Spectral distribution of random matrices from Mutually Unbiased Bases

Chin Hei Chan∗and Maosheng Xiong†

Abstract

Two group randomness tests have been investigated in the literature for linear codes over finite fields, based on the Marchenko-Pastur and Wigner’s semicircle laws respectively. Authors proved that linear codes with dual distance at least 5 perform well in both tests. In this paper, we prove that a large collection of mutually unbiased bases over \( \mathbb{C}^n \) also behave well in these two group randomness tests.

1 Introduction

Random matrix theory is the study of matrices whose entries are random variables. Of particular interest is the study of eigenvalue statistics of random matrices such as the empirical spectral distribution. This has been broadly investigated in a wide variety of areas, including statistics [24], number theory [17], economics [18], theoretical physics [23] and communication theory [21].

Most of the matrix models considered in the literature were matrices whose entries are independent. In a series of papers (see [2, 3, 26], initiated by [1]), the authors studied the behaviour of a sample-covariance type matrix model formed by choosing codewords from linear codes over finite fields randomly. After significant progresses, they finally achieved in the conclusion that such matrices behave like truly sample-covariance matrices in terms of empirical spectral distribution as long as the minimum Hamming distance of the dual code is at least 5. More precisely, the limiting spectral distribution is the Marchenko-Pastur (MP) law. This result can be considered as a joint randomness test on sequences derived from linear codes, and is called a “group randomness” property.

More recently, a different normalization of the sample-covariance type matrix model based on linear codes has been investigated (initiated in [11] and slightly improved in [11]). Authors proved that the model behaves like the truly random analogue that the limiting spectral distribution is the Wigner’s semicircle (SC) law, again under the condition that dual distance of the linear code is at least 5. This hence gives another group randomness test.

In this paper we perform the above two group randomness tests to mutually unbiased bases (MUBs). A collection \( \{ \mathcal{B}_i \}_{i=1}^m \) of orthonormal bases in \( \mathbb{C}^n \) are called mutually unbiased if for any \( i \neq j, v_i \in \mathcal{B}_i \) and \( v_j \in \mathcal{B}_j \), we have

\[
|\langle v_i, v_j \rangle| = \frac{1}{\sqrt{n}}.
\]

∗C. Chan is at the Dept. of Mathematics, Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong (email: chchanam@connect.ust.hk).
†M. Xiong is at the Dept. of Mathematics, Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong (email: mamsxiong@ust.hk).
Here \( \langle v_i, v_j \rangle \) is the standard inner product of the vectors \( v_i \) and \( v_j \) in \( \mathbb{C}^n \). MUBs have been widely studied especially in quantum physics and quantum cryptography (see [6, 7, 8, 19]).

It is well-known that for any \( n \), there can at most be \( n + 1 \) MUBs in \( \mathbb{C}^n \) (see [5, 12, 13, 15, 25]). In particular this upper bound is achieved whenever \( n \) is a prime power (see [5, 14, 25]). Some explicit constructions in this case can be seen in [16]. However for a general \( n \), the true maximum for the number of MUBs in \( \mathbb{C}^n \) is still unknown.

The main results of this paper are as follows.

**Theorem 1.** Let \( \mathcal{B} = \bigsqcup_{i=1}^{m} \mathcal{B}_i \) be a collection of \( m \geq \sqrt{n} \) MUBs in \( \mathbb{C}^n \). Let \( \Phi_n \) be a \( p \times n \) random matrix whose rows are chosen from \( \mathcal{B} \) with uniform probability and independently, where \( y := \frac{p}{n} \in (0, 1) \) is fixed. Let \( G_n = \Phi_n \Phi_n^* \). Let \( F_{G_n} \) and \( F_{MP,y} \) be the empirical spectral distribution of \( G_n \) and the cumulative distribution function of the Marchenko-Pastur law respectively, where the density function of the latter is given by

\[
f_{MP,y}(x) = \frac{1}{2\pi x y} \sqrt{(b-x)(x-a)} 1_{[a,b]}(x)dx.
\]

Here the constant \( a \) and \( b \) are defined as

\[
a = (1 - \sqrt{y})^2, \quad b = (1 + \sqrt{y})^2,
\]

and \( 1_{[a,b]} \) is the indicator function of the interval \([a,b] \).

