrm{p}_1, \mathrm{p}_2, \mathrm{p}_3, \ldots$ in the algebra of non-commutative

polynomials $\mathbb{C}\langle \mathrm{x}_i \mid i \in I\rangle$ taking $Y_{N,k} = \mathrm{p}_k(\{X_{N,i}\}_{i\in I})$ we have

$$\sup_N \left| \mathfrak{c}_n \left[\mathrm{Tr}\left(Y_{N,1}\right), \mathrm{Tr}\left(Y_{N,2}\right), \ldots, \mathrm{Tr}\left(Y_{N,n}\right)\right] \right| < \infty \tag{4.13}$$

for every integer $n \geq 2$.

The bounded cumulants property for the random matrix ensemble $\{\{X_{N,i}\}_{i\in I}\}_{N=1}^{\infty}$ can be formulated in terms of multi-linear funtionals as follows. Let $\mathcal{A}$ be the algebra of non-commutative polynomials $\mathbb{C}\langle \mathrm{x}_i \mid i \in I\rangle$ and let $\mathcal{A}_i$ be the algebra of polynomials $\mathbb{C}[x_i]$ for each $i \in I$. For each integer $N \geq 1$, let us consider the n-linear map $\rho_N : \mathcal{A} \times \cdots \times \mathcal{A} \to \mathbb{C}$ defined by

$$\rho_N\left[\mathrm{p}_1, \mathrm{p}_2, \ldots, \mathrm{p}_n\right] = \mathfrak{c}_n\left[\mathrm{Tr}\left(\mathrm{p}_1(\{X_{N,i}\}_{i\in I})\right), \ldots, \mathrm{Tr}\left(\mathrm{p}_n(\{X_{N,i}\}_{i\in I})\right)\right] \tag{4.14}$$

for all polynomials $\mathrm{p}_1, \mathrm{p}_2, \ldots, \mathrm{p}_n \in \mathcal{A}$ and where $\mathfrak{c}_n[\cdot, \ldots, \cdot]$ denotes the classical cumulant from Section 2.1. The random matrix ensemble $\{\{X_{N,i}\}_{i\in I}\}_{N=1}^{\infty}$ has then the bounded cumulants property if only if

$$\sup_N |\rho_N\left[\mathrm{p}_1, \mathrm{p}_2, \ldots, \mathrm{p}_n\right]| < \infty \tag{4.15}$$

for all $\mathrm{p}_1, \mathrm{p}_2, \ldots, \mathrm{p}_n \in \mathcal{A}$ and any integer $n \geq 2$. Let us now consider the joint distribution of each family $\{X_{N,i}\}_{i\in I}$, the unital linear functional $\mu_N : \mathbb{C}\langle \mathrm{x}_i \mid i \in I\rangle \to \mathbb{C}$ defined by

$$\mu_N\left(\mathrm{p}\right) = \mathbb{E}\left[\mathrm{tr}\left(\mathrm{p}\left(\{X_{N,i}\}_{i\in I}\right)\right)\right]$$

for every polynomial $\mathrm{p} \in \mathbb{C}\langle \mathrm{x}_i \mid i \in I\rangle$. If the ensemble $\{\{X_{N,i}\}_{i\in I}\}_{N=1}^{\infty}$ converge in distribution, i.e., $\lim_{N\to\infty} \mu_N\left[\mathrm{p}\right]$ exists for all polynomials $\mathrm{p} \in \mathcal{A}$, then each polynomial p_k appearing

in (4.15) can be replaced by

$$(\mathrm{p}_1^{(k)} - \mu_N[\mathrm{p}_1^{(k)}])(\mathrm{p}_2^{(k)} - \mu_N[\mathrm{p}_2^{(k)}]) \cdots (\mathrm{p}_{m_k}^{(k)} - \mu_N[\mathrm{p}_{m_k}^{(k)}])$$

for some polynomials $\mathrm{p}_1^{(k)} \in \mathcal{A}_{i_1^{(k)}}, \mathrm{p}_2^{(k)} \in \mathcal{A}_{i_2^{(k)}}, \ldots, \mathrm{p}_{m_k}^{(k)} \in \mathcal{A}_{i_{m_k}^{(k)}}$ and still get the bounded cumulants property under a mild additional condition.

Proposition 4.3.18. Let $\mathcal{A}$ be an algebra over $\mathbb{C}$ and let $\mathcal{A}_i \subset \mathcal{A}$ be a sub-algebra for each $i \in I$ so that the family of sub-algebras $\{\mathcal{A}_i\}_{i\in I}$ generate the algebra $\mathcal{A}$. Suppose $\mu_N : \mathcal{A} \to \mathbb{C}$ is linear functional and $\rho_N : \mathcal{A} \times \cdots \times \mathcal{A} \to \mathbb{C}$ is an n-linear functional for each $N \geq 1$ such that $\lim_{N\to\infty} \mu_N[\mathrm{p}]$ and $\lim_{N\to\infty} \rho_N[\mathrm{p}_1, \mathrm{p}_2, \ldots, \mathrm{p}_n]$ exist for all $\mathrm{p} \in \mathcal{A}, \mathrm{p}_1 \in \mathcal{A}_{i_1}, \mathrm{p}_2 \in \mathcal{A}_{i_2}, \ldots, \mathrm{p}_n \in \mathcal{A}_{i_n}$ with $i_1, i_2, \ldots, i_n \in I$. Then the following three conditions are equivalent:

(a) $\sup_N |\rho_N[\mathrm{p}_1, \mathrm{p}_2, \ldots, \mathrm{p}_n]| < \infty$ for all $\mathrm{p}_1, \mathrm{p}_2, \ldots, \mathrm{p}_n \in \mathcal{A}$

(b) $\sup_N |\rho_N[\mathrm{q}_1, \mathrm{q}_2, \ldots, \mathrm{q}_n]| < \infty$ if each q_k is of the form

$$\mathrm{q}_k = \mathrm{p}_1^{(k)} \mathrm{p}_2^{(k)} \cdots \mathrm{p}_{m_k}^{(k)}$$

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

(c) $\sup_N |\rho_N[\mathrm{q}_{N,1}, \mathrm{q}_{N,2}, \ldots, \mathrm{q}_{N,n}]| < \infty$ if each $\mathrm{q}_{N,k}$ is of the form

$$\mathrm{q}_{N,k} = (\mathrm{p}_1^{(k)} - \mu_N[\mathrm{p}_1^{(k)}])(\mathrm{p}_2^{(k)} - \mu_N[\mathrm{p}_2^{(k)}]) \cdots (\mathrm{p}_{m_k}^{(k)} - \mu_N[\mathrm{p}_{m_k}^{(k)}])$$

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

Proof. Conditions (a) and (b) 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 (a) implies (c) and (c) implies (b).

Suppose (a) holds and let $\mathrm{q}_{N,k}$ is as in (c) for $k = 1, 2, \ldots, n$. Then, by multi-linearity, we have

$$\rho_N\left[\mathrm{q}_{N,1}, \ldots, \mathrm{q}_{N,n}\right] = \sum_{J_1\subset[m_1],\ldots,J_n\subset[m_n]} \left(\prod_{k=1}^{n}\prod_{j\in J_k^c}(-1)^{|J_k^c|}\mu_N[\mathrm{p}_j^{(k)}]\right)\cdot\rho_N\left[\vec{\prod_{j\in J_1}}\mathrm{p}_j^{(1)}, \ldots, \vec{\prod_{j\in J_n}}\mathrm{p}_j^{(k)}\right]$$

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

Let us assume now (c) holds and let J be the set of all positive integers I satisfying the following property: if $m = m_1+m_2+\cdots+m_n$ for some positive integers $m_1, m_2, \ldots, m_n$, and $\mathrm{p}_j^{(k)} \in \mathcal{A}_{i_j^{(k)}}$ for $j = 1, 2, \ldots, m_k$ and $i_1^{(k)} \neq i_2^{(k)}, i_2^{(k)} \neq i_3^{(k)}, \ldots, i_{m_k-1}^{(k)} \neq i_{m_k}^{(k)}$ for $k = 1, 2, \ldots, n$, then $\sup_N|\rho_N(\mathrm{q}_1, \mathrm{q}_2, \ldots, \mathrm{q}_n)| < \infty$ where each q_k is given by $\mathrm{q}_k = \mathrm{p}_1^{(k)}\mathrm{p}_2^{(k)}\cdots\mathrm{p}_{m_k}^{(k)}$. Note that we are done if we show that $J = \{n, n+1, n+2, \ldots\}$. By hypothesis, n belongs to J, so let us assume $n, n+1, \ldots, m-1$ belong to J and let $\mathrm{p}_j^{(k)}$, $\mathrm{q}_{N,k}$ and q_k as above. Consider the equality

$$\begin{aligned}&\rho_N\left[\mathrm{q}_{N,1}, \ldots, \mathrm{q}_{N,n}\right] - \rho_N\left[\mathrm{q}_1, \ldots, \mathrm{q}_n\right]\\ &= \sum_{\substack{J_1\subset[m_1],\ldots,J_n\subset[m_n]\\ \cup_k^n J_k^c\neq\emptyset}} \left(\prod_{k=1}^{n}\prod_{j\in J_k^c}(-1)^{|J_k^c|}\mu_N[\mathrm{p}_i^{(k)}]\right)\cdot\rho_N\left[\vec{\prod_{j\in J_1}}\mathrm{p}_j^{(1)}, \ldots, \vec{\prod_{j\in J_n}}\mathrm{p}_j^{(k)}\right].\end{aligned}$$

given by n-linearity of ρ_N. Now, since (c) holds, $\rho_N(\mathrm{q}_{N,1}, \ldots, \mathrm{q}_{N,n})$ is uniformly bounded with respect to N and, by induction hypothesis, so is $\rho_N[\vec{\prod}_{j\in J_1}\mathrm{p}_j^{(k)}, \ldots, \vec{\prod}_{j\in J_n}\mathrm{p}_j^{(k)}]$ if at least one J_k is not $[m_k]$. Thus, $\rho_N(\mathrm{q}_1, \ldots, \mathrm{q}_n)$ is also uniformly bounded with respect to N, and hence I belongs to J. □

Very similar arguments show that the previous result still holds if we replace the supremum by the limit.

Proposition 4.3.19. If $\mathcal{A}$, $\mathcal{A}_i$, μ_N, and ρ_N be as in Proposition 4.3.19, then the following are equivalent:

(a) $\lim_{N\to\infty} \rho_N[\mathrm{p}_1, \mathrm{p}_2, \ldots, \mathrm{p}_n]$ exists for all $\mathrm{p}_1, \mathrm{p}_2, \ldots, \mathrm{p}_n \in \mathcal{A}$

(b) $\lim_{N\to\infty} \rho_N[\mathrm{q}_1, \mathrm{q}_2, \ldots, \mathrm{q}_n]$ exists if each q_k is of the form

$$\mathrm{q}_k = \mathrm{p}_1^{(k)}\mathrm{p}_2^{(k)}\cdots\mathrm{p}_{m_k}^{(k)}$$

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

(c) $\lim_{N\to\infty} \rho_N[\mathrm{q}_{N,1}, \mathrm{q}_{N,2}, \ldots, \mathrm{q}_{N,n}]$ exists if each $\mathrm{q}_{N,k}$ is of the form

$$\mathrm{q}_{N,k} = (\mathrm{p}_1^{(k)} - \mu_N[\mathrm{p}_1^{(k)}])(\mathrm{p}_2^{(k)} - \mu_N[\mathrm{p}_2^{(k)}])\cdots(\mathrm{p}_{m_k}^{(k)} - \mu_N[\mathrm{p}_{m_k}^{(k)}])$$

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

Now, if each multi-linear functional $\rho_N : \mathcal{A}\times\cdots\times\mathcal{A} \to \mathbb{C}$ in Proposition 4.3.18 is *tracial in each entry*, i.e., for ever integer $k \in [n]$ and polynomials $\mathrm{q}_0, \mathrm{q}_1, \ldots, \mathrm{q}_n \in \mathcal{A}$, we have

$$\rho_N[\mathrm{q}_1, \ldots, \mathrm{q}_{k-1}, \mathrm{q}_0\mathrm{q}_k, \mathrm{q}_{k+1}, \ldots, \mathrm{q}_n] = \rho_N[\mathrm{q}_1, \ldots, \mathrm{q}_{k-1}, \mathrm{q}_k\mathrm{q}_0, \mathrm{q}_{k+1}, \ldots, \mathrm{q}_n],$$

we can impose the condition that $i_{m_k}^{(k)} \neq i_1^{(k)}$ in (b) and (c) from Proposition 4.3.18 and still get uniform boundedness of $\rho_N[\mathrm{p}_1, \mathrm{p}_2, \ldots, \mathrm{p}_n]$ with respect to N.

Corollary 4.3.20. Suppose $\mathcal{A}$, $\mathcal{A}_i$, μ_N, and ρ_N are as in Proposition 4.3.18. If ρ_N is tracial in each entry, then condition (a) from Proposition 4.3.18 is equivalent to any of the following:

(b') $\sup_N |[\mathrm{q}_1, \mathrm{q}_2, \ldots, \mathrm{q}_n]| < \infty$ if each q_k is of the form $\mathrm{q}_k = \mathrm{p}_1^{(k)}\mathrm{p}_2^{(k)}\cdots\mathrm{p}_{m_k}^{(k)}$ with $\mathrm{p}_j^{(k)} \in \mathcal{A}_{i_j^{(k)}}$ and $i_1^{(k)} \neq i_2^{(k)}, i_2^{(k)} \neq i_3^{(k)}, \ldots, i_{m_k-1}^{(k)} \neq i_{m_k}^{(k)}$, and $i_{m_k}^{(k)} \neq i_1^{(k)}$

(c') $\sup_N |\rho_N[\mathrm{q}_{N,1}, \mathrm{q}_{N,2}, \ldots, \mathrm{q}_{N,n}]| < \infty$ if each $\mathrm{q}_{N,k}$ is of the form

$$\mathrm{q}_{N,k} = (\mathrm{p}_1^{(k)} - \mu_N[\mathrm{p}_1^{(k)}])(\mathrm{p}_2^{(k)} - \mu_N[\mathrm{p}_2^{(k)}])\cdots(\mathrm{p}_{m_k}^{(k)} - \mu_N[\mathrm{p}_{m_k}^{(k)}])$$

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

Proof. Note that while condition (b) from Proposition 4.3.18 allows the indexes i_1^k and $i_{m_k}^k$ to be possibly the same, condition (b') above explicitly prohibits this. Thus, by traciality of ρ_N in each entry, we have that (b') and (b) are equivalent, and hence, it only remains to show that (c') above implies (c) from Proposition 4.3.18.

Assume (c') holds and let J be the set of all positive integers I satisfying the following property: if $m = m_1+m_2+\cdots+m_n$ for some positive integers $m_1, m_2, \ldots, m_n$, and $\mathrm{p}_j^{(k)} \in \mathcal{A}_{i_j^{(k)}}$ for $j = 1, 2, \ldots, m_k$ and $i_1^{(k)} \neq i_2^{(k)}, i_2^{(k)} \neq i_3^{(k)}, \ldots, i_{m_k-1}^{(k)} \neq i_{m_k}^{(k)}$ for $k = 1, 2, \ldots, n$, then

$$\sup_N |\rho_N[\mathrm{q}_{N,1}, \mathrm{q}_{N,2}, \ldots, \mathrm{q}_{N,n}]| < \infty \tag{4.16}$$

where each $\mathrm{q}_{N,k}$ as above. By hypothesis, n belongs to J, so let us assume $n, n+1, \ldots, m-1$ belong to J and let $\mathrm{p}_j^{(k)}$, $\mathrm{q}_{N,k}$ and q_k as above. Thus, if $i_{m_k}^{(k)} \neq i_1^{(k)}$ for $k = 1, 2, \ldots, n$, Inequality (4.16) holds. On the other hand, if $i_{m_k}^{(k)} = i_1^{(k)}$ for some $k \in \{1, 2, \ldots, n\}$, let us consider polynomials $\widetilde{\mathrm{p}}_{N,k}$ and $\widetilde{\mathrm{r}}_{N,k}$ given by

$$\begin{aligned}\widetilde{\mathrm{p}}_{N,k} =& (\mathrm{p}_{m_k}^{(k)} - \mu_N[\mathrm{p}_{m_k}^{(k)}])(\mathrm{p}_1^{(k)} - \mu_N[\mathrm{p}_1^{(k)}])\\ \widetilde{\mathrm{r}}_{N,k} =& (\mathrm{p}_2^{(k)} - \mu_N[\mathrm{p}_2^{(k)}])(\mathrm{p}_3^{(k)} - \mu_N[\mathrm{p}_3^{(k)}])\cdots(\mathrm{p}_{m_k-1}^{(k)} - \mu_N[\mathrm{p}_{m_k-1}^{(k)}])\end{aligned}$$

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

$$\rho_N\left[\mathrm{q}_{N,1},\ldots,\mathrm{q}_{N,k},\ldots,\mathrm{q}_{N,n}\right]=\rho_N\left[\mathrm{q}_{N,1},\ldots,\widetilde{\mathrm{p}}_{N,k}\widetilde{\mathrm{r}}_{N,k},\ldots,\mathrm{q}_{N,n}\right];$$

moreover, from the relation

$$\begin{aligned}\widetilde{\mathrm{p}}_{N,k}=&(\mathrm{p}_{m_k}^{(k)}\mathrm{p}_1^{(k)}-\mu_N[\mathrm{p}_{m_k}^{(k)}\mathrm{p}_1^{(k)}])+\mu_N[\mathrm{p}_{m_k}^{(k)}\mathrm{p}_1^{(k)}]-\mu_N[\mathrm{p}_{m_k}^{(k)}]\mu_N[\mathrm{p}_1^{(k)}]\\&-\mu_N[\mathrm{p}_{m_k}^{(k)}](\mathrm{p}_1^{(k)}-\mu_N[\mathrm{p}_1^{(k)}])-\mu_N[\mathrm{p}_1^{(k)}](\mathrm{p}_{m_k}^{(k)}-\mu_N[\mathrm{p}_{m_k}^{(k)}])\end{aligned}$$

we get the equality

$$\begin{aligned}\rho_N[\mathrm{q}_{N,1},\ldots,\mathrm{q}_{N,n}]=&\rho_N[\mathrm{q}_{N,1},\ldots,(\mathrm{p}_{m_k}^{(k)}\mathrm{p}_1^{(k)}-\mu_N[\mathrm{p}_{m_k}^{(k)}\mathrm{p}_1^{(k)}])\widetilde{\mathrm{r}}_{N,k},\ldots,\mathrm{q}_{N,n}]\\&+\mu_N[\mathrm{p}_{m_k}^{(k)}\mathrm{p}_1^{(k)}]\rho_N[\mathrm{q}_{N,1},\ldots,\widetilde{\mathrm{r}}_{N,k},\ldots,\mathrm{q}_{N,n}]\\&-\mu_N[\mathrm{p}_{m_k}^{(k)}]\mu_N[\mathrm{p}_1^{(k)}]\rho_N[\mathrm{q}_{N,1},\ldots,\widetilde{\mathrm{r}}_{N,k},\ldots,\mathrm{q}_{N,n}]\\&-\mu_N[\mathrm{p}_1^{(k)}]\rho_N[\mathrm{q}_{N,1},\ldots,(\mathrm{p}_{m_k}^{(k)}-\mu_N[\mathrm{p}_{m_k}^{(k)}])\widetilde{\mathrm{r}}_{N,k},\ldots,\mathrm{q}_{N,n}]\\&-\mu_N[\mathrm{p}_{m_k}^{(k)}]\rho_N[\mathrm{q}_{N,1},\ldots,(\mathrm{p}_1^{(k)}-\mu_N[\mathrm{p}_1^{(k)}])\widetilde{\mathrm{r}}_{N,k},\ldots,\mathrm{q}_{N,n}]\end{aligned}$$

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 $\rho_N[\mathrm{q}_{N,1},\ldots,\mathrm{q}_{N,n}]$. □

4.4 Asymptotic liberation of deterministic matrices

The notion of asymptotically liberating random matrix ensemble, introduced by G. Anderson and B. Farren in [1], aims to enclose those random unitary matrix ensembles that give rise

to asymptotic free independence when used for conjugation of constant matrices, a feature already seen in matrix ensembles composed of independent Haar-unitary random matrices or independent Haar-orthogonal random matrices. As we describe next, this notion arises naturally from the application of Corollary 3.2.5 to random matrices.