Then as \( n \to \infty \), we have

\[
F_{G_n}(x) \to F_{MP,y}(x) \quad \forall x \in \mathbb{R} \quad \text{in probability}.
\]

**Theorem 2.** Let \( \mathcal{B} = \bigsqcup_{i=1}^{m} \mathcal{B}_i \) be a collection of \( m \geq \sqrt{n} \) MUBs in \( \mathbb{C}^n \). Let \( \Phi_n \) be a \( p \times n \) random matrix whose rows are chosen from \( \mathcal{B} \) with uniform probability and pairwisely distinct. Let \( G_n = \Phi_n \Phi_n^* \) and \( M_n = \left(n/p\right)^{1/2}(G_n - I_p) \). Let \( F_{M_n} \) and \( F_{SC} \) be the empirical spectral distribution of \( M_n \) and the cumulative distribution function of the Wigner’s semicircle law respectively, where the density function of the latter is given by

\[
f_{SC}(x) = \frac{1}{2\pi} \sqrt{4 - x^2} 1_{[-2,2]}(x)dx.
\]

Assume \( p \to \infty \) and \( \frac{p}{n} \to 0 \) as \( n \to \infty \). Then as \( n \to \infty \), we have

\[
F_{M_n}(x) \to F_{SC}(x) \quad \forall x \in \mathbb{R} \quad \text{in probability}.
\]

### 2 Proof of Theorem 1

Let \( \mathcal{B} = \bigsqcup_{i=1}^{m} \mathcal{B}_i \) be a collection of \( m \) MUBs in \( \mathbb{C}^n \) written as row vectors, where \( m \geq \sqrt{n} \), each \( \mathcal{B}_i \) is an orthonormal basis of \( \mathbb{C}^n \), and for \( 1 \leq i \neq j \leq m \) and any \( v_i \in \mathcal{B}_i, v_j \in \mathcal{B}_j \), we have

\[
|\langle v_i, v_j \rangle| = \frac{1}{\sqrt{n}}. \tag{1}
\]

To choose \( p \) elements from \( \mathcal{B} \), we define the probability space \( \Omega_p \) to be the set of all maps \( s : [1..p] \to \mathcal{B} \) endowed with uniform probability. Here \([1..p]\) denotes the set of all integers between 1 and \( p \) (both inclusive). Then we have \( \#\Omega_p = (mn)^p \).
For each \( s \in \Omega_p \), we can construct the corresponding \( p \times n \) matrix

\[
\Phi(s) = \begin{bmatrix}
s(1) \\
s(2) \\
\vdots \\
s(p)
\end{bmatrix}.
\]

Let

\[
G(s) = \Phi(s)\Phi(s)^*.
\]

This is a \( p \times p \) matrix whose \((i, j)\)-th entry is given by \( \langle s(i), s(j) \rangle \).

Let \( \lambda_1(s), \lambda_2(s), \ldots, \lambda_p(s) \in \mathbb{R} \) be the eigenvalues of \( G(s) \). Given any positive integer \( \ell \), define

\[
A_{\ell}(s) := \frac{1}{p} \sum_{i=1}^{p} \lambda_i(s)^\ell = \frac{1}{p} \text{Tr}(G(s)^\ell),
\]

which is the \( \ell \)-th moment of the empirical spectral distribution of \( G(s) \). Here \( \text{Tr}(G(s)^\ell) \) is the trace of the matrix \( G(s)^\ell \).

Denote by \( \mathbb{E}(\cdot, \Omega_p) \) and \( \text{Var}(\cdot, \Omega_p) \) the expectation and variance over the probability space \( \Omega_p \) respectively. In order to prove Theorem 1 it suffices to prove the following two statements (see [4]):

(i) \( \mathbb{E}(A_{\ell}(s), \Omega_p) \to A_{\ell,\text{MP}} \) as \( n \to \infty \), where \( A_{\ell,\text{MP}} \) is the \( \ell \)-th moment of the Marchenko-Pastur law given explicitly by

\[
A_{\ell,\text{MP}, y} = \sum_{i=0}^{\ell-1} \frac{y^i}{i+1} \binom{\ell}{i} \left( \frac{\ell}{i} \right) - \frac{1}{m+1} \left( \frac{1}{m} + \frac{1}{n} \right).
\]

(ii) \( \text{Var}(A_{\ell}(s), \Omega_p) \to 0 \) as \( n \to \infty \).

More precisely, we have the following two estimates:

**Theorem 3.** For any fixed positive integer \( \ell \),

\[
\mathbb{E}(A_{\ell}(s), \Omega_p) = \sum_{i=0}^{\ell-1} \frac{y^i}{i+1} \binom{\ell}{i} \left( \frac{\ell}{i} \right) - \frac{1}{m+1} \left( \frac{1}{m} + \frac{1}{n} \right) + O_{\ell} \left( \frac{1}{m} + \frac{1}{n} \right).
\]

**Theorem 4.** For any fixed positive integer \( \ell \),

\[
\text{Var}(A_{\ell}(s), \Omega_p) = O_{\ell} \left( \frac{1}{mn} + \frac{1}{n^2} \right).
\]

The rest of this section will be devoted to the proofs of these two theorems.

### 2.1 Problem Set-up

We define \( \gamma : [0..\ell] \to [1..p] \) to be a closed path if \( \gamma(0) = \gamma(\ell) \). Denote by \( \Pi_{\ell,p} \) the set of all closed paths from \([0..\ell]\) to \([1..p]\).

Now for any \( s \in \Omega_p \) and \( \gamma \in \Pi_{\ell,p} \), we define

\[
\omega_\gamma(s) := \langle s \circ \gamma(0), s \circ \gamma(1) \rangle \langle s \circ \gamma(1), s \circ \gamma(2) \rangle \cdots \langle s \circ \gamma(\ell - 1), s \circ \gamma(\ell) \rangle.
\]

(4)
Expanding $\text{Tr}(\mathcal{G}(s)^\ell)$, it is easy to see that

$$A_\ell(s) = \frac{1}{p} \sum_{\gamma \in \Pi_{\ell,p}} \omega_\gamma(s).$$

This implies

$$\mathbb{E}(A_\ell(s), \Omega_p) = \frac{1}{p} \sum_{\gamma \in \Pi_{\ell,p}} \mathbb{E}(\omega_\gamma(s), \Omega_p).$$

Denote by $\Sigma_p$ the set of all permutations of $[1..p]$, and define

$$V_\gamma = \gamma([0..\ell]) \subset [1..p], \quad v_\gamma = \#V_\gamma, \quad \Omega(V_\gamma) := \{s : V_\gamma \to 2^\mathcal{B}\},$$

where $\Omega(V_\gamma)$ is made into a probability space by endowing with uniform probability. Note that we have $\#\Omega(V_\gamma) = (mn)^{v_\gamma}$.

Following the argument in [26], it can be easily seen that

$$\mathbb{E}(A_\ell(s), \Omega_p) = \frac{1}{p} \sum_{\gamma \in \Pi_{\ell,p}/\Sigma_p} \frac{p!}{(p - v_\gamma)!} W_\gamma,$$

where $\Pi_{\ell,p}/\Sigma_p$ is the set of representatives of equivalence classes under the equivalence relation

$$\gamma \sim \gamma' \iff \gamma = \sigma \circ \gamma' \quad \exists \sigma \in \Sigma_p,$$

and

$$W_\gamma := \mathbb{E}(\omega_\gamma(s), \Omega(V_\gamma)).$$

### 2.2 Proof of Theorem 3

The evaluation of $W_\gamma$ as defined in (6) involves a combinatorial argument and is quite technical. In order to streamline the proof, we assume its estimation in this section and first give a proof of Theorem 3 from it.