Let I be an index set. Assume $D_{N,i}$ is a deterministic matrix in $\mathrm{Mat}_N(\mathbb{C})$ and $U_{N,i}$ is a random unitary matrix in $\mathrm{Mat}_N(L^{\infty-})$ for each index $i \in I$ and each integer $N \geq 1$. We would like to find sufficient conditions for the random matrix ensembles $\{U_{N,i}^* D_{N,i} U_{N,i}\}_{N=1}^{\infty}$ with $i \in I$ to be asymptotically freely independent. To that end, let us consider the joint distribution of the collection of random matrices $\{U_{N,i}^* D_{N,i} U_{N,i}\}_{i \in I}$, the unital linear functional $\mu_N : \mathbb{C}\langle \mathrm{x}_i \mid i \in I \rangle \to \mathbb{C}$ given by

$$\mu_N(\mathrm{p}) := \mathbb{E}\left[\mathrm{tr}\left(\mathrm{p}\left(\{U_{N,i}^* D_{N,i} U_{N,i}\}_{i \in I}\right)\right)\right]$$

for every polynomial $\mathrm{p} \in \mathbb{C}\langle \mathrm{x}_i \mid i \in I \rangle$. By Corollary 3.2.5, the random matrix ensembles $\{U_{N,i}^* D_{N,i} U_{N,i}\}_{N=1}^{\infty}$ with $i \in I$ are asymptotically freely independent if and only if the following two conditions hold:

(i) $\lim_{N \to \infty} \mu_N(\mathrm{x}_i^k)$ exists for every integer $k \geq 1$ and every index $i \in I$ and

(ii) $\lim_{N \to \infty} \mu_N\left((\mathrm{p}_1 - \mu_N(\mathrm{p}_1))(\mathrm{p}_2 - \mu_N(\mathrm{p}_2)) \cdots (\mathrm{p}_m - \mu_N(\mathrm{p}_m))\right) = 0$ for all integers $m \geq 2$, indexes $i_1, \ldots, i_m \in I$ with $i_1 \neq i_2$, …, $i_{m-1} \neq i_m$, and polynomials $\mathrm{p}_1 \in \mathbb{C}[\mathrm{x}_{i_1}], \mathrm{p}_2 \in \mathbb{C}[\mathrm{x}_{i_2}], \ldots, \mathrm{p}_m \in \mathbb{C}[\mathrm{x}_{i_m}]$.

Note that conjugation by unitary matrices does not modify individual distribution, meaning that for each index $i \in I$ we have

$$\mu_N(\mathrm{x}_i^k) = \mathbb{E}\left[\mathrm{tr}((U_{N,i}^* D_{N,i} U_{N,i})^k)\right] = \mathrm{tr}(D_{N,i}^k)$$

for every integer $k \geq 1$, and hence, since the condition (i) above must hold, we have to assume each matrix ensemble $\{D_{N,i}\}_{N=1}^{\infty}$ has a limiting distribution, i.e., $\lim_{N\to\infty} \mathrm{tr}(D_{N,i}^k)$ exists for every integer $k \geq 1$. Therefore, the feature of unitary ensembles inducing asymptotic free independence on constant matrices relies primarily on whether or not the unitary ensembles make the condition (ii) above hold. Suppose $\mathrm{p}_1, \mathrm{p}_2, \ldots, \mathrm{p}_m$ are polynomials as in (ii) above and note that if $\mathrm{q} \in \mathbb{C}[\mathrm{x}_{i'}]$ for some $i' \in I$, then

$$\mathrm{q}\left(\{U_{N,i}^* D_{N,i} U_{N,i}\}_{i\in I}\right) = \mathrm{q}\left(U_{N,i'}^* D_{N,i'} U_{N,i'}\right) = U_{N,i'}^* \mathrm{q}\left(D_{N,i'}\right) U_{N,i'}.$$

Thus, letting $\mathrm{q}_{N,k} = \mathrm{p}_k - \mu_N(\mathrm{p}_k) \in \mathbb{C}[\mathrm{x}_{i_k}]$ and $A_{N,k} = \mathrm{q}_{N,k}\left(D_{N,i_k}\right)$ for $1 \leq k \leq m$, we have

$$\mu_N\left(\mathrm{q}_{N,1}\mathrm{q}_{N,2}\cdots\mathrm{q}_{N,m}\right) = \mathbb{E}\left[\mathrm{tr}\left((U_{N,i_1}^* A_{N,1} U_{N,i_1})(U_{N,i_2}^* A_{N,2} U_{N,i_2})\cdots(U_{N,i_m}^* A_{N,m} U_{N,i_m})\right)\right].$$

Moreover, each matrix $A_{N,k}$ is of trace zero since $\mu_N(\mathrm{p}_k) = \mathrm{tr}\left(\mathrm{p}_k(D_{N,i_k})\right)$ implies $A_{N,k} = \mathrm{p}_k(D_{N,i_k}) - \mathrm{tr}(\mathrm{p}_k(D_{N,i_k}))I_N$. Therefore, the random matrix ensembles $\{U_{N,i}^* D_{N,i} U_{N,i}\}_{N=1}^{\infty}$ with $i \in I$ are asymptotically freely independent provided

$$\lim_{N\to\infty} \frac{1}{N}\mathbb{E}\left[\mathrm{Tr}\left((U_{N,i_1}^* A_{N,1} U_{N,i_1})\cdots(U_{N,i_m}^* A_{N,m} U_{N,i_m})\right)\right] = 0 \tag{4.17}$$

for all indexes $i_1, \ldots, i_m \in I$ satisfying $i_1 \neq i_2$, …, $i_{m-1} \neq i_m$ and matrices $A_{N,1}, \ldots, A_{N,m} \in \mathrm{Mat}_N(\mathbb{C})$ of trace zero.

Definition 4.4.1. Let $\{U_{N,i}\}_{i\in I}$ be a family of N-by-N random unitary matrices for each integer $N \geq 1$. The random unitary matrix ensemble $\{\{U_{N,i}\}_{i\in I}\}_{N=1}^{\infty}$ is said to be *asymptotically liberating* if for every integer $m \geq 2$ and indexes $i_1, \ldots, i_m \in I$ satisfying $i_1 \neq i_2, \ldots, i_{m-1} \neq i_m$, there exists a constant $C(i_1, \ldots, i_m)$ depending only on the m-tuple

$(i_1, i_2, \ldots, i_m)$ such that

$$\left|\mathbb{E}\big[\mathrm{Tr}(U_{N,i_1}A_{N,1}U_{N,i_1}^* \cdots U_{N,i_m}A_{N,m}U_{N,i_m}^*)\big]\right| \leq C(i_1, \ldots, i_m)\prod_{k=1}^{m}\|A_{N,k}\| \tag{4.18}$$

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

In view of (4.17) and (4.18), to conclude that random matrix ensembles $\{U_{N,i}D_{N,i}U_{N,i}^*\}_{N=1}^{\infty}$ with $i \in I$ are asymptotically free, provided $\{\{U_{N,i}\}_{i\in I}\}_{N=1}^{\infty}$ is asymptotically liberating and $\lim_{N\to\infty}\mathrm{tr}(D_{N,i}^k)$ exists for every integer $k \geq 1$ and every index $i \in I$, we still need a condition ensuring that if $A_{N,k} = \mathrm{p}_k(D_{N,i_k}) - \mathrm{tr}(\mathrm{p}_k(D_{N,i_k}))I_N$ for any given polynomial $\mathrm{p}_k \in \mathbb{C}[\mathrm{x}]$ and index $i_k \in I$ with $k = 1, 2, \ldots, m$, then

$$\sup_{N\geq 1}\prod_{k=1}^{m}\|A_{N,k}\| < \infty.$$

Note that if $\mathrm{p}(\mathrm{x}) = \sum_{j=0}^{n}\alpha_j\mathrm{x}^j \in \mathbb{C}[\mathrm{x}]$ and we take $A_N = \mathrm{p}(D_{N,i}) - \mathrm{tr}(\mathrm{p}(D_{N,i}))I_N$, then

$$\|A_N\| \leq \|\mathrm{p}(D_{N,i})\| + \|\mathrm{tr}(\mathrm{p}(D_{N,i}))I_N\| \leq 2\sum_{j=0}^{n}|\alpha_j|\|D_{N,i}\|^j.$$

Therefore, the desired condition is the uniform boundedness of each sequence $\{D_{N,i}\}_{N=1}^{\infty}$ with respect to the operator norm, namely, $\sup_{N\geq 1}\|D_{N,i}\| < \infty$.

Theorem 4.4.2. Let $\{D_{N,i}\}_{i\in I}$ be a family of N-by-N deterministic matrices for each integer $N \geq 1$ such that $\sup_{N\geq 1}\|D_{N,i}\| < \infty$ and $\lim_{N\to\infty}\mathrm{tr}(D_{N,i}^k)$ exists for ever integer $k \geq 1$ and every index $i \in I$. If $\{\{U_{N,i}\}_{i\in I}\}_{N=1}^{\infty}$ is an asymptotically liberating random unitary matrix ensemble, then $\{U_{N,i}D_{N,i}U_{N,i}^*\}_{N=1}^{\infty}$ with $i \in I$ are asymptotically freely independent.

Although conjugation of constant matrices by any asymptotically liberating ensemble does give rise to asymptotic free independence, provided individual distributions exist and

each ensemble is uniformly bounded with respect to the operator norm, nothing has been said about the existence of liberating ensembles. Moreover, matrix ensembles composed of independent Haar-unitary random matrices, or independent Haar-orthogonal random matrices, should be asymptotically liberating since we want the notion of asymptotically liberating ensemble to enclose those random unitary matrix ensembles that induce asymptotic free independence when used for conjugation. The next theorem, due to G. Anderson and B. Farren in [1], addresses these two concerns by establishing sufficient conditions on a random unitary matrix ensemble $\{\{U_{N,i}\}_{i\in I}\}_{N=1}^{\infty}$ to be asymptotically liberating.

Theorem 4.4.3. Let $\{U_{N,i}\}_{i\in I}$ be a family of N-by-N random unitary matrices for each integer $N \geq 1$. Suppose the following two conditions hold:

(I) for every integer $N \geq 1$ and every signed permutation matrix $\mathrm{W} \in \mathrm{Mat}_N(\mathbb{C})$ the families $\{U_{N,i_1}^* U_{N,i_2}\}_{i_1,i_2\in I}$ and $\{\mathrm{W}^* U_{N,i_1}^* U_{N,i_2}\mathrm{W}\}_{i_1,i_2\in I}$ are equal in distribution and

(II) for all integers $p \geq 1$ and indexes $i_1, i_2 \in I$ with $i_1 \neq i_2$ we have

$$\sup_{N\geq 1} \max_{1\leq j_1,j_2\leq N} \sqrt{N}\left\|\left(U_{N,i_1}^* U_{N,i_2}\right)(j_1,j_2)\right\|_p < \infty$$

Then the ensemble $\{\{U_{N,i}\}_{i\in I}\}_{N=1}^{\infty}$ is asymptotically liberating.

Note that matrix ensembles composed of independent Haar-unitary random matrices, or independent Haar-orthogonal random matrices, are asymptotically liberating. Suppose U_{N,i_1} and U_{N,i_2} are independent Haar-unitary (resp. Haar-orthogonal) random matrices. 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. The distribution of $U_{N,i_1}^* U_{N,i_2}$ is unitarily-invariant and each entry of a Haar-unitary (resp. Haar-orthogonal) is approximately a centered complex (resp. real) Gaussian random variable of variance $1/N$.

Another ensemble known to be asymptotically liberating is the unitary random matrix ensemble $\{W_N, H_N W_N/\sqrt{N}, X_N H_N W_N/\sqrt{N}\}_{N=1}^{\infty}$ 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. This is actually a consequence of a more general result due to G. Anderson and B. Farrel in [1] that we state next.

Theorem 4.4.4. Suppose W_N is an N-by-N uniformly distributed random signed permutation matrix, $\{X_{N,i}\}_{i\in I}$ is a family of independent N-by-N uniformly distributed signature matrices independent from W_N, and $H_N \in \mathrm{Mat}_N(\mathbb{C})$ is a complex Hadamard matrix for each integer $N \geq 1$. Then the random unitary matrix ensemble

$$\left\{\left\{W_N, \tfrac{1}{\sqrt{N}} H_N W_N\right\} \cup \left\{\tfrac{1}{\sqrt{N}} X_{N,i} H_N W_N \mid i \in I\right\}\right\}_{N=1}^{\infty}$$

satisfies hypothesis (I) and (II) from Theorem 4.4.3, and therefore, it is asymptotically liberating.

We end this section with a proposition that allows to reformulate the notion of asymptotically liberating ensemble. By traciality, the constants $C(i_1, \ldots, i_m)$ from Definition 4.4.1 can be taken with or without the additional condition that $i_m \neq i_1$.

Proposition 4.4.5. A random unitary matrix ensemble $\{\{U_{N,i}\}_{i\in I}\}$ is asymptotically liberating (if and only) if for every integer $m \geq 2$ and indexes $i_1, \ldots, i_m \in I$ satisfying $i_1 \neq i_2, i_2 \neq i_3, \ldots, i_{m-1} \neq i_m$, and $i_m \neq i_1$ there exists a constant $C(i_1, \ldots, i_m)$, depending only on $(i_1, \ldots, i_m)$ such that inequality (4.18) holds for all positive integers $N \geq 1$ and N-by-N complex matrices $A_{N,1}, \ldots, A_{N,m}$ of trace zero.

Proof. Let J be the set of all positive integers $m \geq 2$ satisfying the following property: if the indexes $i_1, \ldots, i_m \in I$ satisfy $i_1 \neq i_2, i_2 \neq i_3, \ldots, i_{m-1} \neq i_m$, there exists a constant

$C(i_1, \ldots, i_m)$ independent from N such that

$$\left|\mathbb{E}\big[\mathrm{Tr}(U_{N,i_1}A_{N,1}U_{N,i_1}^* \cdots U_{N,i_m}A_{N,m}U_{N,i_m}^*)\big]\right| \leq C(i_1, \ldots, i_m) \prod_{k=1}^{m} \|A_{N,k}\| \tag{4.19}$$

for all integers $N \geq 1$ and matrices $A_{N,1}, \ldots, A_{N,m} \in \mathrm{Mat}_N(\mathbb{C})$ of trace zero. We will show that $J = \{m \in \mathbb{N} \mid m \geq 2\}$.

Suppose $2, 3, \ldots, m-1$ belong to J and assume we are given indexes $i_1, \ldots, i_m \in I$ satisfying $i_1 \neq i_2, i_2 \neq i_3, \ldots, i_{m-1} \neq i_m$ and matrices $A_{N,1}, A_{N,2}, \ldots, A_{N,m} \in \mathrm{Mat}_N(\mathbb{C})$ of trace zero. By hypothesis, if $i_1 \neq i_m$, there is a constant $C(i_1, \ldots, i_m)$ such that (4.19) holds, so we can assume $i_1 = i_m$; moreover, if $m = 2$ and $i_1 = i_m$, then we have

$$\left|\mathbb{E}\big[\mathrm{Tr}(U_{N,i_1}A_{N,1}U_{N,i_1}^*U_{N,i_2}A_{N,2}U_{N,i_2}^*)\big]\right| = \left|\mathrm{Tr}(A_{N,1}A_{N,2})\right| \leq \left\|A_{N,1}\right\|\left\|A_{N,2}\right\|,$$

so we can further assume $m \geq 3$. Now, consider the matrices X_N and A_N given by

$$X_N = (U_{N,i_2}A_{N,2}U_{N,i_2}^*)(U_{N,i_3}A_{N,3}U_{N,i_3}^*) \cdots (U_{N,i_{m-1}}A_{N,m-1}U_{N,i_{m-1}}^*)$$

and

$$A_N = A_{N,m}A_{N,1} - \frac{1}{N}\mathrm{Tr}(A_{N,m}A_{N,1})I_N,$$

and not that

$$\mathrm{Tr}\left(U_{N,i_1}A_{N,1}U_{N,i_1}^*U_{N,i_2}A_{N,2} \cdots U_{N,i_m}A_{N,m}U_{N,i_m}^*\right) = \mathrm{Tr}\left(U_{N,i_m}A_{N,m}U_{N,i_m}^*U_{N,i_1}A_{N,1}U_{N,i_1}^*X_N\right).$$

Moreover, since $i_1 = i_m$, we have $U_{N,i_m}^*U_{N,i_1} = I_N$, and hence, by linearity of the trace, we

get

$$\mathrm{Tr}\left(U_{N,i_m}A_{N,m}U_{N,i_m}^*U_{N,i_1}A_{N,1}U_{N,i_1}^*X_N\right) = \mathrm{Tr}\left(U_{N,i_1}A_NU_{N,i_1}^*X_N\right) + \frac{1}{N}\mathrm{Tr}\left(A_{N,m}A_{N,1}\right)\mathrm{Tr}\left(X_N\right)$$

By induction hypothesis, $m-1$ and $m-2$ belong to J, so there are constants $C(i_1,\ldots,i_{m-1})$ and $C(i_2,\ldots,i_{m-1})$ independent from N such that

$$\left|\mathbb{E}\big[\mathrm{Tr}(U_{N,i_1}A_NU_{N,i_1}^*X_N)\big]\right| \leq C(i_1,\ldots,i_{m-1})\|A_N\|\prod_{k=2}^{m-1}\|A_{N,k}\|$$

and

$$\left|\mathbb{E}\big[\mathrm{Tr}(X_N)\big]\right| \leq C(i_2,\ldots,i_{m-1})\prod_{k=2}^{m-1}\|A_{N,k}\|.$$

Thus, since $\left|\frac{1}{N}\mathrm{Tr}(A_{N,m}A_{N,1})\right| \leq \|A_{N,m}\|\|A_{N,1}\|$ and $\|A_N\| \leq 2\|A_{N,m}\|\|A_{N,1}\|$, if we take x $C(i_1,\ldots,i_m) = 2C(i_1,\ldots,i_{m-1}) + C(i_2,\ldots,i_{m-1})$, we obtain

$$\left|\mathbb{E}\big[\mathrm{Tr}(U_{N,i_1}A_{N,1}U_{N,i_1}^*\cdots U_{N,i_m}A_{N,m}U_{N,i_m}^*)\big]\right| \leq C(i_1,\ldots,i_m)\prod_{k=1}^{m}\|A_k\|\ .$$

Therefore, m belongs to J, and by induction on m, we conclude $J = \{m \in \mathbb{N} \mid m \geq 2\}$. $\square$

Chapter 5

Graph Sums of Square Matrices

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

$$\sum_{\substack{\mathbf{j}:[\pm m]\to[N]\\ \ker(\mathbf{j})\geq\pi}} A_1(j_{-1}, j_1)A_2(j_{-2}, j_2)\cdots A_m(j_{-m}, j_m) \quad = \sum_{\substack{\mathbf{j}:[\pm m]\to[N]\\ \ker(\mathbf{j})\geq\pi}} \prod_{k=1}^{m} A_k(j_{-k}, j_k) \tag{5.1}$$

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 $\pi = \{\{1, -2\}, \{2, -3\}, \ldots, \{m-1, -m\}, \{m, -1\}\}$, then $\ker(\mathbf{j}) \geq \pi$ only if $j_1 = j_{-2}, j_2 = j_{-3}, \ldots, j_{m-1} = j_{-m}$, and $j_m = j_{-1}$, and thus we get

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

It is worth mentioning that although the labeling of the entries of A_k in (5.1) is not customary, it has proven to be suitable for many of our calculations; moreover, for a bijection $\sigma : [\pm m] \to$

S, the relation

$$\sum_{\substack{\mathbf{j}:S\to[N]\\ \ker(\mathbf{j})\geq\hat{\pi}}}\prod_{k=1}^{m}A_k(j_{\sigma(-k)},j_{\sigma(k)})=\sum_{\substack{\mathbf{j}:[\pm m]\to[N]\\ \ker(\mathbf{j})\geq\sigma^{-1}\circ\hat{\pi}}}\prod_{k=1}^{m}A_k(j_{-k},j_k)\qquad\forall\hat{\pi}\in P(S)\tag{5.2}$$

provides the link between the labeling of the entries of A_k in (5.1) and any other labeling. For instance, if $\sigma:[\pm m]\to[2m]$ is given by $\sigma(-k)=2k-1$ and $\sigma(k)=2k$ for $1\leq k\leq m$, then

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

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

5.1 Bounds of graph sums of general square matrices

Suppose we are given a partition π in $P(\pm m)$ and let $\#(\pi)$ denote the number of blocks of π. Note that, for all integers $N\geq 1$ and all matrices $A_1,A_2,\ldots,A_m\in\mathrm{Mat}_N(\mathbb{C})$, we have

$$\left|\sum_{\substack{\mathbf{j}:[\pm m]\to[N]\\ \ker(\mathbf{j})\geq\pi}}\prod_{k=1}^{m}A_k(j_{-k},j_k)\right|\leq N^{\#(\pi)}\prod_{k=1}^{m}\|A_k\|\leq N^{2m}\prod_{k=1}^{m}\|A_k\|\tag{5.3}$$

since $\#(\pi) \leq 2m$ and $|A_k(j_{-k}, j_k)| \leq \|A_k\|$ for any matrix $A_k \in \mathrm{Mat}_N(\mathbb{C})$. Thus, we might ask for the least number $\tau \geq 0$ such that the inequality

$$\left| \sum_{\substack{\mathbf{j}:[\pm m]\to[N] \\ \ker(\mathbf{j})\geq\pi}} \prod_{k=1}^{m} A_k(j_{-k}, j_k) \right| \leq N^{\tau} \prod_{k=1}^{m} \|A_k\| \tag{5.4}$$

holds for all integers $N \geq 1$ and all matrices $A_1, A_2, \ldots, A_m \in \mathrm{Mat}_N(\mathbb{C})$. The minimal $\tau \geq 0$ satisfying (5.4) always exists since (5.3) holds, so we call such minimal τ the *graph sum exponent* of π and denote it by τ_π.