**Lemma 5.** For any $\gamma \in \Pi_{\ell,p}/\Sigma_p$,

$$W_\gamma = \begin{cases} n^{1-v_\gamma} & (\gamma \in \Gamma_\ell) \\ O_{v_\gamma} (n^{1-v_\gamma}(m^{-1} + n^{-1})) & (\gamma \notin \Gamma_\ell), \end{cases}$$

where $\Gamma_\ell \subset \Pi_{\ell,p}/\Sigma_p$ is the subset consisting of all closed paths $\gamma$ that can be reduced to a single loop on a single point through reduction processes to be defined later.

Assuming Lemma 5 and also noting the fact that

$$\sum_{\gamma \in \Pi_{\ell,p}/\Sigma_p} 1 < v_\ell \leq \ell^\ell, \quad \forall v \leq \ell,$$  

(7)
Equation (5) implies

\[ \mathbb{E}(A_t(s), \Omega_p) = \frac{1}{p} \sum_{\gamma \in \Gamma_t} \frac{p!}{(p-v_{\gamma})!} n^{1-v_{\gamma}} + \frac{1}{p} \sum_{\gamma \notin \Gamma_t} \frac{p!}{(p-v_{\gamma})!} O_{v_{\gamma}} \left( n^{1-v_{\gamma}} \left( \frac{1}{m} + \frac{1}{n} \right) \right) \]

\[ = \sum_{\gamma \in \Gamma_t} \left( \frac{p}{n} \right)^{v_{\gamma}-1} \left( 1 + O_t \left( \frac{1}{p} \right) \right) + O \left( \frac{1}{m} + \frac{1}{n} \right) \]

\[ = \sum_{v=1}^{\ell} y^{v-1} \sum_{\gamma \in \Gamma_t} 1 + O_t \left( \frac{1}{m} + \frac{1}{n} \right) \]

A simple combinatorial argument (see [4, Section IV-E]) shows that the quantity \( \sum_{\gamma \in \Gamma_t, v_{\gamma}=1} 1 \) counts the number of double-trees (that is, the graph of non-coincident edges of the path is a tree and each involved edge is traversed exactly twice) with \( \ell \) non-coincident edges and \( v \) vertices in one bipartite side, and can be evaluated as (see [4, Lemma 3.4])

\[ \sum_{\gamma \in \Gamma_t \atop v_{\gamma}=1} 1 = \frac{1}{v} \left( \frac{\ell}{v-1} \right)^{\ell-1}. \]

Combining all the above completes the proof of Theorem 3.

2.3 Proof of Theorem 4

Now we proceed to prove Theorem 4.

First we define the notations

\[ V_{\gamma_1, \gamma_2} := V_{\gamma_1} \cup V_{\gamma_2}, \quad V_{\gamma_1 \cap \gamma_2} := V_{\gamma_1} \cap V_{\gamma_2}, \quad v_{\gamma_1, \gamma_2} := \# V_{\gamma_1, \gamma_2}, \quad v_{\gamma_1 \cap \gamma_2} = \# V_{\gamma_1 \cap \gamma_2}. \]

Then we can expand the quantity \( \text{Var}(A_t(s), \Omega_p) \) as

\[ \text{Var}(A_t(s), \Omega_p) = \mathbb{E}(|A_t(s)|^2, \Omega_p) - |\mathbb{E}(A_t(s), \Omega_p)|^2 \]

\[ = \frac{1}{p^2} \sum_{\gamma_1, \gamma_2 \in \Pi_{\ell,p}} \left( \mathbb{E}(\omega_{\gamma_1}(s), \overline{\omega_{\gamma_2}(s)}, \Omega_p) - \mathbb{E}(\omega_{\gamma_1}(s), \Omega_p) \overline{\mathbb{E}(\omega_{\gamma_2}(s), \Omega_p)} \right) \]

\[ = \frac{1}{p^2} \sum_{(\gamma_1, \gamma_2) \in \Pi_{\ell,p}^2 / \Sigma_p} \frac{p!}{(p-v_{\gamma_1, \gamma_2})!} (W_{\gamma_1, \gamma_2} - W_{\gamma_1 \overline{\gamma_2}}), \quad (8) \]

where \( \Pi_{\ell,p}^2 / \Sigma_p \) is the set of representatives of equivalence classes of all the pairs \((\gamma_1, \gamma_2) \in \Pi_{\ell,p}^2 \) under the equivalence relation

\[(\gamma_{11}, \gamma_{12}) \sim (\gamma_{21}, \gamma_{22}) \iff (\gamma_{11}, \gamma_{12}) = (\sigma \circ \gamma_{21}, \sigma \circ \gamma_{22}) \quad \exists \sigma \in \Sigma_p, \]

and

\[ W_{\gamma_1, \gamma_2} := \mathbb{E}(\omega_{\gamma_1}(s), \overline{\omega_{\gamma_2}(s)}, \Omega(V_{\gamma_1, \gamma_2})). \quad (9) \]

If \( v_{\gamma_1 \cap \gamma_2} = 0 \) (or equivalently \( V_{\gamma_1 \cap \gamma_2} = \emptyset \)), then the quantities \( \omega_{\gamma_1}(s) \) and \( \omega_{\gamma_2}(s) \) are independent. Hence we clearly have \( W_{\gamma_1, \gamma_2} = W_{\gamma_1} \overline{W}_{\gamma_2} \).

Now we consider the case \( v_{\gamma_1 \cap \gamma_2} \geq 1 \). By choosing different starting points if necessary, we may
assume $\gamma_1(0) = \gamma_2(0)$.

Then it is easy to see that the map $\gamma_{1,2} : [0..2\ell] \to [1..p]$ defined by

$$
\gamma_{1,2}(i) = \begin{cases} 
\gamma_1(i) & (0 \leq i \leq \ell) \\
\gamma_2(2\ell - i) & (\ell \leq i \leq 2\ell)
\end{cases}
$$  \hspace{1cm} (10)

is a closed path with length $2\ell$ and $v_{\gamma_1,\gamma_2}$ vertices. In addition, we have $W_{\gamma_1,\gamma_2} = W_{\gamma_{1,2}}$.

Let $\Gamma$ denote the set of pairs $(\gamma_1, \gamma_2) \in \Pi^2_{\ell,p}/\Sigma_p$ with $v_{\gamma_1,\gamma_2} \geq 1$ such that $\gamma_{1,2} \in \Gamma_2$. If $(\gamma_1, \gamma_2) \in \Gamma$, then $\gamma_{1,2}$ corresponds to double-trees, and therefore $\gamma_1$ and $\gamma_2$ are both traversed on trees. This means that for both $\gamma_1$ and $\gamma_2$ each edge involved should be traversed at least twice. If $v_{\gamma_1,\gamma_2} \geq 2$, then by considering the paths between two distinct overlapping vertices, we see that they either form a cycle or the edges involved are traversed at least four times overall, a contradiction. Hence $v_{\gamma_1,\gamma_2} = 1$, so that the edges of $\gamma_1$ and $\gamma_2$ do not overlap and both $\gamma_1, \gamma_2 \in \Gamma_2$.

On the other hand, if $v_{\gamma_1,\gamma_2} = 1$ and both $\gamma_1, \gamma_2 \in \Gamma_\ell$, then it is clear that $\gamma_{1,2} \in \Gamma_\ell$.

Hence if $(\gamma_1, \gamma_2) \in \Gamma$, then by Lemma 5, we have

$$
W_{\gamma_1,\gamma_2} = n^{1-v_{\gamma_1,\gamma_2}} = n^{1-v_1 - v_2 + v_{\gamma_1 \cap \gamma_2}} = n^{1-v_1} n^{1-v_2} = W_{\gamma_1} W_{\gamma_2}.
$$