A main result in [14] states that the graph sum exponent τ_π can be algorithmically computed analyzing the two-edge connectedness of a graph associated to π. For the reader's convenience, we recount the algorithm from [14] next.

Step 1. Given a partition $\pi \in P(\pm m)$, consider the undirected graph $\mathcal{G}_\pi$ resulting from, first, taking edges $E_1, E_2, \ldots, E_m$ with endpoints $-1, +1, -2, +2, \ldots, -m, +m$, 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 $\mathcal{G}_\pi$. 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 $\mathcal{F}_\pi$ denote the graph with vertex set given by the set of all two-edge connected components of $\mathcal{G}_\pi$ and edge set given by the set of all cutting-edges of $\mathcal{G}_\pi$, the graph

sum exponent τ_π is given by

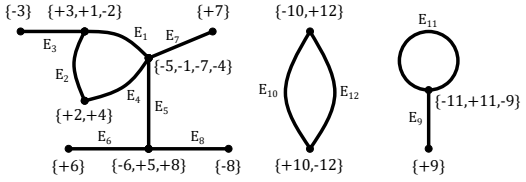
$$\tau_\pi = \sum_{v \text{ vertex in } \mathcal{F}_\pi} \mathfrak{l}(v) \quad \text{where} \quad \mathfrak{l}(v) := \begin{cases} \frac{1}{2} & \text{if } \deg(v) = 1, \\ 1 & \text{if } \deg(v) = 0, \\ 0 & \text{otherwise.} \end{cases} \tag{5.5}$$

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

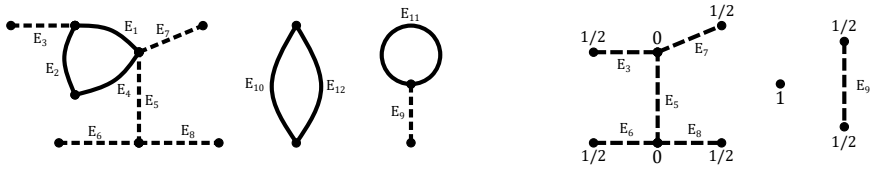
Example. The undirected graph $\mathcal{G}_\pi$ associated to the partition

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

can be represented as



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



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

The main result in [14] concerns more general graph sums, allowing the matrices A_k in (5.1) to be rectangular and not necessarily square. For graph sums of square matrices, however, the result takes the following form.

Theorem 5.1.1. Suppose π is a partition in $P(\pm m)$. If τ_π is computed as above, i.e., τ_π is given by (5.5), then the following two conditions hold:

(a) for all integers $N \geq 1$ and all matrices $A_1, A_2, \ldots, A_m \in \mathrm{Mat}_N(\mathbb{C})$ we have

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

(b) if $\tau \geq 0$ satisfies

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

for all integers $N \geq 1$ and all matrices $A_1, A_2, \ldots, A_m \in \mathrm{Mat}_N(\mathbb{C})$, then $\tau_\pi \leq \tau$.

Proposition 5.1.2. If $\pi \in P(\pm m)$ is an even partition, then the graph sum exponent τ_π equals the number of connected components of $\mathcal{G}_\pi$.

Proof. By Equation (5.5), it suffices to show that the graph $\mathcal{G}_\pi$ has no cutting-edges. Suppose $\mathcal{G}_\pi$ 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 vertexes 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, $\mathcal{G}_\pi$ has no cutting-edges, and hence all its connected components are two-edge connected. □

Remark 5.1.3. Resulting from endowing each edge E_k in the graph $\mathcal{G}_\pi$ 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 $\mathcal{G}_\pi$ are bouquets, to which we refer as multiple-loops, or cycles, each connected component gives rise to a trace. For example, for the partition

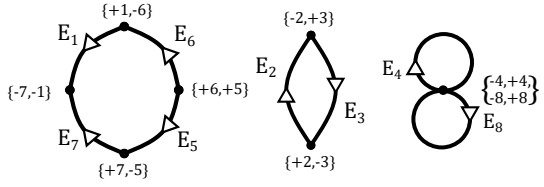
$$\pi = \{\{1,-6\},\{6,5\},\{-5,7\},\{-7,-1,\},\{-2,3\},\{-3,2\},\{-4,4\}\}$$

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

$$\sum_{\substack{\mathbf{j}:[\pm 7]\to[N]\\ \ker(\mathbf{j})\geq\pi}} \prod_{k=1}^{7} A_k(j_{-k}, j_k) = \mathrm{Tr}\left(A_1 A_6 A_5^T A_7^T\right) \mathrm{Tr}\left(A_2 A_3\right) \mathrm{Tr}\left(A_4 \circ A_8\right) \tag{5.6}$$

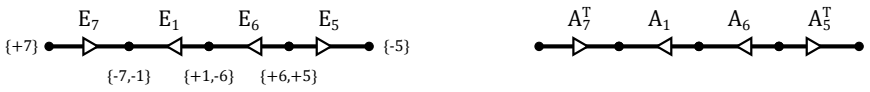
where the right hand side can be deduced from analyzing the directed graph $\vec{\mathcal{G}}_\pi$ as follows:

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 (5.6).

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 $\mathrm{Tr}\,(\cdot)$ 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



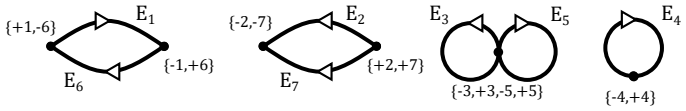
And so, we obtain the trace $\mathrm{Tr}\left(A_7^T A_1 A_6 A_5^T\right)$ in (5.6). Note that $\mathrm{Tr}\left(A_1 A_6 A_5^T A_7^T\right)$ and $\mathrm{Tr}\,(A_2 A_2)$ do not depend on how the cycles in $\vec{\mathcal{G}}_\pi$ are unfolded since for any matrices $A, B \in \mathrm{Mat}_N(\mathbb{C})$ we have $\mathrm{Tr}\,(AB) = \mathrm{Tr}\,(BA)$, $\mathrm{Tr}\,(A) = \mathrm{Tr}\left(A^T\right)$, and $(AB)^T = B^T A^T$.

3. On the other hand, a multiple-loop in $\vec{\mathcal{G}}_\pi$ with edges $E_{k_1}, E_{k_2}, \ldots, E_{k_n}$ yields to the trace of the Hadamard product of $A_{k_1}, A_{k_2}, \ldots, A_{k_n}$. This way, we get $\mathrm{Tr}\,(A_4 \circ A_8)$ in (5.6).

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

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

5.2 Bounds of graph sums of The Discrete Fourier Transform

Although the bound for graph sums given by Theorem 5.1.1 is optimal in the set of all square matrices, it might not 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

$$H(j_1, j_2) = \omega^{(j_1-1)(j_2-1)} \tag{5.7}$$

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

$$\mathbf{h}(\mathbf{j}) = \prod_{k=1}^{m} H(j_{-2k+1}, j_{2k-1}) H^*(j_{-2k}, j_{2k}) \tag{5.8}$$

for each function $\mathbf{j} : [\pm 2m] \to [N]$, Theorem 5.1.1 gives us that

$$\left| \sum_{\substack{\mathbf{j}:[\pm 2m]\to[N] \\ \ker(\mathbf{j}) \geq \pi}} \mathbf{h}(\mathbf{j}) \right| \leq N^{\tau_\pi} \prod_{k=1}^{m} \|H\| \prod_{k=1}^{m} \|H^*\| = N^{m+\tau_\pi} \tag{5.9}$$

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

$$\left| \sum_{\substack{\mathbf{j}:[\pm 2m]\to[N] \\ \ker(\mathbf{j}) \geq \pi}} \mathbf{h}(\mathbf{j}) \right| \leq \sum_{\substack{\mathbf{j}:[\pm 2m]\to[N] \\ \ker(\mathbf{j}) \geq \pi}} 1 = N^{\#(\pi)}. \tag{5.10}$$

Thus, if π is the partition $\{\{2k-1, -2k+1, 2k, -2k\} \mid k = 1, 2, \ldots, m\}$, then the graph sum exponent τ_π equals m, and hence $\tau_\pi + m = 2m$, but also $\#(\pi) = m$, so (5.10) is a sharper

bound than (5.9) in this case. In general, we prefer (5.10) over (5.9) since (5.10) is invariant under re-labeling of the entries of H and H^* in (5.8), namely, if $\sigma : [\pm 2m] \to [\pm 2m]$ is bijective and we take

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

for any function $\mathbf{j} : [\pm 2m] \to [N]$, then the inequality in (5.10) implies

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

since we have the relation

$$\sum_{\substack{\mathbf{j}:[\pm 2m]\to[N] \\ \ker(\mathbf{j}) \geq \pi}} \mathbf{h}(\mathbf{j} \circ \boldsymbol{\sigma}) \quad = \sum_{\substack{\mathbf{j}:[\pm 2m]\to[N] \\ \ker(\mathbf{j}) \geq \sigma^{-1} \circ \pi}} \mathbf{h}(\mathbf{j}). \tag{5.11}$$

Moreover, in the proof of Theorem 1.2.1, we will need to consider sums of the form

$$\sum_{\substack{\mathbf{j}:[\pm 2m]\to[N] \\ \ker(\mathbf{j}) = \pi}} \mathbf{h}(\mathbf{j} \circ \boldsymbol{\sigma}) \quad = \sum_{\substack{\mathbf{j}:[\pm 2m]\to[N] \\ \ker(\mathbf{j}) = \sigma^{-1} \circ \pi}} \mathbf{h}(\mathbf{j}) \tag{5.12}$$

where $m = m_1 + m_2$ for some integers $m_1, m_2 \geq 1$ and $\sigma : [\pm 2m] \to [\pm 2m]$ is the permutation with cycle decomposition given by

$$\sigma = (-1, 1, -2, 2, \ldots, -2m_1, 2m_1)(-2m_1 - 1, 2m_1 + 1, \ldots, -2m_1 - 2m_2, 2m_1 + 2m_2). \tag{5.13}$$

Although the sum in (5.12) is not a graph sum, it can be determined up to a term of order $N^{\#\pi-1}$ analyzing (5.11) since for every partition $\pi \in P(\pm 2m)$ we have

$$\sum_{\substack{\mathbf{j}:[\pm 2m]\to[N]\\ \ker(\mathbf{j})=\pi}} \mathbf{h}(\mathbf{j}) \quad = \sum_{\substack{\mathbf{j}:[\pm 2m]\to[N]\\ \ker(\mathbf{j})\geq\pi}} \mathbf{h}(\mathbf{j}) \quad - \sum_{\substack{\theta\in P(\pm 2m)\\ \theta>\pi}} \sum_{\substack{\mathbf{j}:[\pm 2m]\to[N]\\ \ker(\mathbf{j})=\theta}} \mathbf{h}(\mathbf{j}). \tag{5.14}$$

The rest of this section is devoted to find and classify partitions π such that (5.10) 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 $\pi = \{B_1, B_2, \ldots, B_r\} \in P(\pm 2m)$, we let $\mathrm{p}_\pi(\mathrm{x}_1, \mathrm{x}_2, \ldots, \mathrm{x}_r)$, or simply p_π, be the polynomial obtained from the expression

$$-\mathrm{x}_{-1}\mathrm{x}_1 + \mathrm{x}_{-2}\mathrm{x}_2 - \mathrm{x}_{-3}\mathrm{x}_3 + \cdots + \mathrm{x}_{-2m}\mathrm{x}_{2m} \tag{5.15}$$

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

$$\mathrm{p}_\pi(\mathrm{x}_1, \mathrm{x}_2, \mathrm{x}_3, \mathrm{x}_4) = -\mathrm{x}_1\mathrm{x}_2 + \mathrm{x}_3\mathrm{x}_3 - \mathrm{x}_2\mathrm{x}_1 + \mathrm{x}_4\mathrm{x}_4.$$

Equivalently, the polynomial $\mathrm{p}_\pi(\mathrm{x}_1, \mathrm{x}_2, \ldots, \mathrm{x}_r)$ is the image of (5.15) under the unique homomorphism from $\mathbb{Z}[\mathrm{x}_{-1}, \mathrm{x}_1, \ldots, \mathrm{x}_{-2m}, \mathrm{x}_{2m}]$ to $\mathbb{Z}[\mathrm{x}_1, \mathrm{x}_2, \ldots, \mathrm{x}_r]$ such that $\mathrm{x}_k \mapsto \mathrm{x}_l$ whenever $k \in B_l$. Note that $\mathrm{p}_\pi(\mathrm{x}_1, \mathrm{x}_2, \ldots, \mathrm{x}_r)$ has degree either 0 or 2 and can also be explicitly defined as

$$\mathrm{p}_\pi(\mathrm{x}_1, \mathrm{x}_2, \ldots, \mathrm{x}_r) = \sum_{1\leq t\leq s\leq r} a_{t,s}\mathrm{x}_t\mathrm{x}_s \tag{5.16}$$

where

$$a_{t,t} = \sum_{\substack{k\in[2m]\\ -k,k\in B_t}} (-1)^k \quad \text{and} \quad a_{t,s} = \sum_{\substack{k\in[2m]\\ -k\in B_t, k\in B_s}} (-1)^k + \sum_{\substack{l\in[2m]\\ l\in B_t, -l\in B_s}} (-1)^l \quad \text{for } t\neq s; \tag{5.17}$$

moreover, $\mathrm{p}_\pi(\mathrm{x}_1,\mathrm{x}_2,\ldots,\mathrm{x}_r)$ satisfies the relation

$$\sum_{\substack{\mathbf{j}:[\pm 2m]\to[N]\\ \ker(\mathbf{j})\geq\pi}} \mathbf{h}(\mathbf{j}) = \sum_{j_1,j_2,\ldots,j_r=0}^{N-1} e^{\frac{2\pi\sqrt{-1}}{N}\mathrm{p}_\pi(j_1,j_2,\ldots,j_r)}. \tag{5.18}$$

Therefore, (5.10) becomes an equality precisely when $\mathrm{p}_\pi(\mathrm{x}_1,\mathrm{x}_2,\ldots,\mathrm{x}_r)$ is the zero polynomial. On the other hand, if $\mathrm{p}_\pi(\mathrm{x}_1,\mathrm{x}_2,\ldots,\mathrm{x}_r)$ is a non-zero polynomial, we can then find a sharper bound than (5.10) 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

$$S(a,b,c) := \sum_{j=0}^{|c|-1} e^{\pi\sqrt{-1}\frac{aj^2+bj}{c}} = \left|\frac{c}{a}\right|^{\frac{1}{2}} e^{\pi\sqrt{-1}\frac{|ac|-b^2}{4ac}} \sum_{j=0}^{|a|-1} e^{\pi\sqrt{-1}\frac{-cj^2-bj}{a}} \tag{5.19}$$

Proposition 5.2.1. If $\mathrm{p}(\mathrm{x}_1,\mathrm{x}_2,\ldots,\mathrm{x}_r)$ is a non-zero polynomial of degree at most 2 in the algebra of polynomials with integer coefficients $\mathbb{Z}[\mathrm{x}_1,\mathrm{x}_2,\ldots,\mathrm{x}_r]$, then there exist a constant C_p independent of N such that

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

Proof. Suppose $\mathrm{p}(\mathrm{x}_1,\ldots,\mathrm{x}_r)\in\mathbb{Z}[\mathrm{x}_1,\ldots,\mathrm{x}_r]$ is a non-zero polynomial of degree at most

2. Without loss of generality, we can assume that there is a non-zero linear polynomial $\mathrm{q}_1(\mathrm{x}_1,\ldots,\mathrm{x}_r)=\alpha_1\mathrm{x}_1+\alpha_2\mathrm{x}_2+\cdots+\alpha_r\mathrm{x}_r\in\mathbb{Z}\left[\mathrm{x}_1,\mathrm{x}_2,\ldots,\mathrm{x}_r\right]$ and a polynomial $\mathrm{q}_2(\mathrm{x}_2,\ldots,\mathrm{x}_r)\in\mathbb{Z}\left[\mathrm{x}_2,\mathrm{x}_3,\ldots,\mathrm{x}_r\right]$ of degree at most 2 such that

$$\mathrm{p}(\mathrm{x}_1,\ldots,\mathrm{x}_r)=\mathrm{x}_1\mathrm{q}_1(\mathrm{x}_1,\ldots,\mathrm{x}_r)+\mathrm{q}_2(\mathrm{x}_2,\ldots,\mathrm{x}_r).$$

Since we have the inequality

$$\left|\sum_{j_1,j_2,\ldots,j_r=0}^{N-1}e^{-\frac{2\pi\sqrt{-1}}{N}\mathrm{p}(j_1,j_2,\ldots,j_r)}\right|\leq\sum_{j_2,\ldots,j_r=0}^{N-1}\left|\sum_{j_1=0}^{N-1}e^{-\frac{2\pi\sqrt{-1}}{N}j_1\mathrm{q}_1(j_1,j_2,\ldots,j_r)}\right|,$$

we only need to show that there is a constant C_{p} independent from N such that

$$\sum_{j_2,\ldots,j_r=0}^{N-1}\left|\sum_{j_1=0}^{N-1}e^{-\frac{2\pi\sqrt{-1}}{N}j_1\mathrm{q}_1(j_1,j_2,\ldots,j_r)}\right|\leq C_{\mathrm{p}}N^{r-\frac{1}{2}}.$$

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

$$\sum_{j_1=0}^{N-1}e^{-\frac{2\pi\sqrt{-1}}{N}j_1q(j_1,j_2,\ldots,j_m)}=\sum_{j_1=0}^{N-1}e^{\pi\sqrt{-1}\frac{-2\alpha_1j_1^2-2\sum_{k=2}^{r}\alpha_kj_kj_1}{N}}=S\left(-2\alpha_1,-2\sum_{k=2}^{r}\alpha_kj_k,N\right)$$

where $S(a,b,c)$ denotes the generalized Gauss quadratic sum as in (5.19). Thus, by the reciprocity theorem for generalized Gauss sums, we get

$$\left|S\left(-2\alpha_1,-2\sum_{k=2}^{r}\alpha_kj_k,N\right)\right|\leq\left|\frac{N}{-2a_1}\right|^{\frac{1}{2}}|-2a_1|=|2\alpha_1N|^{\frac{1}{2}},$$

and therefore, we obtain

$$\sum_{j_2,\ldots,j_r=0}^{N-1}\left|\sum_{j_1=0}^{N-1} e^{-\frac{2\pi\sqrt{-1}}{N}j_1\mathrm{q}_1(j_1,j_2,\ldots,j_r)}\right| \leq |2\alpha_1|^{\frac{1}{2}}N^{r-\frac{1}{2}}.$$

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

$$\sum_{j_1=0}^{N-1} e^{-\frac{2\pi\sqrt{-1}}{N}j_1\mathrm{q}_1(j_1,j_2,\ldots,j_r)} = \begin{cases} N, & \text{if } \mathrm{q}_1(j_1,\ldots,j_r) = \sum_{l=2}^{r}\alpha_l j_l \equiv 0 \mod N \\ 0, & \text{otherwise} \end{cases}$$

So, we have

$$\sum_{j_2,\ldots,j_r=0}^{N-1}\left|\sum_{j_1=0}^{N-1} e^{-\frac{2\pi\sqrt{-1}}{N}j_1\mathrm{q}_1(j_1,\ldots,j_r)}\right| =$$
$$N\cdot\#\left\{(j_2,\ldots,j_r)\in[0,N-1]^{r-1} : \sum_{l=2}^{r}\alpha_l j_l \equiv 0 \mod N\right\}.$$

But, since the polynomial $\mathrm{q}_1(\mathrm{x}_1,\ldots,\mathrm{x}_r) = \alpha_1\mathrm{x}_1+\cdots+\alpha_r\mathrm{x}_r$ is non-zero, we must have $\alpha_k \neq 0$ for some $k \neq 1$, and hence, the equation

$$\alpha_k\mathrm{x}+\beta \equiv 0 \mod N$$

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

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

and therefore, we get

$$\sum_{j_2,\ldots,j_r=0}^{N-1}\left|\sum_{j_1=0}^{N-1} e^{-\frac{2\pi\sqrt{-1}}{N}j_1 \mathrm{q}_1(j_1,j_2,\ldots,j_r)}\right| \leq |\alpha_k| N^{r-1}.$$

□

As an immediate consequence from (5.14), (5.18), and Proposition 5.2.1, we have the following.

Corollary 5.2.2. If $\mathrm{p}_\pi(\mathrm{x}_1, \mathrm{x}_2, \ldots, \mathrm{x}_r)$ is a non-zero polynomial for some given partition $\pi = \{B_1, B_2, \ldots, B_r\} \in P(\pm 2m)$, then there is a constant C independent from N so that

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

The next two propositions establish necessary and sufficient conditions for the polynomial $\mathrm{p}_\pi(\mathrm{x}_1, \mathrm{x}_2, \ldots, \mathrm{x}_r)$ to be zero. Roughly speaking, the polynomial $\mathrm{p}_\pi(\mathrm{x}_1, \mathrm{x}_2, \ldots, \mathrm{x}_r)$ is zero if only and 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 (5.15) cancel each other out.

Proposition 5.2.3. Suppose $\pi = \{B_1, B_2, \ldots, B_{2m}\}$ is a pairing partition in $P(\pm 2m)$. Then the polynomial $\mathrm{p}_\pi(\mathrm{x}_1, \mathrm{x}_2, \ldots, \mathrm{x}_{2m})$ 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 $\mathrm{p}_\pi(\mathrm{x}_1, \mathrm{x}_2, \ldots, \mathrm{x}_{2m})$ is the zero polynomial and take $a_{t,s}$ as (5.17) 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 exist 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 $\mathrm{p}_\pi(\mathrm{x}_1, \ldots, \mathrm{x}_{2m}) = \sum_{1 \le t \le s \le r} a_{t,s} \mathrm{x}_t \mathrm{x}_s$ is the zero polynomial, we must have $a_{t',s'} = 0$. Now, if $t' \neq s'$, from (5.17) we get that

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

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 $\pi = \{B_1, B_2, \ldots, B_{2m}\}$ with $B_1 = \{-k_1, -l_1\}, B_2 = \{k_1, l_1\}, B_3 = \{-k_2, -l_2\}, B_2 = \{k_2, l_2\}, \ldots, B_{2m} = \{k_m, l_{2m}\}$ and $k_1, l_1, k_2, l_2, \ldots, l_m \in [\pm 2m]$ satisfying $k_i + l_i$ odd for $i = 1, 2, \ldots, m$. Moreover, since $\bigcup_{i=1}^{2m} B_i = [\pm 2m]$ and $(-1)^k = (-1)^{-k}$ for $k \in [\pm 2m]$, we have

$$-\mathrm{x}_{-1}\mathrm{x}_1 + \mathrm{x}_{-2}\mathrm{x}_2 - \mathrm{x}_{-3}\mathrm{x}_3 + \cdots + \mathrm{x}_{-2m}\mathrm{x}_{2m} = \sum_{i=1}^{m} (-1)^{k_i} \mathrm{x}_{-k_i}\mathrm{x}_{k_i} + (-1)^{l_i} \mathrm{x}_{-l_i}\mathrm{x}_{l_i}.$$

Therefore, from the definition of $\mathrm{p}_\pi(\mathrm{x}_1, \mathrm{x}_2, \ldots, \mathrm{x}_{2m})$ and the fact that $k_i + l_i$ is odd for $i = 1, 2, \ldots, m$, we get

$$\mathrm{p}_\pi(\mathrm{x}_1, \mathrm{x}_2, \ldots, \mathrm{x}_{2m}) = \sum_{i=1}^{m} (-1)^{k_i} \mathrm{x}_{2i-1}\mathrm{x}_{2i} + (-1)^{l_i} \mathrm{x}_{2i-1}\mathrm{x}_{2i} = 0.$$

□

Proposition 5.2.4. Let $\pi = \{B_1, B_2, \ldots, B_n\}$ be a partition in $P(\pm 2m)$. If there is a partition $\theta \in P(\pm 2m)$ such that $\theta \le \pi$ 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 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 $\theta = \{B_{1,1}, B_{1,2}, \ldots, B_{1,m_1}, \ldots, B_{n,m_n}\}$ with $B_i = \cup_{j=1}^{m_i} B_{i,j}$ for $i = 1, 2, \ldots, n$. Take $\mathcal{A} = \mathbb{Z}[\mathrm{x}_1, \mathrm{x}_{-1}, \ldots, \mathrm{x}_{2m}, \mathrm{x}_{-2m}]$, $\mathcal{B} = \mathbb{Z}[\mathrm{x}_{1,1}, \mathrm{x}_{1,2}, \ldots, \mathrm{x}_{1,m_1}, \ldots, \mathrm{x}_{n,m_n}]$, and $\mathcal{C} = \mathbb{Z}[\mathrm{x}_1, \mathrm{x}_2, \ldots, \mathrm{x}_n]$ and let $\Phi : \mathcal{A} \to \mathcal{B}$ and $\Psi : \mathcal{B} \to \mathcal{C}$ be the unique homomorphisms such that $\Phi(\mathrm{x}_k) = \mathrm{x}_{i,j}$ if $k \in B_{i,j}$ and $\Psi(\mathrm{x}_{i,j}) = \mathrm{x}_i$. Note that $(\Psi \circ \Phi)(\mathrm{x}_k) = \mathrm{x}_l$ only if $k \in B_l$, and thus, by definition of p_π and p_θ, we have that

$$\mathrm{p}_\pi = \Psi \circ \Phi \left(\sum_{k=1}^{m} (-1)^k \mathrm{x}_{-k} \mathrm{x}_k \right) = \Psi \left(\mathrm{p}_\theta \right).$$

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 $\{\widehat{\pi} \in P(\pm 2m) : \widehat{\pi} \leq \pi \text{ and } \mathrm{p}_{\widehat{\pi}} = 0\}$ endowed with the partial order inherited from $P(\pm 2m)$. By Proposition 5.2.3, the partition θ has no singletons, and thus, either θ is a pairing partition or θ has a block with at least three elements. Let us assume $\theta = \{C_1, C_2, \ldots, C_n\}$ has a block with at least three elements, say C_n. By Proposition 5.2.3, 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 $i = 1, 2, \ldots n-1$, $\widehat{C}_n = C_n \setminus \{k, l\}$, and $\widehat{C}_{n+1} = \{k, l\}$, we have $\widehat{\theta} = \{\widehat{C}_1, \widehat{C}_2, \ldots, \widehat{C}_{n+1}\}$ is a partition of $[\pm 2m]$ such that $\widehat{\theta} \lneq \theta$, i.e., $\theta \geq \widehat{\theta}$ but $\theta \neq \widehat{\theta}$. Let us show that $\mathrm{p}_{\widehat{\theta}}$ must be the zero polynomial, contradicting the minimality of θ. Take $\mathcal{A} = \mathbb{Z}[\mathrm{x}_1, \mathrm{x}_{-1}, \ldots, \mathrm{x}_m, \mathrm{x}_{-m}]$,

$\mathcal{B} = \mathbb{Z}[\mathrm{x}_1, \mathrm{x}_2, \ldots, \mathrm{x}_n]$, and $\widehat{\mathcal{B}} = \mathbb{Z}[\mathrm{x}_1, \mathrm{x}_2, \ldots, \mathrm{x}_{n+1}]$ and let $\Phi : \mathcal{A} \to \mathcal{B}$ and $\widehat{\Phi} : \mathcal{A} \to \widehat{\mathcal{B}}$ be the unique homomorphisms such that $\Phi(\mathrm{x}_i) = \mathrm{x}_j$ if $i \in C_j$ and $\widehat{\Phi}(\mathrm{x}_i) = \mathrm{x}_j$ if $i \in \widehat{C}_j$. Since $\Phi(\mathrm{x}_i) = \widehat{\Phi}(\mathrm{x}_i)$ for $i \in [\pm 2m] \setminus \{k, l\}$, we have

$$\sum_{\substack{i=1 \\ i \neq k,l}}^{2m} (-1)^i \Phi(\mathrm{x}_{-i})\Phi(\mathrm{x}_i) = \sum_{\substack{i=1 \\ i \neq k,l}}^{2m} (-1)^i \widehat{\Phi}(\mathrm{x}_{-i})\widehat{\Phi}(\mathrm{x}_i).$$

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

$$\begin{aligned} 0 &= (-1)^k \Phi(\mathrm{x}_{-k})\Phi(\mathrm{x}_k) + (-1)^l \Phi(\mathrm{x}_{-l})\Phi(\mathrm{x}_l) \\ &= (-1)^k \widehat{\Phi}(\mathrm{x}_{-k})\widehat{\Phi}(\mathrm{x}_k) + (-1)^l \widehat{\Phi}(\mathrm{x}_{-l})\widehat{\Phi}(\mathrm{x}_l) \end{aligned}$$

since $k + l$ is odd, $\Phi(\mathrm{x}_k) = \Phi(\mathrm{x}_l) = \mathrm{x}_n$, and $\widehat{\Phi}(\mathrm{x}_k) = \widehat{\Phi}(\mathrm{x}_l) = \mathrm{x}_{n+1}$. Thus, we obtain

$$\mathrm{p}_{\widehat{\theta}} = \sum_{i=1}^{2m} (-1)^i \widehat{\Phi}(\mathrm{x}_{-i})\widehat{\Phi}(\mathrm{x}_i) = \sum_{i=1}^{2m} (-1)^i \Phi(\mathrm{x}_{-i})\Phi(\mathrm{x}_i) = \mathrm{p}_\theta = 0$$

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 5.2.3. □

As mentioned earlier, in proving Theorem 1.2.1, we need to consider sums as in (5.12). Note that if $\sigma : [\pm 2m] \to [\pm 2m]$ is bijective and $\mathrm{p}_{\sigma^{-1} \circ \pi}$ is the zero polynomial, then $\mathbf{h}(\mathbf{j}) = 1$ for any function $\mathbf{j} : [\pm 2m] \to [N]$ satisfying $\ker(\mathbf{j}) \geq \sigma^{-1} \circ \pi$, and hence, we would get

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

On the other hand, if the polynomial $\mathrm{p}_{\sigma^{-1}\circ\pi}$ is non-zero, we have that (5.12) is of order $N^{\#(\pi)-1/2}$ by Corollary 5.2.2. We will now use the previous results to classify all symmetric pairing partitions so that $\mathrm{p}_{\sigma^{-1}\circ\pi}$ is the zero polynomial.

Lemma 5.2.5. Let $m = m_1 + m_2$ for some integers $m_1, m_2 \geq 1$ and let σ be the permutation given by (5.13). Suppose k and l are integers in $[2m]$ and π is a symmetric pairing partition in $P(\pm 2m)$ such that $\mathrm{p}_{\sigma^{-1}\circ\pi}$ 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 5.2.4, the partition $\sigma^{-1}\circ\pi$ is symmetric since $\mathrm{p}_{\sigma^{-1}\circ\pi}$ 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 $t \geq 0$. □

Proposition 5.2.6. Let $m = m_1 + m_2$ for some integers $m_1, m_2 \geq 1$ and let σ be the

permutation given by (5.13). 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 $\mathrm{p}_{\sigma^{-1}\circ\pi}$ 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 $\pi = \{\{\sigma^t(-k), \sigma^{-t}(l)\} \mid 1 \leq t \leq 2m_1 + 2m_2\}$.

(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 $\pi = \{\{\sigma^t(-k), \sigma^t(-l)\} \mid 1 \leq t \leq 2m_1 + 2m_2\}$.

(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 $\pi_1 = \{\{\sigma^{t_1}(-k), \sigma^{-t_1}(k)\} \mid 1 \leq t_1 \leq 2m_1\}$ and $\pi_2 = \{\{\sigma^{t_2}(-l), \sigma^{-t_2}(l)\} \mid 1 \leq t_2 \leq 2m_2\}$.

(4) $\pi = \pi_1 \sqcup \pi_2$, m_1 and m_2 are odd, $\pi_1 = \{\{\sigma^{t_1}(-1), \sigma^{t_1}(-m_1-1)\} \mid 1 \leq t_1 \leq 2m_1\}$, and $\pi_2 = \{\{\sigma^{t_2}(-2m_1-1), \sigma^{t_2}(-2m_1-m_2-1)\} \mid 1 \leq t_2 \leq 2m_2\}$.

(5) $\pi = \pi_1 \sqcup \pi_2$, m_2 is odd, $\pi_2 = \{\{\sigma^{t_2}(-2m_1-1), \sigma^{t_2}(-2m_1-m_2-1)\} \mid 1 \leq t_2 \leq 2m_2\}$, and there is an integer $1 \leq k \leq 2m_1$ such that $\pi_1 = \{\{\sigma^{t_1}(-k), \sigma^{-t_1}(k)\} \mid 1 \leq t_1 \leq 2m_1\}$.

(6) $\pi = \pi_1 \sqcup \pi_2$, m_1 is odd, $\pi_1 = \{\{\sigma^{t_1}(-1), \sigma^{t_1}(-m_1-1)\} \mid 1 \leq t_1 \leq 2m_1\}$, and there is an integer $2m_1+1 \leq l \leq 2m_1+2m_2$ such that $\pi_2 = \{\{\sigma^{t_2}(-l), \sigma^{-t_2}(l)\} \mid 1 \leq t_2 \leq 2m_2\}$.

Proof. Put $\hat{\pi} = \sigma^{-1} \circ \pi$. Suppose $\hat{\pi} = \{B_1, B_2, \ldots, B_r\}$ and let Φ be the unique homomorphism from $\mathbb{Z}[\mathrm{x}_{-1}, \mathrm{x}_1, \ldots, \mathrm{x}_{-2m}, \mathrm{x}_{2m}]$ to $\mathbb{Z}[\mathrm{x}_1, \mathrm{x}_2, \ldots, \mathrm{x}_r]$ such that $\Phi(\mathrm{x}_i) = \mathrm{x}_j$ if $i \in B_j$. If condition (1) holds, then $\hat{\pi} = \{\{\sigma^t(-k), \sigma^{-t-2}(l)\} \mid t = 1, 2, \ldots, 4m_1\}$ and $\sigma^t(-k) + \sigma^{-t-2}(l)$ is odd for $t = 1, 2, \ldots, 4m_1$. Thus, since we can write

$$2 \cdot \sum_{i=1}^{2m} (-1)^i \mathrm{x}_{-i}\mathrm{x}_i = \sum_{t=1}^{2m_1} (-1)^{\sigma^{2t}(-k)} \mathrm{x}_{\sigma^{2t}(-k)} \mathrm{x}_{\sigma^{2t+1}(-k)} + \sum_{t=1}^{2m_1} (-1)^{\sigma^{-2t-2}(l)} \mathrm{x}_{\sigma^{-(2t+1)-2}(l)} \mathrm{x}_{\sigma^{-2t-2}(l)},$$

we get $\mathrm{p}_{\hat{\pi}} = \Phi(\sum_{i=1}^{2m}(-1)^i \mathrm{x}_{-i}\mathrm{x}_i) = 0$. It follows from similar arguments that $\mathrm{p}_{\hat{\pi}}$ is the zero polynomial if (2) holds. Now, if (4) holds and we take $l = 2m_1+1$, we have $\sigma^t(-k)+\sigma^{-t-2}(k)$ 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

$$\begin{aligned}\sum_{i=1}^{2m}(-1)^i \mathrm{x}_{-i}\mathrm{x}_i =& \frac{1}{2}\sum_{t=1}^{2m_1}(-1)^{\sigma^{2t}(-k)}\mathrm{x}_{\sigma^{2t}(-k)}\mathrm{x}_{\sigma^{2t+1}(-k)} + \frac{1}{2}\sum_{t=1}^{2m_1}(-1)^{\sigma^{-2t-2}(k)}\mathrm{x}_{\sigma^{-(2t+1)-2}(k)}\mathrm{x}_{\sigma^{-2t-2}(k)} \\ &+ \sum_{t=1}^{m_2}(-1)^{\sigma^{2t}(-l)}\mathrm{x}_{\sigma^{2t}(-l)}\mathrm{x}_{\sigma^{2t+1}(-l)} + \sum_{t=1}^{m_2}(-1)^{\sigma^{2t}(-m_2-l)}\mathrm{x}_{\sigma^{2t}(-m_2-l)}\mathrm{x}_{\sigma^{2t+1}(-m_2-l)}\end{aligned}$$

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

Suppose now $\mathrm{p}_{\hat{\pi}}$ 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 5.2.3, 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 5.2.5, 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 5.2.3, 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 5.2.5. 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

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

On the other hand, if (b) holds, it follows from Lemma 5.2.5 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,

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

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

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

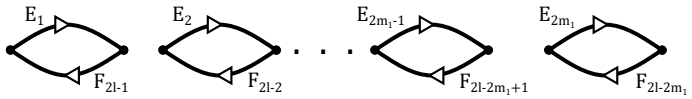
and if (B) holds, then there is an integer l such that

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

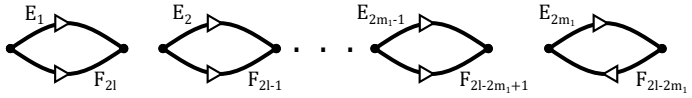
This completes the proof that if $\mathrm{p}_{\hat{\pi}}$ is the zero polynomial, then $\hat{\pi}$ must satisfy either (1), (2), (3), (4), (5), or (6). □

Remark 5.2.7. Notice the results regarding the polynomials p_π and $\mathrm{p}_{\sigma^{-1}\circ\pi}$ being zero can be restated in terms of the graphs $\mathcal{G}_\pi$ and $\vec{\mathcal{G}}_\pi$ from Section 5.1. For instance, Proposition 5.2.6 states that if $\pi \in P(\pm 2m)$ is a symmetric partition, then the polynomial $\mathrm{p}_{\sigma^{-1}\circ\pi}$ is zero 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 $t = 1, 2, \ldots, 2m_2$, holds:

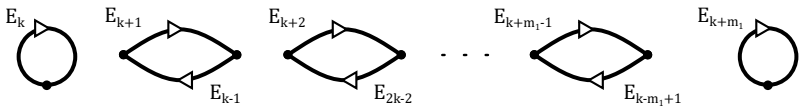
1. $m_1 = m_2$ and there is an integer $1 \leq l \leq m_2$ so that the graph $\vec{\mathcal{G}}_\pi$ can be represented as



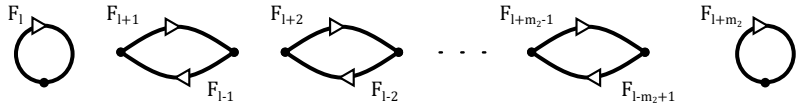
2. $m_1 = m_2$ and there is an integer $1 \leq l \leq m_2$ so that the graph $\vec{\mathcal{G}}_\pi$ can be represented as



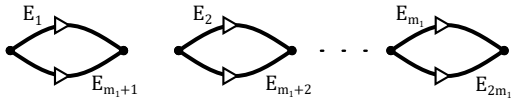
3. $\vec{\mathcal{G}}_\pi$ is the disjoint union of $\vec{\mathcal{G}}_{\pi_1}$ and $\vec{\mathcal{G}}_{\pi_2}$, there is an integer $1 \leq k \leq 2m_1$ so that $\vec{\mathcal{G}}_{\pi_1}$ can be represented as



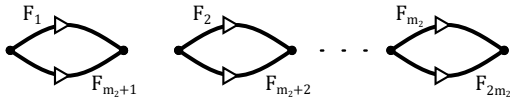
and there is an integer $2m_1 + 1 \leq l \leq 2m_1 + 2m_2$ so that $\vec{\mathcal{G}}_{\pi_2}$ can be represented as



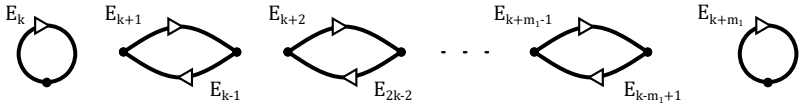
4. m_1 and m_2 are odd integers, the graph $\vec{\mathcal{G}}_{\pi}$ is the disjoint union of $\vec{\mathcal{G}}_{\pi_1}$ and $\vec{\mathcal{G}}_{\pi_2}$, the graph $\vec{\mathcal{G}}_{\pi_1}$ can be represented as



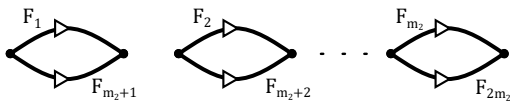
and the graph $\vec{\mathcal{G}}_{\pi_2}$ can be represented as



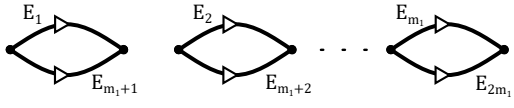
5. m_2 is odd, $\vec{\mathcal{G}}_{\pi}$ is the disjoint union of $\vec{\mathcal{G}}_{\pi_1}$ and $\vec{\mathcal{G}}_{\pi_2}$, there is an integer $1 \leq k \leq 2m_1$ so that $\vec{\mathcal{G}}_{\pi_1}$ can be represented as



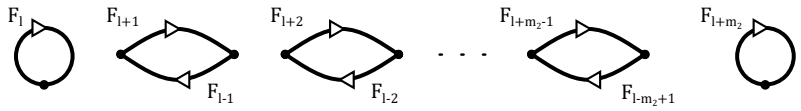
and the graph $\vec{\mathcal{G}}_{\pi_2}$ can be represented as



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 $t = 1, 2, \ldots, 2m_1$ and $l \pm t$ is taken modulo $2m_2$ for $t = 1, 2, \ldots, 2m_2$.