If $v_{\gamma_1,\gamma_2} \geq 1$ and $(\gamma_1, \gamma_2) \notin \Gamma$, then either $\gamma_1 \notin \Gamma_\ell$ or $\gamma_2 \notin \Gamma_\ell$, and we have

$$
W_{\gamma_1,\gamma_2} \ll_{\ell} n^{1-v_{\gamma_1,\gamma_2}} \left( \frac{1}{m} + \frac{1}{n} \right)
$$

and

$$
W_{\gamma_1} W_{\gamma_2} \ll_{\ell} n^{2-v_{\gamma_1,\gamma_2}} \left( \frac{1}{m} + \frac{1}{n} \right) \ll_{\ell} n^{1-v_{\gamma_1,\gamma_2}} \left( \frac{1}{m} + \frac{1}{n} \right).
$$

Summarizing the above, for any $(\gamma_1, \gamma_2) \in \Pi^2_{\ell,p}/\Sigma_p$, we have

$$
W_{\gamma_1,\gamma_2} - W_{\gamma_1} W_{\gamma_2} \ll_{\ell} n^{1-v_{\gamma_1,\gamma_2}} \left( \frac{1}{m} + \frac{1}{n} \right). \hspace{1cm} (11)
$$

Finally, putting (11) and the trivial bound

$$
\sum_{(\gamma_1, \gamma_2) \in \Pi^2_{\ell,p}/\Sigma_p} 1 < v_{\gamma_{1,2}} \leq (2\ell)^{2\ell} \hspace{1cm} (12)
$$

into (8) yields

$$
\text{Var}(A_\ell(s), \Omega_p) \ll_{\ell} \frac{1}{p^2} \sum_{(\gamma_1, \gamma_2) \in \Pi^2_{\ell,p}/\Sigma_p} p^{v_{\gamma_1,\gamma_2}} n^{1-v_{\gamma_1,\gamma_2}} \left( \frac{1}{m} + \frac{1}{n} \right)
$$

$$
\ll_{\ell} \sum_{v=1}^{2\ell} g^{v-2} \left( \frac{1}{mn} + \frac{1}{n^2} \right) \sum_{(\gamma_1, \gamma_2) \in \Pi^2_{\ell,p}/\Sigma_p} 1
$$

$$
\ll_{\ell} \frac{1}{mn} + \frac{1}{n^2}.
$$

This completes the proof of Theorem 4.
2.4 Proof of Lemma 5

Now we give a detailed proof of Lemma 5.

First, as in [26], we define a closed path $\gamma$ to be reduced if either $\ell_\gamma = v_\gamma = 1$, or $v_\gamma \geq 2$ and the following two both hold:

(a) $\gamma(u) \neq \gamma(u + 1)$ for all $u \in [0..\ell_\gamma - 1]$;

(b) $\# I_a \geq 2$ for all $a \in V_\gamma$, where $I_a := \gamma^{-1}(a)$.

Now if $\gamma$ is not reduced, then at least one of the following happens:

Case 1: Consecutive elements
There exists $u \in [0..\ell_\gamma - 1]$ such that $\gamma(u) = \gamma(u + 1)$;

Case 2: Leaves
There exist $u \in [0..\ell_\gamma - 1]$ and $a \in V_\gamma$ such that $I_a = \{u\}$ and $\gamma(u - 1) = \gamma(u + 1)$.

Case 2b: Transition elements
There exist $u \in [0..\ell_\gamma - 1]$ and $a \in V_\gamma$ such that $I_a = \{u\}$ and $\gamma(u - 1) \neq \gamma(u + 1)$.

For each case, we can perform a reduction process as follows:

Case 1: Since $\gamma(u) = \gamma(u + 1)$, by the fact that each vector in $\mathfrak{B}$ is normal, we see that the $(u - 1)$-th inner product in the right side of (11) is 1. This means we can consider the closed path $\gamma' : [0..\ell_\gamma - 1] \rightarrow [1..p]$ defined by

$$
\gamma'(i) = \begin{cases} 
\gamma(i) & (0 \leq i \leq u - 1) \\
\gamma(i + 1) & (u \leq i \leq \ell_\gamma - 1)
\end{cases}.
$$

We have

$$
\ell_{\gamma'} = \ell_\gamma - 1, \quad v_{\gamma'} = v_\gamma, \quad \text{and} \quad W_\gamma = W_{\gamma'}.
$$

Case 2a: Denote $b := \gamma(u - 1) = \gamma(u + 1)$.