Moreover, since holds,

The inequality implies t

we have there always exists a

for all matrices $A_1, A_2, \ldots, A_m \in \mathrm{Mat}_N(\mathbb{C})$ and all integers $N \geq 1$,

For graph sums of square matrices, given a partition in $\pi \in P(\pm m)$, the result gives an answer to the problem of finding the least number $\tau \geq 0$ such that the inequality

$$\left| \sum_{\substack{\mathbf{j}:[\pm m]\to[N] \\ \ker(\mathbf{j})\geq\pi}} \prod_{k=1}^{m} A_k(j_{-k}, j_k) \right| \leq N^{\tau} \prod_{k=1}^{m} \|A_k\| \tag{5.20}$$

holds for all matrices $A_1, A_2, \ldots, A_m \in \mathrm{Mat}_N(\mathbb{C})$ and all integers $N \geq 1$. Note that, letting $\#(\pi)$ denote the number of blocks of π, we always have

$$\left| \sum_{\substack{\mathbf{j}:[\pm m]\to[N] \\ \ker(\mathbf{j})\geq\pi}} \prod_{k=1}^{m} A_k(j_{-k}, j_k) \right| \leq N^{\#(\pi)} \prod_{k=1}^{m} \|A_k\| \leq N^{2m} \prod_{k=1}^{m} \|A_k\|$$

since $\#(\pi) \leq 2m$ and $|A_k(j_{-k}, j_k)| \leq \|A_k\|$ for any matrix $A_k \in \mathrm{Mat}_N(\mathbb{C})$. Thus, given a partition in $\pi \in P(\pm m)$, there always exists a minimal $\tau \geq 0$ making (5.4) hold for all

matrices $A_1, A_2, \ldots, A_m \in \mathrm{Mat}_N(\mathbb{C})$ and all integers $N \geq 1$, we call such minimal τ the *graph sum exponent* of π and denote it by τ_π.

concerns more general graph sums, allowing the matrices A_k in (5.1) to be rectangular and not necessarily square.

It is also shown in [14] that

the existence of a minimal τ making (5.4) hold the main result in [14] provides us with an algorithm to compute it.

$$dd$$

that

given a partition in $\pi \in P(\pm m)$ there is an *optimal*

Given a partition in $\pi \in P(\pm m)$, we can consider the map $\mathcal{G}_\pi : \mathrm{Mat}_N(\mathbb{C}) \times \cdots \times \mathrm{Mat}_N(\mathbb{C}) \to \mathbb{C}$

$$\mathcal{G}_\pi(A_1, A_2, \ldots, A_m) = \sum_{\substack{\mathbf{j}:[\pm m]\to[N] \\ \ker(\mathbf{j})\geq\pi}} \prod_{k=1}^{m} A_k(j_{-k}, j_k)$$

there are some non-zero matrices $B_1, B_2, \ldots, B_m \in \mathrm{Mat}_N(\mathbb{C})$ satisfying

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

Chapter 6

Main Proofs

This chapter contains the proofs to our main results, namely, Theorem 1.2.1, Theorem 1.2.2, Lemma 1.2.3, and Theorem 1.2.4. The relation (6.3) from the proof of Lemma 1.2.3 is a starting point to the proof of Theorem 1.2.1, so we prove Lemma 1.2.3 first. Then, we show how the conclusion in Theorem 1.2.4 is be obtained from Lemma 1.2.3 and Proposition 4.3.18. Finally, Theorem 1.2.1 are Theorem 1.2.2 are proved with the assistance of the bounds on graph sums of the Discrete Fourier Transform from Section 5.2.

6.1 Proof of Lemma 1.2.3

Let I be an index set. Suppose $U_{N,i}$ is an N-by-N random unitary matrix for each index $i \in I$ and each integer $N \geq 1$ such that the following two conditions hold:

(I) the families of random matrices $\{U_{N,i_1}^* U_{N,i_2}\}_{i_1,i_2 \in I}$ and $\{\mathrm{W}^* U_{N,i_1}^* U_{N,i_2} \mathrm{W}\}_{i_1,i_2 \in I}$ are equal in distribution for every N-by-N signed permutation matrix W,

(II) for every positive integer m there is a constant C_m independent from N such that

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

for all integers $j_1, j_2 \in \{1, 2, \ldots, N\}$ and indexes $i_1, i_2 \in I$ with $i_1 \neq i_2$, and

Fix an integer $n \geq 1$. Assume $m = m_1 + m_2 + \cdots + m_n$ for some positive integers $m_1, m_2, \ldots, m_n$, take $m'_k = m'_{k-1} + m_{k-1}$ for $k = 2, 3, \ldots, n$ with $m'_1 = 0$, and consider the permutation γ with cycle decomposition

$$\gamma = (1, 2, \ldots, m'_1 + m_1)(m'_2 + 1, m'_2 + 2, \ldots, m'_2 + m_2) \cdots (m'_n + 1, \ldots, m'_n + m_n).$$

Now, given matrices $A_1, A_2, \ldots, A_m \in \mathrm{Mat}_N(\mathbb{C})$ of trace zero and indexes $i_1, i_2, \ldots, i_m \in I$ satisfying $i_k \neq i_{\gamma(k)}$ for $k = 1, 2, \ldots, m$, we let $Y_{N,k}$ be given by

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

for $k = 1, 2, \ldots, m$. Thus, putting $V_k = U^*_{N,i_k} U_{N,i_{\gamma(k)}}$ for $k = 1, 2, \ldots, m$, we have that

$$\mathrm{Tr}\left(Y_{N,k}\right) = \mathrm{Tr}\left(A_{m'_k+1} V_{m'_k+1} A_{m'_k+2} V_{m'_k+2} \cdots A_{m'_k+m_k} V_{m'_k+m_k}\right).$$

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

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

for each function $\mathbf{j} : [\pm m] \to [N]$, we obtain

$$\mathfrak{c}_n\left[\mathrm{Tr}\left(Y_1\right), \ldots, \mathrm{Tr}\left(Y_n\right)\right] = \sum_{\mathbf{j}:[\pm m]\to[N]} \mathbf{a}(\mathbf{j}) \mathfrak{c}_n\left[\mathbf{v}_1(\mathbf{j}), \mathbf{v}_2(\mathbf{j}), \ldots, \mathbf{v}_n(\mathbf{j})\right] \tag{6.1}$$

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, and thus, given a function $\mathbf{j} : [\pm m] \to [N]$ we have

$$\mathfrak{c}_n\left[\mathbf{v}_1(\mathbf{j}), \ldots, \mathbf{v}_n(\mathbf{j})\right] = \prod_{k=1}^{m} \epsilon_{\sigma(j_k)}\epsilon_{\sigma(j_{-k})}\mathfrak{c}_n\left[\mathbf{v}_1(\sigma \circ \mathbf{j}), \ldots, \mathbf{v}_n(\sigma \circ \mathbf{j})\right]$$

for all signs $\epsilon_1, \epsilon_2, \ldots, \epsilon_N \in \{\pm 1\}$ and permutations $\sigma \in \{f : [N] \to [N] \mid f \text{ is bijective}\}$. This implies that

$$\mathfrak{c}_n\left[\mathbf{v}_1(\mathbf{j}), \ldots, \mathbf{v}_n(\mathbf{j})\right] = 0$$

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

$$\mathfrak{c}_n\left[\mathbf{v}_1(\mathbf{j}), \ldots, \mathbf{v}_n(\mathbf{j})\right] = \mathfrak{c}_n\left[\mathbf{v}_1(\mathbf{j}'), \ldots, \mathbf{v}_n(\mathbf{j}')\right]$$

provided a function $\mathbf{j}' : [\pm m] \to [N]$ satisfies $\ker(\mathbf{j}') = \ker(\mathbf{j})$. Hence, letting $\mathfrak{c}_n[\pi]$ denote the common value $\mathfrak{c}_n\left[\mathbf{v}_1(\mathbf{j}), \ldots, \mathbf{v}_n(\mathbf{j})\right]$ among all those functions $\mathbf{j} : [\pm m] \to [N]$ satisfying $\ker(\mathbf{j}) = \pi$, Equation (6.1) becomes

$$\mathfrak{c}_n\left[\mathrm{Tr}(Y_1), \ldots, \mathrm{Tr}(Y_n)\right] = \sum_{\pi \in P_{\mathrm{even}}(\pm m)} \mathfrak{c}_n[\pi] \sum_{\substack{\mathbf{j}:[\pm m]\to[N] \\ \ker(\mathbf{j})=\pi}} \mathbf{a}(\mathbf{j}). \tag{6.2}$$

Moreover, the Möbius inversion formula, Equation (2.3), implies

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

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

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

So, we get

$$\mathfrak{c}_n\left[\mathrm{Tr}\left(Y_1\right),\ldots,\mathrm{Tr}\left(Y_n\right)\right] = \sum_{\pi\in P_{\mathrm{even}}(\pm m)} \sum_{\substack{\theta\in P_{\mathrm{even}}(\pm m)\\ \theta\geq\pi}} \mathfrak{c}_n\left[\pi\right]\mu(\pi,\theta) \sum_{\substack{\mathbf{j}:[\pm m]\to[N]\\ \ker(\mathbf{j})\geq\theta}} \mathbf{a}(\mathbf{j}) \tag{6.3}$$

Note that if a partition $\theta \in P(\pm m)$ has a block of the form $\{k,-k\}$, then a function $\mathbf{j}:[\pm m]\to[N]$ satisfies $\ker(\mathbf{j})\geq\theta$ only if $j_{-k}=j_k$, and hence, we can write

$$\sum_{\substack{\mathbf{j}:[\pm m]\to[N]\\ \ker(\mathbf{j})\geq\theta}} \mathbf{a}(\mathbf{j}) = \mathrm{Tr}\left(A_k\right)\cdot \sum_{\substack{\mathbf{j}':S\to[N]\\ \ker(\mathbf{j}')\geq\theta'}} \prod_{\substack{k'=1\\ k'\neq k}}^{m} A_{k'}(j_{-k'},j_{k'})$$

where $S=[\pm m]\setminus\{-k,k\}$ and $\theta'=\theta\setminus\{\{-k,k\}\}$. Therefore, since each A_k is assumed to be of trace zero, we have

$$\mathfrak{c}_n\left[\mathrm{Tr}\left(Y_1\right),\ldots,\mathrm{Tr}\left(Y_n\right)\right] = \sum_{\pi\in P_{\mathrm{even}}(\pm m)} \sum_{\substack{\theta\in P_{\chi}(\pm m)\\ \theta\geq\pi}} \mathfrak{c}_n\left[\pi\right]\mu(\pi,\theta) \sum_{\substack{\mathbf{j}:[\pm m]\to[N]\\ \ker(\mathbf{j})\geq\theta}} \mathbf{a}(\mathbf{j}) \tag{6.4}$$

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

For a partition $\theta\in P_\chi(\pm m)$, each connected component of the graph $\mathcal{G}_\theta$, constructed as in Section 5.1, has at least two edges, and hence, $\mathcal{G}_\theta$ has at most $\frac{m}{2}$ connected components.

Thus, from Theorem 5.1.1, Proposition 5.1.2, and the equality in (6.4), we get

$$|\mathfrak{c}_n\left[\mathrm{Tr}\left(Y_1\right),\ldots,\mathrm{Tr}\left(Y_n\right)\right]| \leq \sum_{\pi\in P_{\mathrm{even}}(\pm m)} \sum_{\substack{\theta\in P_\chi(\pm m)\\ \theta\geq\pi}} |\mathfrak{c}_n\left[\pi\right]||\mu(\pi,\theta)|N^{\frac{m}{2}} \prod_{k=1}^{m}\|A_k\|.$$

Since the sums above are over the finite sets $P_{\mathrm{even}}(\pm m)$ and $P_\chi(\pm m)$, to conclude that

$$|\mathfrak{c}_n\left[\mathrm{Tr}\left(Y_{N,1}\right),\mathrm{Tr}\left(Y_{N,2}\right),\ldots,\mathrm{Tr}\left(Y_{N,n}\right)\right]| \leq C(i_1,i_2,\ldots,i_m)\|A_1\|\|A_2\|\cdots\|A_m\|$$

for some constant $C(i_1,\ldots,i_m)$ independent from N, it only remains to show that there is a constant C_n independent from N such that

$$|\mathfrak{c}_n\left[\mathbf{v}_1(\mathbf{j}),\ldots,\mathbf{v}_n(\mathbf{j})\right]| \leq C_n N^{-\frac{m}{2}}$$

for all functions $\mathbf{j}:[\pm m]\to[N]$.

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

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

But, by hypothesis, the p-norms of the entries of $\sqrt{N}V_l$ are uniformly bounded, i.e., there are constants $C_1,C_2,\ldots,C_m$ such that

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

for all integers $1 \leq j_l, j_{-\gamma(l)} \leq N$ and $p, l = 1, 2, \ldots, m$, 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

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

so it follows that

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

And the proof of Lemma 1.2.3 is now complete.

6.2 Proof of Theorem 1.2.4

Let I be an index set. Suppose $D_{N,i}$ is a self-adjoint N-by-N deterministic matrix and $U_{N,i}$ is a random unitary matrix for each index $i \in I$ and each integer $N \geq 1$. Assume the following three conditions hold:

(I) the families of random matrices $\{U^*_{N,i_1} U_{N,i_2}\}_{i_1, i_2 \in I}$ and $\{\mathrm{W}^* U^*_{N,i_1} U_{N,i_2} \mathrm{W}\}_{i_1, i_2 \in I}$ are equal in distribution for every N-by-N signed permutation matrix W,

(II) for every positive integer m there is a constant C_m independent from N such that

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

for all integers $j_1, j_2 \in \{1, 2, \ldots, N\}$ and indexes $i_1, i_2 \in I$ with $i_1 \neq i_2$, and

(III) for every index $i \in I$ and every integer $k \geq 1$ we have $\sup_{N \in \mathbb{N}} \|D_{N,i}\| < \infty$ and $\lim_{N \to \infty} \operatorname{tr}\left(D_{N,i}^k\right)$ exists.

Put $\mathcal{A} = \mathbb{C}\langle \mathrm{x}_i \mid i \in I \rangle$ and $\mathcal{A}_i = \mathbb{C}[x_i] \subset \mathcal{A}$ for each index $i \in I$. Additionally, 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 $\mu_N : \mathbb{C}\langle \mathrm{x}_i \mid i \in I \rangle \to \mathbb{C}$ the joint distribution of $\{X_{N,i}\}_{i \in I}$ given by

$$\mu_N(\mathrm{p}) := \mathbb{E}\left[\operatorname{tr}\left(\mathrm{p}\left(\{X_{N,i}\}_{i \in I}\right)\right)\right] \tag{6.5}$$

for every polynomial $\mathrm{p} \in \mathbb{C}\langle \mathrm{x}_i \mid i \in I \rangle$. Since $\mathrm{p} \in \mathcal{A}_j$ for some $j \in I$ implies $\mathrm{p}\left(\{X_{N,i}\}_{i \in I}\right) = U_{N,j} \mathrm{p}(D_{N,j}) U_{N,j}^*$, we have that $\lim_{N \to \infty} \mu_N[\mathrm{p}]$ exists for every $\mathrm{p} \in \mathcal{A}_i$ and every $i \in I$. Now, suppose we are given polynomials $\mathrm{p}_1 \in \mathcal{A}_{i_1}, \mathrm{p}_2 \in \mathcal{A}_{i_2}, \ldots, \mathrm{p}_m \in \mathcal{A}_{i_m}$ with $i_1, i_2, \ldots, i_m \in I$ and $i_1 \neq i_2, i_2 \neq i_3, \ldots, i_{m-1} \neq i_m$, and $i_m \neq i_1$. Note that

$$N\mu_N\left[(\mathrm{p}_1 - \mu_N[\mathrm{p}_1])(\mathrm{p}_2 - \mu_N[\mathrm{p}_2]) \cdots (\mathrm{p}_m - \mu_N[\mathrm{p}_m])\right] = \mathbb{E}\left[\operatorname{Tr}(Y_N)\right]$$

where

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

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

$$A_{N,i_j} = U_{N,i_j}^* \left(\mathrm{p}_j(X_{N,i_j}) - \mathbb{E}[\mathrm{tr}(\mathrm{p}_j(X_{N,i_j}))] I_N \right) U_{N,i_j} = \mathrm{p}_j(D_{N,i_j}) - \mathrm{tr}(\mathrm{p}_j(D_{N,i_j})) I_N.$$

Thus, by Lemma 1.2.3, there is a constant C depending only on the indexes i_j such that

$$|N\mu_N\left[(\mathrm{p}_1 - \mu_N\left[\mathrm{p}_1\right])(\mathrm{p}_2 - \mu_N\left[\mathrm{p}_2\right]) \cdots (\mathrm{p}_m - \mu_N\left[\mathrm{p}_m\right])\right]| \leq C \prod_{j=1}^{m} \left\| A_{N,i_j} \right\|.$$

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

$$\lim_{N\to\infty} \mu_N\left[(\mathrm{p}_1 - \mu_N\left[\mathrm{p}_1\right])(\mathrm{p}_2 - \mu_N\left[\mathrm{p}_2\right]) \cdots (\mathrm{p}_m - \mu_N\left[\mathrm{p}_m\right])\right] = 0 \tag{6.6}$$

Each linear functional μ_N is tracial, i.e., $\mu_N[pq] = \mu_N[qp]$ for all $p, q \in \mathcal{A}$, and thus, following similar arguments to those in the proof Corollary 4.3.20, we can remove the condition $i_m \neq i_1$ and still get (6.6). Therefore, by Corollary 3.2.5, the random matrix ensembles $\{U_{N,i} D_{N,i} U_{N,i}^*\}_{N=1}^{\infty}$ with $i \in I$ are asymptotically free and $\lim_{N\to\infty} \mu_N[\mathrm{p}]$ exists for every $\mathrm{p} \in \mathcal{A}$.