Expanding the inner products in the right side of (11), we get

$$
\omega_\gamma(s) = \sum_{t_0, t_1, \ldots, t_{\ell_\gamma - 1}} \prod_{i=0}^{\ell_\gamma - 1} s \circ \gamma(i)[t_i] \overline{s \circ \gamma(i + 1)[t_i]} = \sum_{t_0, t_1, \ldots, t_{\ell_\gamma - 1}} \prod_{z \in V_\gamma} \prod_{i \in I_z} s(z)[t_i] \overline{s(z)[t_{i-1}]},
$$

where the sum is taken over all $t_0, t_1, \cdots, t_{\ell_\gamma - 1} \in [1..n]$, and $s(z)[t_i]$ is the $t_i$-th coordinate of the vector $s(z)$.

Taking expectation over $\Omega(V_\gamma)$, we get

$$
W_\gamma = \frac{1}{(mn)^{v_\gamma}} \sum_{s(z) \in \mathfrak{B}} \sum_{z \in V_\gamma} \prod_{i \in I_z} s(z)[t_i] \overline{s(z)[t_{i-1}]}
$$

$$
= \frac{1}{(mn)^{v_\gamma}} \sum_{t_0, t_1, \ldots, t_{\ell_\gamma - 1}} \prod_{z \in V_\gamma} \left( \sum_{s(z) \in \mathfrak{B}} \prod_{i \in I_z} s(z)[t_i] \overline{s(z)[t_{i-1}]} \right).
$$

By assumption, we see that the factor in the bracket corresponding to $a \in V_\gamma$ is $\sum_{s(a) \in \mathfrak{B}} s(a)[t_a] \overline{s(a)[t_{a-1}]}$. 


Noting that each $\mathfrak{B}_j$ is orthonormal, we get

$$\sum_{s(a) \in \mathfrak{B}} s(a)[t_u] s(a)[t_{u-1}] = \sum_{j=1}^{m} \sum_{s(a) \in \mathfrak{B}_j} s(a)[t_u] s(a)[t_{u-1}] = m \delta_{i_u,t_{u-1}},$$

where $\delta_{i,j}$ is the Kronecker delta.

Hence (14) can be rewritten as

$$W_{\gamma} = \frac{m}{(mn)^{v_{\gamma}}} \sum_{t_{u-1}, t_{u-2}} \left[ \prod_{i \in I_z} \left( \sum_{s(z) \in \mathfrak{B}} s(z)[t_i] \overline{s(z)[t_{i-1}]} \right) \right] \times \left[ \sum_{s(b) \in \mathfrak{B}} \left( \prod_{i \in I_b \setminus \{u-1, u+1\}} s(b)[t_i] \overline{s(b)[t_{i-1}]} \right) s(b)[t_{u+1}] s(b)[t_{u-1}] s(b)[t_{u-2}] \right]. \tag{15}$$

The terms involving $t_{u-1}$ are given by $\sum_{t_{u-1}} s(b)[t_{u-1}] \overline{s(b)[t_{u-1}]}$, which is equal to 1 due to the normality of $s(b)$. Hence (15) can be further simplified as

$$W_{\gamma} = \frac{1}{n} \left\{ \frac{1}{(mn)^{v_{\gamma}}-1} \sum_{t_{u-1}, t_{u-2}} \left[ \prod_{i \in I_z} \left( \sum_{s(z) \in \mathfrak{B}} s(z)[t_i] \overline{s(z)[t_{i-1}]} \right) \right] \times \left[ \sum_{s(b) \in \mathfrak{B}} \left( \prod_{i \in I_b \setminus \{u-1, u+1\}} s(b)[t_i] \overline{s(b)[t_{i-1}]} \right) s(b)[t_{u+1}] s(b)[t_{u-1}] s(b)[t_{u-2}] \right].$$