Fix now an arbitrary integer $n \geq 2$. For every integer $N \geq 1$, let $\rho_N : \mathcal{A} \times \cdots \times \mathcal{A} \to \mathbb{C}$ be the n-linear map given by

$$\rho_N\left[\mathrm{p}_1, \mathrm{p}_2, \ldots, \mathrm{p}_n\right] = \mathfrak{c}_n\left[\mathrm{Tr}\left(\mathrm{p}_1(\{X_{N,i}\}_{i\in I})\right), \ldots, \mathrm{Tr}\left(\mathrm{p}_N(\{X_{N,i}\}_{i\in I})\right)\right] \tag{6.7}$$

for polynomials $\mathrm{p}_1, \mathrm{p}_2, \ldots, \mathrm{p}_n \in \mathcal{A}$ and where $\mathfrak{c}_n[\cdot, \ldots, \cdot]$ denotes the classical cumulant. Note that for any indexes $i_1, i_2, \ldots, i_n \in I$ and polynomials $\mathrm{p}_1 \in \mathcal{A}_{i_1}, \mathrm{p}_2 \in \mathcal{A}_{i_2}, \ldots, \mathrm{p}_n \in \mathcal{A}_{i_n}$, we

have

$$\rho_N(\mathrm{p}_1, \mathrm{p}_2, \ldots, \mathrm{p}_n) = \mathfrak{c}_n\left[\mathrm{Tr}\left(\mathrm{p}_1(D_{N,i_1})\right), \ldots, \mathrm{Tr}\left(\mathrm{p}_n(D_{N,i_n})\right)\right] = 0$$

since $\mathrm{Tr}\left(\mathrm{p}_k(D_{N,i_k})\right)$ is a constant. 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 (c') from Corollary 4.3.20, namely,

$$\sup_N |\rho_N\left[\mathrm{q}_{N,1}, \mathrm{q}_{N,2}, \ldots, \mathrm{q}_{N,n}\right]| < \infty$$

whenever each $\mathrm{q}_{N,k}$ is of the form

$$\mathrm{q}_{N,k} = (\mathrm{p}_1^{(k)} - \mu_N[\mathrm{p}_1^{(k)}])(\mathrm{p}_2^{(k)} - \mu_N[\mathrm{p}_2^{(k)}]) \cdots (\mathrm{p}_{m_k}^{(k)} - \mu_N[\mathrm{p}_{m_k}^{(k)}])$$

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

$$\rho_N\left[\mathrm{q}_{N,1}, \mathrm{q}_{N,2}, \ldots, \mathrm{q}_{N,n}\right] = \mathfrak{c}_n\left[\mathrm{Tr}\left(Y_{N,1}\right), \mathrm{Tr}\left(Y_{N,2}\right), \ldots, \mathrm{Tr}\left(Y_{N,n}\right)\right].$$

Moreover, letting $A_{N,i_j^{(k)}} = \mathrm{p}_j^{(k)}(D_{N,i_j^{(k)}}) - \mathrm{tr}(\mathrm{p}_j^{(k)}(D_{N,i_j^{(k)}}))I_N$ 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

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

Therefore, by Lemma 1.2.3, there is a constant C depending only on the indexes $i_j^{(k)}$ such

that

$$|\rho_N\left[\mathrm{q}_{N,1},\mathrm{q}_{N,2},\ldots,\mathrm{q}_{N,n}\right]| \leq C\prod_{k=1}^{n}\prod_{j=1}^{m_k}\left\|A_{N,i_j^{(k)}}\right\| < \infty.$$

6.3 Proof of Theorem 1.2.1

Let $D_{N,1}$ and $D_{N,2}$ be N-by-N self-adjoint matrices for each integer $N \geq 1$ so that the following holds:

(i) $\lim_{N\to\infty} \mathrm{tr}\left(D_{N,i}^k\right)$ exists for every index $i \in \{1,2\}$ and every integer $k \geq 1$ and

(ii) $\sup_{N\in\mathbb{N}} \|D_{N,i}\| < \infty$ for every index $i \in \{1,2\}$.

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 $\{W, HW/\sqrt{N}, XHW/\sqrt{N}\}$ with W an N-by-N uniformly-distributed signed permutation matrix, X an N-by-N uniformly-distributed signature matrix independent from W, and H the N-by-N Discrete Fourier Transform matrix.

Let $m = m_1 + m_2$ for some integers $m_1, m_2 \geq 1$. Assume we are given indexes polynomials $\mathrm{p}_1, \mathrm{p}_2, \ldots, \mathrm{p}_{2m_1}, \mathrm{q}_1, \mathrm{q}_2, \ldots, \mathrm{q}_{2m_2} \in \mathbb{C}[\mathrm{x}]$ and some indexes $i_1, i_2, \ldots, i_{2m_1}, j_1, j_2, \ldots, j_{2m_2} \in \{1,2\}$ satisfying $i_1 = j_1$, $i_1 \neq i_2, i_2 \neq i_3, \ldots, i_{2m_1-1} \neq i_{2m_1}, i_{2m_1} \neq i_1$, and $j_1 \neq j_2, j_2 \neq j_3, \ldots, j_{2m_2-1} \neq j_{2m_2}, j_{2m_2} \neq j_1$. Note that $i_1 = i_{2k-1} = j_{2l-1} \neq i_2 = i_{2k} = j_{2l}$. Consider the random matrices

$$Y_{N,k} = \mathrm{p}_k\left(X_{N,i_k}\right) - \mathbb{E}\left[\mathrm{tr}\left(\mathrm{p}_k\left(X_{N,i_k}\right)\right)\right] I_N \quad \text{and} \quad Z_{N,l} = \mathrm{q}_l(X_{N,j_l}) - \mathbb{E}[\mathrm{tr}(\mathrm{q}_l(X_{N,j_l}))]I_N$$

for $1 \leq k \leq 2m_1$ and $1 \leq l \leq 2m_2$. Now, letting $Y_N = Y_{N,1}Y_{N,2}\cdots Y_{N,2m_1}$ and $Z_N = Z_{N,1}Z_{N,2}\cdots Z_{N,2m_2}$, we have

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

and

$$Z_N = \left(U_{N,j_1} B_{N,1} U_{N,j_1}^*\right)\left(U_{N,j_2} B_{N,2} U_{N,j_2}^*\right)\cdots\left(U_{N,j_{2m_1}} B_{N,2m_1} U_{N,j_{2m_1}}^*\right)$$

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

$$A_{N,k} = \mathrm{p}_k\left(D_{N,i_k}\right) - \mathrm{tr}\left(\mathrm{p}_k\left(D_{N,i_k}\right)\right) I_N \quad \text{and} \quad B_{N,l} = \mathrm{q}_l(D_{N,j_l}) - \mathrm{tr}(\mathrm{q}_l(D_{N,j_l}))I_N$$

for $1 \leq k \leq 2m_1$ and $1 \leq l \leq 2m_2$. Thus, following similar arguments to those in the proof of Lemma 1.2.3, we obtain

$$\mathrm{Cov}\left[\mathrm{Tr}(Y_N), \mathrm{Tr}(Z_N)\right] = \sum_{\theta \in P_\chi(\pm 2m)} \left(\sum_{\substack{\pi \in P_{\mathrm{even}}(\pm 2m) \\ \pi \leq \theta}} \mathfrak{c}_2\left[\pi\right] \mu(\pi, \theta) \right) \sum_{\substack{\mathbf{j}:[\pm 2m] \to [N] \\ \ker(\mathbf{j}) \geq \theta}} \mathbf{a}(\mathbf{j}) \tag{6.8}$$

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

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

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

$$\mathfrak{c}_2\left[\pi\right] = \mathrm{cov}\left[\prod_{k=1}^{2m_1} V_k(j_{\sigma(-k)}, j_{\sigma(k)}), \prod_{k=2m_1+1}^{2m_1+2m_2} V_k(j_{\sigma(-k)}, j_{\sigma(k)})\right] \tag{6.9}$$

with $V_{2k-1} = V_{2k}^* = U_{N,i_1}^* U_{N,i_2}$ for $k = 1, 2, \ldots, m$ and $\sigma : [\pm 2m] \to [\pm 2m]$ is the cyclic permutation given by

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

Notice that (6.8) becomes

$$\mathrm{Cov}\left[\mathrm{Tr}(Y_N), \mathrm{Tr}(Z_N)\right] = \sum_{\theta \in P_{\chi\chi}(\pm 2m)} \left(\sum_{\substack{\pi \in P_{\mathrm{even}}(\pm 2m) \\ \pi \leq \theta}} \mathfrak{c}_2\left[\pi\right] \mu(\pi, \theta) \right) \sum_{\substack{\mathbf{j}:[\pm 2m] \to [N] \\ \ker(\mathbf{j}) \geq \theta}} \mathbf{a}(\mathbf{j}) + O(N^{-1}) \tag{6.10}$$

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 Section 5.1, equals m. Indeed, if we are given partitions $\pi \in P_{\mathrm{even}}(\pm 2m)$ and $\theta \in P_{\chi}(\pm 2m)$ satisfying $\theta \geq \pi$, then Theorem 5.1.1 and Proposition 5.1.2 imply

$$\left| \mathfrak{c}_2\left[\pi\right] \mu(\pi, \theta) \sum_{\substack{\mathbf{j}:[\pm 2m] \to [N] \\ \ker(\mathbf{j}) \geq \theta}} \mathbf{a}(\mathbf{j}) \right| \leq |\mathfrak{c}_2\left[\pi\right]| |\mu(\pi, \theta)| N^{\tau_\theta} \prod_{k=1}^{2m_1} \|A_{N,k}\| \prod_{l=1}^{2m_2} \|B_{N,l}\| \tag{6.11}$$

where τ_θ is the number of connected components of the graph $\mathcal{G}_\theta$. Now, by hypothesis, $\sup_N \|D_{N,i}\| < \infty$ and $\lim_{N\to\infty} \mathrm{tr}(D_{N,i}^k)$ 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 $\mathcal{G}_\theta$ 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 1.2.3, it follows from the proof of Lemma 1.2.3 that there is a constant C_2 independent from N

satisfying

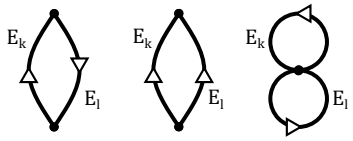
$$|\mathfrak{c}_2[\pi]| \leq C_2 N^{-m}.$$

Therefore, from (6.11) we obtain

$$\mathfrak{c}_2[\pi]\,\mu(\pi,\theta) \sum_{\substack{\mathbf{j}:[\pm 2m]\to[N] \\ \ker(\mathbf{j})\geq\theta}} \mathbf{a}(\mathbf{j}) = O(N^{-1}) \tag{6.12}$$

unless the graph sum exponent $\tau_\theta = m$, and, consequently, we get (6.10).

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 $\mathcal{G}_\theta$ 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 three forms:



And therefore, as illustrated it at the end of Section 5.1, each graph sum $\sum_{\ker(\mathbf{j})\geq\theta} \mathbf{a}(\mathbf{j})$ appearing in (6.10) can be written as a product of traces of matrices where each trace is of the followings forms: $\mathrm{Tr}(C_{N,k}C_{N,l})$, $\mathrm{Tr}(C_{N,k}C_{N,l}^T)$, or $\mathrm{Tr}(C_{N,k}\circ C_{N,l})$ where $C_{N,k}$ and $C_{N,l}$ belong to the set $\{A_{N,1},\ldots,A_{N,2m_1},B_{N,1},\ldots,B_{N,2m_2}\}$. Hence, letting $\mathfrak{c}[\pi]$ be given by (6.9) for each partition $\pi \in P(\pm 2m)$, the conclusions in Theorem 1.2.1 will follow from (6.10) once we determine the order of

$$\sum_{\substack{\pi\in P_{\mathrm{even}}(\pm 2m) \\ \theta\geq\pi}} \mathfrak{c}_2[\pi]\,\mu(\pi,\theta). \tag{6.13}$$

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 (6.13), it is enough to compute $\mathfrak{c}_2[\pi]$ for even partitions $\pi \in P(\pm 2m)$ satisfying $\pi \leq \theta$ for some another partition θ in the set $P_{\chi\chi}(\pm 2m)$.

Proposition 6.3.1. Suppose θ is a partition in $P_{\chi\chi}(\pm 2m)$. If π is an even partition such that $\pi \leq \theta$ and $\mathfrak{c}_2[\pi]$ is given by (6.9), then the following holds:

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

   (a) $N^m \mathfrak{c}_2[\pi] = 1 + O\left(N^{-1}\right)$ if there symmetric pairing partition $\hat{\theta} \leq \pi$ satisfying either (1) or (2) from Proposition 5.2.6

   (b) $N^m \mathfrak{c}_2[\pi] = O\left(N^{-1/2}\right)$ in any other case

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

   (a) $N^m \mathfrak{c}_2[\pi] = 1 + O\left(N^{-1}\right)$ if there symmetric pairing partition $\hat{\theta} \leq \pi$ satisfying (1) from Proposition 5.2.6

   (b) $N^m \mathfrak{c}_2[\pi] = 1 + O\left(N^{-1}\right)$ if there symmetric pairing partition $\hat{\theta} \leq \pi$ satisfying (2) from Proposition 5.2.6 and the graph $\mathcal{G}_\pi$ has only double-loops as connected components

   (c) $N^m \mathfrak{c}_2[\pi] = O\left(N^{-1/2}\right)$ in any other case

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

   (a) $N^m \mathfrak{c}_2[\pi] = 1 + O\left(N^{-1}\right)$ if $m_1 = m_2$ and there are integers $1 \leq k \leq 2m_1 < l \leq 2m_1 + 2m_2$ so that $\sigma^t(-k) \sim_\pi \sigma^{-t}(l)$ for every integer $t \geq 0$

   (b) $N^m \mathfrak{c}_2[\pi] = 2 + O\left(N^{-1}\right)$ if there are integers $1 \leq k \leq 2m_1 < l \leq 2m_1 + 2m_2$ so that $\sigma^{-t}(k) \sim_\pi \sigma^{t+1}(k)$ and $\sigma^{-t}(l) \sim_\pi \sigma^{t+1}(l)$ for every integer $t \geq 0$

   (c) $N^m \mathfrak{c}_2[\pi] = O\left(N^{-1/2}\right)$ in any other case

The proof of Proposition 6.3.1 is based on the expected value of products of entries from X and W, see relations (4.2) and (4.3), and the results on graph sums of the Discrete Fourier Transform from Section 5.2, 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 (6.13) up to a term of order $N^{-m-1/2}$ is quite simple assuming Proposition 6.3.1 holds.

Lemma 6.3.2. Suppose θ is a partition in $P_{\chi\chi}(\pm 2m)$ and let $\mathfrak{c}[\pi]$ be given by (6.9) for each partition $\pi \in P(\pm 2m)$. Then the following holds:

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

(a) $\sum_{\substack{\pi\in P_{\text{even}}(\pm 2m)\\ \pi\leq\theta}} N^m \mathfrak{c}_2[\pi]\,\mu(\pi,\theta) = 1 + O\left(N^{-1}\right)$ if θ is a symmetric pairing partition satisfying either (1) or (2) from Proposition 5.2.6

(b) $\sum_{\substack{\pi\in P_{\text{even}}(\pm 2m)\\ \pi\leq\theta}} N^m \mathfrak{c}_2[\pi]\,\mu(\pi,\theta) = O\left(N^{-1/2}\right)$ in any other case

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

(a) $\sum_{\substack{\pi\in P_{\text{even}}(\pm 2m)\\ \pi\leq\theta}} N^m \mathfrak{c}_2[\pi]\,\mu(\pi,\theta) = 1 + O\left(N^{-1}\right)$ if θ is a symmetric pairing partition satisfying (1) from Proposition 5.2.6

(b) $\sum_{\substack{\pi\in P_{\text{even}}(\pm 2m)\\ \pi\leq\theta}} N^m \mathfrak{c}_2[\pi]\,\mu(\pi,\theta) = 1 + O\left(N^{-1}\right)$ if there symmetric pairing partition $\hat{\theta} \leq \theta$ satisfying (2) from Proposition 5.2.6 and θ has only blocks of size 4 of the form $\{k,-k,l,-l\}$

(c) $\sum_{\substack{\pi\in P_{\text{even}}(\pm 2m)\\ \pi\leq\theta}} N^m \mathfrak{c}_2[\pi]\,\mu(\pi,\theta) = O\left(N^{-1/2}\right)$ in any other case

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

(a) $\sum_{\substack{\pi\in P_{\text{even}}(\pm 2m)\\ \pi\leq\theta}} N^m \mathfrak{c}_2[\pi]\,\mu(\pi,\theta) = 1 + O\left(N^{-1}\right)$ if $m_1 = m_2$ and there is an integer $2m_1+1 \leq l \leq 2m_1+2m_2$ so that $\theta = \{\{\sigma^t(-1), \sigma^{-t-1}(-l)\} \mid t \geq 0\}$

(b) $\sum_{\substack{\pi\in P_{\text{even}}(\pm 2m)\\ \pi\leq\theta}} N^m \mathfrak{c}_2[\pi]\,\mu(\pi,\theta) = 2 + O\left(N^{-1}\right)$ if there are integers $1 \leq l_1 \leq 2m_1 < l_2 \leq 2m_1+2m_2$ so that $\theta = \theta_1 \sqcup \theta_2$ where $\theta_1 = \{\{\sigma^t(-l_1), \sigma^{-t-1}(-l_1)\} \mid t \geq 0\}$ and $\theta_2 = \{\{\sigma^t(-l_2), \sigma^{-t-1}(-l_2)\} \mid t \geq 0\}$

(c) $\sum_{\substack{\pi\in P_{\text{even}}(\pm 2m)\\ \pi\leq\theta}} N^m \mathfrak{c}_2[\pi]\,\mu(\pi,\theta) = O\left(N^{-1/2}\right)$ in any other case

Proof. Suppose $U_{N,i_1}^* U_{N,i_2} = W^* X H W/\sqrt{N}$. Proposition 5.2.6 and Proposition 6.3.1 imply that

$$\sum_{\substack{\pi\in P_{\text{even}}(\pm 2m)\\ \pi\leq\theta}} N^m \mathfrak{c}_2[\pi]\,\mu(\pi,\theta) = O\left(N^{-1/2}\right)$$

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 $\mathcal{G}_\theta$ has only double-loops as components

Assuming (i) above holds, consider the pairing partition $\hat{\theta} = \{\{\sigma^t(-k), \sigma^{-t}(l)\} \mid t \geq 0\}$ and note that Proposition 6.3.1 implies that

$$\sum_{\substack{\pi\in P_{\text{even}}(\pm 2m)\\ \pi\leq\theta}} N^m \mathfrak{c}_2[\pi]\,\mu(\pi,\theta) = \sum_{\substack{\pi\in P_{\text{even}}(\pm 2m)\\ \hat{\theta}\leq\pi\leq\theta}} N^m \mathfrak{c}_2[\pi]\,\mu(\pi,\theta) + O\left(N^{-1/2}\right). \tag{6.14}$$

Moreover, since $N^m \mathfrak{c}_2[\pi] = 1 + O(N^{-1})$ for any partition π satisfying $\hat{\theta} \leq \pi \leq \theta$, we get

$$\sum_{\substack{\pi \in P_{\text{even}}(\pm 2m) \\ \pi \leq \theta}} N^m \mathfrak{c}_2[\pi]\, \mu(\pi, \theta) = \sum_{\substack{\pi \in P_{\text{even}}(\pm 2m) \\ \hat{\theta} \leq \pi \leq \theta}} \mu(\pi, \theta) + O(N^{-1/2}) = \begin{cases} 1 + O\left(N^{-1/2}\right) & \text{if } \hat{\theta} = \theta \\ O\left(N^{-1/2}\right) & \text{if } \hat{\theta} < \theta \end{cases}$$

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 (6.14) above holds also in this case. Hence, since $N^m \mathfrak{c}_2[\theta] = 1 + O(N^{-1})$ and $N^m \mathfrak{c}_2[\pi] = O(N^{-1/2})$ for any partition $\hat{\theta} \leq \pi < \theta$, we obtain

$$\sum_{\substack{\pi \in P_{\text{even}}(\pm 2m) \\ \pi \leq \theta}} N^m \mathfrak{c}_2[\pi]\, \mu(\pi, \theta) = N^m \mathfrak{c}_2[\theta]\, \mu(\theta, \theta) + \sum_{\substack{\pi \in P_{\text{even}}(\pm 2m) \\ \hat{\theta} \leq \pi < \theta}} N^m \mathfrak{c}_2[\pi]\, \mu(\pi, \theta) = 1 + O(N^{-1/2})$$

The other cases, namely, $U^*_{N,i_1} U_{N,i_2} = W^* HW/\sqrt{N}$ and $U^*_{N,i_1} U_{N,i_2} = W^* H^* XHW/N$, are proved in the same way, one chooses a suitable pairing partition $\hat{\theta}$ such that (6.14) holds, and then the corresponding conclusion follows from Proposition 6.3.1 and the equations in (2.1) defining the Möbius function. □

As mentioned earlier, the proof of Theorem 1.2.1 is complete once we apply Lemma 6.3.2 to the relation (6.10). For instance, suppose $U^*_{N,i_1} U_{N,i_2} = W^* H^* XHW/N$. Then, Theorem 5.1.1, Lemma 6.3.2, and (6.10) imply that

$$\text{Cov}\left[\text{Tr}(Y_N), \text{Tr}(Z_N)\right] = \delta_{m_1,m_2} \sum_{\theta \in \mathcal{P}_1} \sum_{\substack{\mathbf{j}:[\pm 2m] \to [N] \\ \ker(\mathbf{j}) \geq \theta}} \mathbf{a}(\mathbf{j}) + \sum_{\theta \in \mathcal{P}_2} 2 \sum_{\substack{\mathbf{j}:[\pm 2m] \to [N] \\ \ker(\mathbf{j}) \geq \theta}} \mathbf{a}(\mathbf{j}) + O\left(N^{-\frac{1}{2}}\right) \quad (6.15)$$

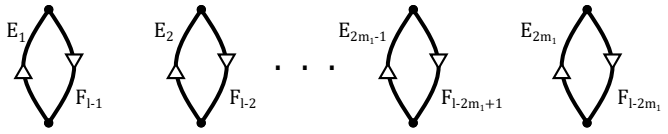
where $\mathcal{P}_1$ and $\mathcal{P}_2$ are subsets of $P_{\chi\chi}(\pm 2m)$ given by

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

and

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

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 $k = 1, 2, \ldots, 2m_1$. Thus, for each integer $1 \leq l \leq 2m_1$, there exists a unique $\theta \in \mathcal{P}_1$ so that

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

and hence, we obtain

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

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 $l_1 = 1, 2, \ldots, m_1$ and $l_2 = 1, 2, \ldots, m_2$. 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 $k_1 = 1, 2, \ldots, m_1$ and $k_2 = 1, 2, \ldots, m_2$. 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

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

Therefore, we have

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

The other cases, namely, $U^*_{N,i_1}U_{N,i_2} = W^*HW/\sqrt{N}$ and $U^*_{N,i_1}U_{N,i_2} = W^*XHW/N$, are proved in the same way, applying Lemma 6.3.2 to the relation (6.10) we obtain similar relations to that in (6.15) that lead to (1) and (2) in Theorem 1.2.1.

The remaining of this section is devoted to the proof of Proposition 6.3.1. For clarity, we have considered two cases: $U^*_{N,i_1}U_{N,i_2} = W^*H^*XHW/N$ and $U^*_{N,i_1}U_{N,i_2} = W^*YHW/\sqrt{N}$ 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

$$\pi^{\text{even}} = \{\{-2, 8\}, \{2, -6\}, \{-4, 6\}, \{4, -8\}\} \qquad \pi_{\text{even}} = \{\{4\}, \{-2\}, \{2, -4\}\}$$

$$\pi^{\text{odd}} = \{\{-1, 7\}, \{1, -5\}, \{-3, 5\}, \{3, -7\}\} \qquad \pi_{\text{odd}} = \{\{-1\}, \{1, -3\}, \{3\}\}.$$

6.3.1 Case $U^*_{N,i_1}U_{N,i_2} = W^*YHW/\sqrt{N}$

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

$$\mathbf{h_1}(\mathbf{i}) = \prod_{k=1}^{m_1} H(i_{-2k+1}, i_{2k-1})H^*(i_{-2k}, i_{2k}), \qquad \mathbf{h}_2(\mathbf{i}) = \prod_{k=m_1+1}^{m_1+m_2} H(i_{-2k+1}, i_{2k-1})H^*(i_{-2k}, i_{2k}),$$
$$\mathbf{y}_1(\mathbf{i}) = \prod_{k=1}^{m_1} Y(i_{-2k+1}, i_{-2k+1})Y(i_{2k-1}, i_{2k-1}), \quad \mathbf{y}_2(\mathbf{i}) = \prod_{k=m_1+1}^{m_1+m_2} Y(i_{-2k+1}, i_{-2k+1})Y(i_{2k-1}, i_{2k-1});$$

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

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

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

$$\sum_{\substack{\mathbf{i}:[\pm 2m]\to[N] \\ \ker(\mathbf{i})=\pi}} \mathbf{h}(\mathbf{i} \circ \boldsymbol{\sigma})\mathbb{E}[\mathbf{w}(\mathbf{i}, \mathbf{j})]\,\mathbb{E}[\mathbf{y}(\mathbf{i})] - \sum_{\substack{\mathbf{i}:[\pm 2m]\to[N] \\ \ker(\mathbf{i})=\pi_1 \sqcup \pi_2}} \mathbf{h}(\mathbf{i} \circ \boldsymbol{\sigma})\mathbb{E}[\mathbf{w}_1(\mathbf{i}, \mathbf{j})]\,\mathbb{E}[\mathbf{w}_2(\mathbf{i}, \mathbf{j})]\,\mathbb{E}[\mathbf{y}_1(\mathbf{i})]\,\mathbb{E}[\mathbf{y}_2(\mathbf{i})]$$

$$= \mathfrak{C}_2[\pi] \tag{6.16}$$

where π_1 and π_2 denote the restrictions of π to $[\pm 2m_1]$ and $[\pm 2m] \setminus [\pm 2m_1]$, respectively, and σ is the cycle permutation given by

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

Proposition 6.3.3. 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 (6.9) and (6.16), respectively, then for every even partition $\pi \in P(\pm 2m)$ we have

$$N^m \mathfrak{c}_2[\pi] = \mathfrak{C}_2[\pi] + O(N^{-1}) \tag{6.17}$$

Proof. Fix a function $\mathbf{j} : [\pm 2m] \to [N]$ 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

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

respectively. Thus, from (6.9) and the linearity of the covariance, we have that

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

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 $\boldsymbol{\sigma}$ are defined as above. But, for every function $\mathbf{i} : [\pm 2m] \to [N]$, we have that

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

so we obtain

$$N^m \mathfrak{c}_2[\pi] = \sum_{\mathbf{i}:[\pm 2m]\to[N]} \mathbf{h}(\mathbf{i}\circ\boldsymbol{\sigma}) \cdot \operatorname{cov}\left[\mathbf{w}_1(\mathbf{i},\mathbf{j})\cdot\mathbf{y}_1(\mathbf{i}), \mathbf{w}_2(\mathbf{i},\mathbf{j})\cdot\mathbf{y}_2(\mathbf{i})\right]. \tag{6.18}$$

Moreover, from (4.3) we get that

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

provided $\ker(\mathbf{i}) \neq \pi$ and $\ker(\mathbf{i}) \not\geq \pi_1 \sqcup \pi_2$, respectively. And hence, equality in (6.18) becomes

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

To obtain (6.17), it only remains to show that for $\theta \gneq \pi_1 \sqcup \pi_2$, i.e., $\theta \geq \pi_1 \sqcup \pi_2$ but $\theta \neq \pi_1 \sqcup \pi_2$,

implies

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

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

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

Now, $\mathbf{h}(\mathbf{i}\circ\boldsymbol{\sigma})$ has absolute value 1 for any function $\mathbf{i} : [\pm 2m] \to [N]$ and $|\mathbb{E}\left[\mathbf{y}_1(\mathbf{i})\right]\mathbb{E}\left[\mathbf{y}_2(\mathbf{i})\right]| \leq 1$, so (4.3) implies

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

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

□

Proof of (1) from Proposition 6.3.1. Let Y be the identity matrix I_N. By Proposition 6.3.3, we only need to show that

$$\mathfrak{C}_2[\pi] = \begin{cases} 1 + O\left(N^{-1}\right) & \text{if there symmetric pairing partition } \hat{\theta} \leq \pi \text{ satisfying either (1) or} \\ & \text{(2) from Proposition 5.2.6,} \\ O\left(N^{-1/2}\right) & \text{otherwise.} \end{cases}$$

where $\mathfrak{C}_2[\pi]$ is given by (6.16). Note that from (4.3) and (6.16) we obtain the inequality

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

But then, if $\mathrm{p}_{\sigma^{-1}\circ\pi}$ is a non-zero polynomial, so is $\mathrm{p}_{\sigma^{-1}\circ\pi_1\sqcup\pi_2}$ by Proposition 5.2.4, and therefore, the last inequality and Corollary 5.2.2 would imply $\mathfrak{C}_2[\pi] = O(N^{-1/2})$. And so, we can assume $\mathrm{p}_{\sigma^{-1}\circ\pi}$ is the zero polynomial without loss of generality.

Now, for every function $\mathbf{i}:[\pm 2m]\to[N]$ satisfying $\ker(\mathbf{i}) = \pi$ we have $\mathbf{h}(\mathbf{i}\circ\boldsymbol{\sigma}) = 1$ since $\mathrm{p}_{\sigma^{-1}\circ\pi}$ is the zero polynomial; additionally, (4.3) gives $\mathbb{E}[\mathbf{w}(\mathbf{i},\mathbf{j})] = \frac{(N-\#(\pi))!}{N!}$ since π is an even partition. Thus, from (6.16) we obtain

$$\mathfrak{C}_2[\pi] = 1 - \sum_{\substack{\mathbf{i}:[\pm 2m]\to[N]\\ \ker(\mathbf{i})=\pi_1\sqcup\pi_2}} \mathbf{h}(\mathbf{i}\circ\boldsymbol{\sigma})\mathbb{E}[\mathbf{w}_1(\mathbf{i},\mathbf{j})]\,\mathbb{E}[\mathbf{w}_2(\mathbf{i},\mathbf{j})]\,. \tag{6.19}$$

Moreover, by Proposition 5.2.4, there is a symmetric pairing partition $\hat{\theta}\leq\pi$ such that $\mathrm{p}_{\sigma^{-1}\circ\hat{\theta}}$ is also the zero polynomial, and hence, the partition $\hat{\theta}$ must satisfy one of the conditions *(1)-(6)* from Proposition 5.2.6. 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

$$\mathfrak{C}_2[\pi] = 1 - \frac{(N-\#(\pi_1))!}{N!}\cdot\frac{(N-\#(\pi_2))!}{N!}\cdot\frac{N!}{(N-\#(\pi_1\sqcup\pi_2))!} = O\left(N^{-1}\right). \tag{6.20}$$

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 (4.3) 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 $\mathbf{i} : [\pm 2m] \to [N]$ satisfying $\ker(\mathbf{i}) = \pi_1 \sqcup \pi_2$; moreover, Proposition 5.2.4 implies the polynomial $\mathrm{p}_{\sigma^{-1}\circ\pi_1\sqcup\pi_2}$ is also zero since $\hat{\theta} = \hat{\theta}_1 \sqcup \hat{\theta}_2 \leq \pi_1 \sqcup \pi_2$, and thus, we obtain

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

Hence, (6.20) follows from (6.19) provided $\hat{\theta}$ satisfies either *(3)*, *(4)*, *(5)*, or *(6)* from Proposition 5.2.6.

Assume now $\hat{\theta}$ satisfies either *(1)* or *(2)* from Proposition 5.2.6. 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 $\vec{\mathcal{G}}_{\pi_1\sqcup\pi_2}$ does not satisfy none of the conditions *(1)*-*(6)* from Remark 5.2.7 since $m_1 + m_2 > 2$, and hence, the polynomial $\mathrm{p}_{\sigma^{-1}\circ\pi_1\sqcup\pi_2}$ is non-zero. Thus, by (4.3) and Corollary 5.2.2, we have

$$\left| \sum_{\substack{\mathbf{i}:[\pm 2m]\to[N] \\ \ker(\mathbf{i})=\pi_1\sqcup\pi_2}} \mathbf{h}(\mathbf{i} \circ \boldsymbol{\sigma}) \mathbb{E}\left[\mathbf{w}_1(\mathbf{i}, \mathbf{j})\right] \mathbb{E}\left[\mathbf{w}_2(\mathbf{i}, \mathbf{j})\right] \right| \leq C N^{\#(\pi_1\sqcup\pi_2)-\frac{1}{2}} \cdot \frac{(N - \#(\pi_1))!}{N!} \cdot \frac{(N - \#(\pi_2))!}{N!} \tag{6.21}$$

for some constant $C > 0$ independent from N. Therefore, from (6.19) we get that

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

□

Proof of (2) from Proposition 6.3.1. 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 $\mathrm{p}_{\sigma^{-1}\circ\pi}$ is the zero polynomial and it suffices to show that

$$\mathfrak{C}_2[\pi] = \begin{cases} 1 + O\left(N^{-1}\right) & \text{if there symmetric pairing partition } \hat{\theta} \leq \pi \text{ satisfying (1) from Proposition 5.2.6,} \\ 1 + O\left(N^{-1}\right) & \text{if there symmetric pairing partition } \hat{\theta} \leq \pi \text{ satisfying (2) from Proposition 5.2.6 and the components of } \mathcal{G}_\pi \text{ are all double-loops,} \\ O\left(N^{-1/2}\right) & \text{otherwise.} \end{cases}$$

Let $\pi_{\mathrm{odd},1}$ and $\pi_{\mathrm{odd},2}$ 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 $\pi_{\mathrm{odd},1}$ or $\pi_{\mathrm{odd},2}$ is not even, and hence, we obtain $\mathfrak{C}_2[\pi] = 0$ since (4.2) would imply $\mathbb{E}\left[\mathbf{y}_1(\mathbf{i})\right]\mathbb{E}\left[\mathbf{y}_2(\mathbf{i})\right] = \mathbb{E}\left[\mathbf{y}(\mathbf{i})\right] = 0$ for every function $\mathbf{i} : [\pm 2m] \to [N]$ satisfying $\ker(\mathbf{i}) = \pi$. Thus, we can further assume π_{odd} is even. It then follows from (4.2) and (4.3) that

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

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

$$\mathfrak{C}_2[\pi] = 1 - \sum_{\substack{\mathbf{i}:[\pm 2m]\to[N] \\ \ker(\mathbf{i})=\pi_1 \sqcup \pi_2}} \mathbf{h}(\mathbf{i} \circ \boldsymbol{\sigma}) \mathbb{E}\left[\mathbf{y}_1(\mathbf{i})\right] \mathbb{E}\left[\mathbf{y}_2(\mathbf{i})\right] \mathbb{E}\left[\mathbf{w}_1(\mathbf{i},\mathbf{j})\right] \mathbb{E}\left[\mathbf{w}_2(\mathbf{i},\mathbf{j})\right]. \tag{6.22}$$

By Proposition 5.2.4, there is a symmetric pairing partition $\hat{\theta} \leq \pi$ such that $\mathrm{p}_{\sigma^{-1}\circ\hat{\theta}}$ is also the zero polynomial, and thus, the partition $\hat{\theta}$ must satisfy one of the conditions *(1)-(6)* from Proposition 5.2.6. However, if $\hat{\theta}$ satisfies either *(3)*, *(4)*, *(5)*, or *(6)*, then

$$\mathfrak{C}_2[\pi] = 1 - \frac{N!}{(N - \#(\pi_1 \sqcup \pi_2))!} \cdot \frac{(N - \#(\pi_1))!}{N!} \cdot \frac{(N - \#(\pi_2))!}{N!} = O\left(N^{-1}\right). \tag{6.23}$$

Indeed, suppose $\hat{\theta}$ satisfies either *(3)*, *(4)*, *(5)*, or *(6)* from Proposition 5.2.6, 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 $\mathbf{i} : [\pm 2m] \to [N]$ 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 5.2.4, the polynomial $\mathrm{p}_{\sigma^{-1} \circ \pi_1 \sqcup \pi_2}$ is zero, and hence, we get

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

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 (4.3), 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 $\pi_{\mathrm{odd},1}$ and $\pi_{\mathrm{odd},2}$ are also even since $\hat{\theta}_{\mathrm{odd}}$ is even and $\hat{\theta} = \hat{\theta}_1 \sqcup \hat{\theta}_2 \leq \pi$ implies $\hat{\theta}_{\mathrm{odd}} = \hat{\theta}_{\mathrm{odd},1} \sqcup \hat{\theta}_{\mathrm{odd},2}$, $\hat{\theta}_{\mathrm{odd},1} \leq \pi_{\mathrm{odd},1}$, and $\hat{\theta}_{\mathrm{odd},2} \leq \pi_{\mathrm{odd},2}$ where $\hat{\theta}_{\mathrm{odd},1}$ and $\hat{\theta}_{\mathrm{odd},2}$ denote the restrictions of $\hat{\theta}_{\mathrm{odd}}$ to $[\pm 2m_1]$ and $[\pm 2m] \setminus [\pm 2m_1]$, respectively. Thus, from (4.2), we have

$$\mathbb{E}[\mathbf{y}_1(\mathbf{i})]\,\mathbb{E}[\mathbf{y}_2(\mathbf{i})] = 1.$$

Consequently, we obtain (6.23) from (6.22). Now, similar to $U^*_{N,i_1} U_{N,i_2} = W^* H W / \sqrt{N}$, if the partition $\hat{\theta}$ satisfies either *(1)* or *(2)* from Proposition 5.2.6, then $\mathrm{p}_{\sigma^{-1} \circ \pi_1 \sqcup \pi_2}$ is a non-zero polynomial and (6.21) holds, so, from (6.22), 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 $\mathbf{i} : [\pm 2m] \to [N]$.

It only remains to show that the undirected graph $\mathcal{G}_\pi$ must have only double-loops as connected components if $\hat{\theta}$ satisfies *(2)* from Proposition 5.2.6. So, suppose $\hat{\theta}$ satisfies *(2)* from Proposition 5.2.6. 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 $\mathcal{G}_\pi$ has only double loops as connected components. □

6.3.2 Case $U^*_{N,i_1} U_{N,i_2} = W^* H^* X H W / N$

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

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

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

$$\mathbf{t} = (t_{-1}, t_1, t_{-3}, t_3, \ldots, t_{4m_1+4m_2-1}) = (j_{-1}, j_1, j_{-2}, j_2, \ldots, j_{-2m}, j_{2m}) \tag{6.24}$$

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

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

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

$$\sum_{\substack{\mathbf{i}:[\pm 4m]\to[N] \\ \ker(\mathbf{i})=\widehat{\alpha}\sqcup\pi^{\mathrm{odd}}}} \widehat{\mathbf{h}}(\mathbf{i}\circ\widehat{\boldsymbol{\sigma}})\mathbb{E}[\widehat{\mathbf{w}}(\mathbf{i})]\,\mathbb{E}[\widehat{\mathbf{x}}(\mathbf{i})] - \sum_{\substack{\mathbf{i}:[\pm 4m]\to[N] \\ \ker(\mathbf{i})=\widehat{\alpha}\sqcup\pi_1^{\mathrm{odd}}\sqcup\pi_2^{\mathrm{odd}}}} \widehat{\mathbf{h}}(\mathbf{i}\circ\widehat{\boldsymbol{\sigma}})\mathbb{E}[\widehat{\mathbf{w}}_1(\mathbf{i})]\,\mathbb{E}[\widehat{\mathbf{w}}_2(\mathbf{i})]\,\mathbb{E}[\widehat{\mathbf{x}}_1(\mathbf{i})]\,\mathbb{E}[\widehat{\mathbf{x}}_2(\mathbf{i})]$$

$$= N^m \mathfrak{C}_2[\pi, \alpha] \tag{6.25}$$

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 $\widehat{\sigma} : [\pm 4m] \to [\pm 4m]$ is the permutation with cycle decomposition

$$\widehat{\sigma} = (-1, 1, -2, 2, \ldots, -4m_1, 4m_1)(-4m_1 - 1, 4m_1 + 1, -4m_2 - 2, \ldots, 4m_1 + 4m_2).$$

Proposition 6.3.4. Suppose π is an even partition in $P(\pm 2m)$ and assume $U_{N,i_1}^* U_{N,i_2} = W^* H^* X H W/N$. If $\mathfrak{c}_2[\pi]$ is given by (6.9) and $\mathfrak{C}_2[\pi, \alpha]$ is given by (6.25) for every pairing partition $\alpha \in P_2(2m)$, then

$$N^{2m} \mathfrak{c}_2[\pi] = \left(\sum_{\alpha \in P_2(2m)} \mathfrak{C}_2[\pi, \alpha] \right) + O\left(N^{m-1}\right) \tag{6.26}$$

Proof. Fix a function $\mathbf{j} : [\pm 2m] \to [N]$ satisfying $\ker(\mathbf{j}) = \pi$ and let $\mathbf{t}$ be as in (6.24). The (j_{-k}, j_k)-entry of $U_{N,i_1}^* U_{N,i_2}$ is then given by the sum

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

and hence, by Equation (6.9) and the linearity of the covariance, we get

$$N^{2m}\mathfrak{c}_2[\pi] = \sum_{\mathbf{i}:[\pm 4m]\to[N]} \widehat{\mathbf{g}}(\mathbf{i}) \cdot \operatorname{cov}\big[\widehat{\mathbf{w}}_1(\mathbf{i}, \mathbf{t}\circ\widetilde{\boldsymbol{\sigma}}) \cdot \widehat{\mathbf{x}}_1(\mathbf{i}), \mathbf{w}_2(\mathbf{i}, \mathbf{t}\circ\widetilde{\boldsymbol{\sigma}}) \cdot \widehat{\mathbf{x}}_2(\mathbf{i})\big]$$

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 $\widetilde{\sigma} : [\pm 4m] \to [\pm 4m]$ is the permutation with cycle decomposition

$$\widetilde{\sigma} = (-1, 1, -3, 3, \ldots, -4m_1 + 1, 4m_1 - 1)(-4m_1 - 1, 4m_1 + 1, \ldots, 4m_1 + 4m_2 - 1).$$

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

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

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

$$N^{2m}\mathfrak{c}_2[\pi] = \sum_{\mathbf{i}:[\pm 4m]\to[N]} \widehat{\mathbf{h}}(\mathbf{i}\circ\widehat{\boldsymbol{\sigma}}) \cdot \operatorname{cov}\left[\widehat{\mathbf{w}}_1(\mathbf{i},\mathbf{t}) \cdot \widehat{\mathbf{x}}_1(\mathbf{i}), \mathbf{w}_2(\mathbf{i},\mathbf{t}) \cdot \widehat{\mathbf{x}}_2(\mathbf{i})\right].$$

Now, suppose $\theta = \ker(\mathbf{i})$ for a function $\mathbf{i} : [\pm 4m] \to [N]$. Since $\pi^{\mathrm{odd}} = \ker(\mathbf{t})$, from (4.3) we have that

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

provided $\theta_{\mathrm{odd}} \neq \pi^{\mathrm{odd}}$ and $\theta_{\mathrm{odd}} \not\geq (\pi_1 \sqcup \pi_2)^{\mathrm{odd}} = \pi_1^{\mathrm{odd}} \sqcup \pi_2^{\mathrm{odd}}$, respectively; moreover, (4.2) implies that

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

if θ_{even} is not an even partition, θ_{even} has a block of the form $\{2k, -2k\}$, or $2k \not\sim_\theta -2k$ for

some $k \in [2m]$. Thus, we obtain

$$N^{2m}\mathfrak{c}_2[\pi] = \sum_{\theta\in\widetilde{P}_\pi(\pm 4m)} \sum_{\substack{\mathbf{i}:[\pm 4m]\to[N]\\ \ker(\mathbf{i})=\theta}} \widehat{\mathbf{h}}(\mathbf{i}\circ\widehat{\boldsymbol{\sigma}})\mathbb{E}\left[\widehat{\mathbf{w}}_1(\mathbf{i},\mathbf{t})\widehat{\mathbf{w}}_2(\mathbf{i},\mathbf{t})\right]\mathbb{E}\left[\widehat{\mathbf{x}}_1(\mathbf{i})\widehat{\mathbf{x}}_2(\mathbf{i})\right]$$
$$- \sum_{\theta\in\widetilde{P}_{\pi_1\sqcup\pi_2}(\pm 4m)} \sum_{\substack{\mathbf{i}:[\pm 4m]\to[N]\\ \ker(\mathbf{i})=\theta}} \widehat{\mathbf{h}}(\mathbf{i}\circ\widehat{\boldsymbol{\sigma}})\mathbb{E}\left[\widehat{\mathbf{w}}_1(\mathbf{i},\mathbf{t})\right]\mathbb{E}\left[\widehat{\mathbf{w}}_2(\mathbf{i},\mathbf{t})\right]\mathbb{E}\left[\widehat{\mathbf{x}}_1(\mathbf{i})\right]\mathbb{E}\left[\widehat{\mathbf{x}}_2(\mathbf{i})\right]$$

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 (6.26), it only remains to show that

$$N^{2m}\mathfrak{c}_2[\pi] = \sum_{\theta\in\widehat{P}_\pi(\pm 4m)} \sum_{\substack{\mathbf{i}:[\pm 4m]\to[N]\\ \ker(\mathbf{i})=\theta}} \widehat{\mathbf{h}}(\mathbf{i}\circ\widehat{\boldsymbol{\sigma}})\mathbb{E}\left[\widehat{\mathbf{w}}(\mathbf{i},\mathbf{t})\right]\mathbb{E}\left[\widehat{\mathbf{x}}(\mathbf{i})\right]$$
$$- \sum_{\theta\in\widehat{P}_{\pi_1\sqcup\pi_2}(\pm 4m)} \sum_{\substack{\mathbf{i}:[\pm 4m]\to[N]\\ \ker(\mathbf{i})=\theta}} \widehat{\mathbf{h}}(\mathbf{i}\circ\widehat{\boldsymbol{\sigma}})\mathbb{E}\left[\widehat{\mathbf{w}}_1(\mathbf{i},\mathbf{t})\right]\mathbb{E}\left[\widehat{\mathbf{w}}_2(\mathbf{i},\mathbf{t})\right]\mathbb{E}\left[\widehat{\mathbf{x}}_1(\mathbf{i})\right]\mathbb{E}\left[\widehat{\mathbf{x}}_2(\mathbf{i})\right]$$
$$+ O\left(N^{m-1}\right).$$

Suppose $\theta \in \widetilde{P}_{\pi_1\sqcup\pi_2}(\pm 4m)$. 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., $\theta \in \widehat{P}_{\pi_1 \sqcup \pi_2}(\pm 4m)$; moreover, (4.2) and (4.3) imply that

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

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

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

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

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

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

Proposition 6.3.5. 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 (6.25), then

$$\mathfrak{C}_2[\pi,\alpha] = \begin{cases} 1 + O\left(N^{-1}\right) & \text{if there is a symmetric pairing } \eta \in P(\pm 4m) \text{ satisfying (1) from} \\ & \text{Proposition 5.2.6 and such that } \eta \leq \widehat{\alpha} \sqcup \pi^{\text{odd}}, \\ 1 + O\left(N^{-1}\right) & \text{if } \alpha \neq \alpha_1 \sqcup \alpha_2 \text{ and there is a symmetric pairing } \eta \in P(\pm 4m) \\ & \text{satisfying (3) from Proposition 5.2.6 with k and l even and} \\ & \text{such that } \eta \leq \widehat{\alpha} \sqcup \pi^{\text{odd}}, \\ O(N^{-\frac{1}{2}}) & \text{otherwise.} \end{cases}$$

Proof. Note that if the polynomial $\mathrm{p}_{\widehat{\sigma}^{-1} \circ (\widehat{\alpha} \sqcup \pi^{\text{odd}})}$ is non-zero, then $\mathfrak{C}_2[\pi, \alpha] = O(N^{-1/2})$. Indeed, if $\mathrm{p}_{\widehat{\sigma}^{-1} \circ (\widehat{\alpha} \sqcup \pi^{\text{odd}})}$ is a non-zero polynomial, so is $\mathrm{p}_{\widehat{\sigma}^{-1} \circ (\widehat{\alpha} \sqcup \pi_1^{\text{odd}} \sqcup \pi_2^{\text{odd}})}$ by Proposition 5.2.4, and thus, Corollary 5.2.2 implies there is a constant C independent from N such that

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

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 (4.2), (4.3), and (6.25) we have

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

Assume $\mathrm{p}_{\widehat{\sigma}^{-1} \circ (\widehat{\alpha} \sqcup \pi^{\text{odd}})}$ is the zero polynomial. Then, by Proposition 5.2.4, there is a symmetric pairing partition $\eta \leq \widehat{\alpha} \sqcup \pi^{\text{odd}}$ such that $\mathrm{p}_{\widehat{\sigma}^{-1} \circ \eta}$ is also the zero polynomial, and hence, the partition η must satisfy one of the conditions *(1)-(6)* from Proposition 5.2.6. 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)* can not hold. Now, note that if $\mathrm{p}_{\widehat{\sigma}^{-1}\circ(\widehat{\alpha}\sqcup\beta^{\mathrm{odd}})}$ is zero polynomial for some partition $\beta \in P(\pm 2m)$, then

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

since we would have $\widehat{\mathbf{h}}(\mathbf{i}\circ\widehat{\boldsymbol{\sigma}}) = 1$ for any function $\mathbf{i} : [\pm 4m] \to [N]$ satisfying $\ker(\mathbf{i}) = \widehat{\alpha}\sqcup\beta^{\mathrm{odd}}$. Hence, if α_1, α_2, π_1, and π_2 are all even partitions and the polynomial $\mathrm{p}_{\sigma^{-1}\circ\hat{\alpha}\sqcup\pi_1^{\mathrm{odd}}\sqcup\pi_2^{\mathrm{odd}}}$ is zero, from (4.2), (4.3), and (6.25), we obtain

$$\begin{aligned}&\frac{(N-\#(\pi))!}{N!}\cdot\sum_{\substack{\mathbf{i}:[\pm 4m]\to[N]\\ \ker(\mathbf{i})=\hat{\alpha}\sqcup\pi^{\mathrm{odd}}}}\widehat{\mathbf{h}}(\mathbf{i}\circ\widehat{\boldsymbol{\sigma}}) - \frac{(N-\#(\pi_1))!}{N!}\cdot\frac{(N-\#(\pi_2))!}{N!}\cdot\sum_{\substack{\mathbf{i}:[\pm 4m]\to[N]\\ \ker(\mathbf{i})=\hat{\alpha}\sqcup\pi_1^{\mathrm{odd}}\sqcup\pi_2^{\mathrm{odd}}}}\widehat{\mathbf{h}}(\mathbf{i}\circ\widehat{\boldsymbol{\sigma}})\\ &= N^m\mathfrak{C}_2[\pi,\alpha] = O\left(N^{m-1}\right)\end{aligned} \tag{6.27}$$

On the other hand, if either α_1 or α_2 is not an even partition, from (4.2) and (6.25), we get

$$\mathfrak{C}_2[\pi,\alpha] = \frac{1}{N^m}\cdot\frac{(N-\#(\pi))!}{N!}\cdot\sum_{\substack{\mathbf{i}:[\pm 4m]\to[N]\\ \ker(\mathbf{i})=\hat{\alpha}\sqcup\pi^{\mathrm{odd}}}}\widehat{\mathbf{h}}(\mathbf{i}\circ\widehat{\boldsymbol{\sigma}}) = 1 + O\left(N^{-1}\right). \tag{6.28}$$

Suppose η satisfies *(3)* from Proposition 5.2.6 and let $1 \le k \le 4m_1$ and $4m_1+1 \le l \le 4m_1+4m_2$ such that $\eta = \{\{\widehat{\sigma}^{t_1}(-k), \widehat{\sigma}^{-t_1}(k)\}, \{\widehat{\sigma}^{t_2}(-l), \widehat{\sigma}^{-t_2}(l)\} \mid t_2, t_2 \ge 0\}$. 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 $\mathrm{p}_{\sigma^{-1}\circ\hat{\alpha}\sqcup\pi_1^{\mathrm{odd}}\sqcup\pi_2^{\mathrm{odd}}}$ is also the zero polynomial, π_1 and π_2 are both even partitions, and $\alpha = \alpha_1 \sqcup \alpha_2$, so (6.27) holds. Second, if $k+l$ is odd, then $\alpha = \alpha_1 \sqcup \alpha_2$ and $\pi = \pi_1 \sqcup \pi_2$, but then (6.27) 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 $\alpha \ne \alpha_1 \sqcup \alpha_2$. However, if $\alpha = \alpha_1 \sqcup \alpha_2$, we already know that

$\mathfrak{C}_2[\pi,\alpha] = O(N^{-1})$ from (6.27), and if $\alpha \neq \alpha_1 \sqcup \alpha_2$, then α_1 and α_2 are not even partitions, so (6.28) holds. Finally, if η satisfies *(1)* from Proposition 5.2.6, we must have $\alpha \neq \alpha_1 \sqcup \alpha_2$, so we obtain $\mathfrak{C}_2[\pi,\alpha] = 1 + O\left(N^{-1}\right)$. □

Proof of (3) from Proposition 6.3.1. 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 (6.25) for each pairing partition $\alpha \in P_2(2m)$. By Proposition 6.3.5, we have that

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

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

$$E_\pi = \left\{ \alpha \in P_2(2m) \;\middle|\; \begin{array}{c} \eta \leq \widehat{\alpha} \sqcup \pi^{\mathrm{odd}} \text{ for some symmetric pairing } \eta \in P(\pm 4m) \\ \text{satisfying (1) from Proposition 5.2.6} \end{array} \right\}$$

and

$$F_\pi = \left\{ \alpha \in P_2(2m) \;\middle|\; \begin{array}{c} \alpha \neq \alpha_1 \sqcup \alpha_2 \text{ and } \eta \leq \widehat{\alpha} \sqcup \pi^{\mathrm{odd}} \text{ for some symmetric pairing} \\ \eta \in P(\pm 4m) \text{ satisfying (3) from Proposition 5.2.6 with } k \text{ and } l \text{ even} \end{array} \right\}.$$

Thus, by Proposition 6.3.4, 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 5.2.6, $\eta_\alpha \leq \widehat{\alpha} \sqcup \pi^{\mathrm{odd}}$, and $\eta_\beta \leq \widehat{\beta} \sqcup \pi^{\mathrm{odd}}$. 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

$$\widehat{\sigma} = (-1, 1, -2, 2, \ldots, -4m_1, 4m_1)(-4m_1{-}1, 4m_1{+}1, -4m_1{-}2, \ldots, -4m_1{-}4m_2, 4m_1{+}4m_2).$$

But then, we must have

$$\widehat{\sigma}^{-t}(2l_\alpha - 1) \sim_{\widehat{\alpha}\sqcup\pi^{\mathrm{odd}}} \widehat{\sigma}^{t}(-1) \sim_{\widehat{\beta}\sqcup\pi^{\mathrm{odd}}} \widehat{\sigma}^{-t}(2l_\beta - 1) \quad \forall t \geq 0 \tag{6.29}$$

since $\eta_\alpha \leq \widehat{\alpha} \sqcup \pi^{\mathrm{odd}}$ and $\eta_\beta \leq \widehat{\beta} \sqcup \pi^{\mathrm{odd}}$, 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

$$\sigma = (-1, 1, -2, 2, \ldots, -2m_1, 2m_1)(-2m_1{-}1, 2m_1{+}1, -2m_1{-}2, \ldots, -2m_1{-}2m_2, 2m_1{+}2m_2).$$

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 (6.29) 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 5.2.6 with k and l even, $\eta_\alpha \leq \widehat{\alpha} \sqcup \pi^{\mathrm{odd}}$, and $\eta_\beta \leq \widehat{\beta} \sqcup \pi^{\mathrm{odd}}$. Then, there exists 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

$$\widehat{\sigma}^t(-2k_\alpha) \sim_{\widehat{\alpha}\sqcup\pi^{\text{odd}}} \widehat{\sigma}^{-t}(2k_\alpha) \quad \text{and} \quad \widehat{\sigma}^t(-2k_\beta) \sim_{\widehat{\beta}\sqcup\pi^{\text{odd}}} \widehat{\sigma}^{-t}(2k_\beta) \quad \forall t \geq 0 \tag{6.30}$$

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

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

and

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

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 (6.30), we also have that

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

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

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

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 $s \equiv 0 \mod 4m_1$, 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

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

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 $2m_1+1\le l\le 2m_1+2m_2$ so that

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

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

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

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

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 $\pi=\pi_1\sqcup\pi_2$. □

Chapter 7

Conclusions

(1) The random matrix ensemble $\{W_{N,1}, H_N W_{N,2}\}_{N=1}^{\infty}$ satisfies the hypothesis in Lemma 1.2.3, and hence, Theorem 1.2.2 is proved once we show (1.12) 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 (6.17) still holds in this case. Then, following similar steps to those in the proof of Proposition 6.3.1 and Lemma 6.3.2 and letting $U_{N,i_1}^* U_{N,i_2} = \frac{1}{\sqrt{N}} W_{N,1}^* H_N W_{N,2}$, we conclude

$$\sum_{\substack{\pi \in P_{\text{even}}(\pm 2m) \\ \pi \leq \theta}} N^m \mathfrak{c}_2[\pi]\, \mu(\pi,\theta) = \begin{cases} 1 + O\left(N^{-1/2}\right) & \text{if } \theta \text{ is a pairing partition satisfying (1)} \\ & \text{from Proposition 5.2.6,} \\ O\left(N^{-1/2}\right) & \text{otherwise.} \end{cases}$$

(2) 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 holds when we replace H_N by a general Hadamard matrix H'_N, for

instance, (5.10), (5.12), and (5.14). Thus, to determine the corresponding induced fluctuations moments, one needs to compute graph sums of H'_N and obtain similar results to those from Section 5.2. However, the results for graph sums of H_N were possible thanks to the reciprocity theorem for generalized Gauss sums and it is not obvious what could be used for a general H'_N.

(3) Although Proposition 4.3.18 and Corollary 4.3.20 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 multi-linear functionals. These conditions together with bounds for graph sums can be exploited to study higher order moments. In particular, the relations (6.4) and (6.10) can be used to determine the higher order moments induced by Haar-unitary and Haar-orthogonal via the Weingarten Calculus from [4] and [5].

Bibliography

[1] Greg W. Anderson and Brendan Farrell. Asymptotically liberating sequences of random unitary matrices. *Adv. Math.*, 255:381–413, 2014.

[2] Greg W. Anderson, Alice Guionnet, and Ofer Zeitouni. *An introduction to random matrices*, volume 118 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2010.

[3] Bruce C. Berndt, Ronald J. Evans, and Kenneth S. Williams. *Gauss and Jacobi sums*. Canadian Mathematical Society Series of Monographs and Advanced Texts. John Wiley & Sons, Inc., New York, 1998. A Wiley-Interscience Publication.

[4] Benoît Collins. Moments and cumulants of polynomial random variables on unitary groups, the Itzykson-Zuber integral, and free probability. *Int. Math. Res. Not.*, (17):953–982, 2003.

[5] Benoît Collins and Piotr Śniady. Integration with respect to the Haar measure on unitary, orthogonal and symplectic group. *Comm. Math. Phys.*, 264(3):773–795, 2006.

[6] Alan Edelman and N. Raj Rao. Random matrix theory. *Acta Numer.*, 14:233–297, 2005.

[7] Zhiwei Hao and Mihai Popa. A combinatorial result on asymptotic independence relations for random matrices with non-commutative entries. *J. Operator Theory*, 80(1):47–76, 2018.

[8] Yong Jiao and Mihai Popa. On fluctuations of traces of large matrices over a non-commutative algebra. *J. Operator Theory*, 73(1):71–90, 2015.

[9] J. Keating. The Riemann zeta-function and quantum chaology. In *Quantum chaos (Varenna, 1991)*, Proc. Internat. School of Phys. Enrico Fermi, CXIX, pages 145–185. North-Holland, Amsterdam, 1993.

[10] James A. Mingo and Mihai Popa. Real second order freeness and Haar orthogonal matrices. *J. Math. Phys.*, 54(5):051701, 35, 2013.

[11] James A. Mingo and Mihai Popa. Freeness and the transposes of unitarily invariant random matrices. *J. Funct. Anal.*, 271(4):883–921, 2016.

[12] James A. Mingo, Piotr Śniady, and Roland Speicher. Second order freeness and fluctuations of random matrices. II. Unitary random matrices. *Adv. Math.*, 209(1):212–240, 2007.

[13] James A. Mingo and Roland Speicher. Second order freeness and fluctuations of random matrices. I. Gaussian and Wishart matrices and cyclic Fock spaces. *J. Funct. Anal.*, 235(1):226–270, 2006.

[14] James A. Mingo and Roland Speicher. Sharp bounds for sums associated to graphs of matrices. *J. Funct. Anal.*, 262(5):2272–2288, 2012.

[15] James A. Mingo and Roland Speicher. *Free probability and random matrices*, volume 35 of *Fields Institute Monographs*. Springer, New York; Fields Institute for Research in Mathematical Sciences, Toronto, ON, 2017.

[16] Naofumi Muraki. The five independences as natural products. *Infin. Dimens. Anal. Quantum Probab. Relat. Top.*, 6(3):337–371, 2003.

[17] Alexandru Nica and Roland Speicher. *Lectures on the combinatorics of free probability*, volume 335 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 2006.

[18] Catherine Emily Iska Redelmeier. Real second-order freeness and the asymptotic real second-order freeness of several real matrix models. *Int. Math. Res. Not. IMRN*, (12):3353–3395, 2014.

[19] Roland Speicher. On universal products. In *Free probability theory (Waterloo, ON, 1995)*, volume 12 of *Fields Inst. Commun.*, pages 257–266. Amer. Math. Soc., Providence, RI, 1997.

[20] Antonio M. Tulino and Sergio Verdú. Random matrix theory and wireless communications. *Commun. Inf. Theory*, 1(1):1–182, 2004.

[21] D. V. Voiculescu, K. J. Dykema, and A. Nica. *Free random variables*, volume 1 of *CRM Monograph Series*. American Mathematical Society, Providence, RI, 1992. A noncommutative probability approach to free products with applications to random matrices, operator algebras and harmonic analysis on free groups.

[22] Dan Voiculescu. Symmetries of some reduced free product C^*-algebras. In *Operator algebras and their connections with topology and ergodic theory (Buşteni, 1983)*, volume 1132 of *Lecture Notes in Math.*, pages 556–588. Springer, Berlin, 1985.

[23] Dan Voiculescu. Limit laws for random matrices and free products. *Invent. Math.*, 104(1):201–220, 1991.

[24] Eugene P. Wigner. Characteristic vectors of bordered matrices with infinite dimensions. *Ann. of Math. (2)*, 62:548–564, 1955.

[25] John Wishart. The generalised product moment distribution in samples from a normal multivariate population. *Biometrika*, 20A(1/2):32–52, 1928.