After renaming the variables appropriately, we can see that the whole term inside the curly bracket above is simply $W_{\gamma'}$, where $\gamma'$ is the closed path defined by

$$\gamma'(i) = \begin{cases} \gamma(i) & (0 \leq i \leq u-2) \\ \gamma(i + 2) & (u-1 \leq i \leq \ell_{\gamma} - 2) \end{cases}.$$

Furthermore, we have

$$\ell_{\gamma'} = \ell_{\gamma} - 2, \quad v_{\gamma'} = v_{\gamma} - 1 \quad \text{and} \quad W_{\gamma} = \frac{1}{n} W_{\gamma'}.$$

**Case 2b:** Denote $b := \gamma(u-1)$ and $c := \gamma(u+1)$. All the arguments of Case 2a up to the step before (15) work for this case as well. However since $c \neq b$, (14) has to be rewritten as

$$W_{\gamma} = \frac{1}{n} \left\{ \frac{1}{(mn)^{v_{\gamma}}-1} \sum_{t_{u-1}, t_{u-2}} \left[ \prod_{i \in I_z} \left( \sum_{s(z) \in \mathfrak{B}} s(z)[t_i] \overline{s(z)[t_{i-1}]} \right) \right] \times \left[ \sum_{s(c) \in \mathfrak{B}} \left( \prod_{i \in I_c \setminus \{u+1\}} s(c)[t_i] \overline{s(c)[t_{i-1}]} \right) s(c)[t_{u+1}] s(c)[t_{u-1}] s(c)[t_{u-2}] \right].$$

After renaming the variables appropriately, we can see that the whole term inside the curly bracket
above is simply $W_{\gamma'}$ where $\gamma'$ is the closed path defined by
\[
\gamma'(i) = \begin{cases} 
\gamma(i) & (0 \leq i \leq u - 1) \\
\gamma(i + 1) & (u \leq i \leq \ell_{\gamma} - 1) 
\end{cases}
\].

Furthermore, we have
\[
\ell_{\gamma'} = \ell_{\gamma} - 1, \quad v_{\gamma'} = v_{\gamma} - 1 \quad \text{and} \quad W_{\gamma} = \frac{1}{n} W_{\gamma'}.
\]

Finally, given a general non-reduced closed path $\gamma$, we can consecutively apply the above three kinds of reductions finitely many times until one gets a reduced path. Denote $\widetilde{\gamma}$ to be this resulting path, and assume we apply $u, v$ and $w$ reductions of Cases 1, 2a and 2b respectively. From the above calculations we get
\[
\ell_{\widetilde{\gamma}} = \ell_{\gamma} - u - 2v - w, \quad v_{\widetilde{\gamma}} = v_{\gamma} - v - w \quad \text{and} \quad W_{\gamma} = \frac{1}{n^{v+w}} W_{\widetilde{\gamma}}.
\] (16)

Now we look at the case $\gamma$ is reduced.

First, if $\ell_{\gamma} = v_{\gamma} = 1$, $\gamma$ is a single point with a single loop. Then in this case we clearly have $\omega_{\gamma}(s) = 1$ and hence $W_{\gamma} = 1$.

Now we consider the case $v_{\gamma} \geq 2$. As we have, for $v_1, v_2 \in B$,
\[
\langle v_1, v_2 \rangle = \begin{cases} 
1 & (v_1 = v_2) \\
O(n^{-\frac{1}{2}}) & (v_1 \neq v_2)
\end{cases}
\],

from the expansion it suffices to check the minimum possible number of $i \in [0..\ell_{\gamma} - 1]$ such that $s \circ \gamma(i) \neq s \circ \gamma(i + 1)$ for a given $s \in \Omega(V_{\gamma})$. We call such an $i$ a transition with respect to $s \circ \gamma$.

Define $N_{s,\gamma} := \#\{s(z) : z \in V_{\gamma}\}$. This is a random variable on the probability space $\Omega(V_{\gamma})$ taking values in $[1..v_{\gamma}]$.

**Case I.** $N_{s,\gamma} = 1$. Then there are no transitions, and we have $\omega_{\gamma}(s) = 1$.

**Case II.** $N_{s,\gamma} \geq 2$. Then there are clearly at least $N_{s,\gamma}$ transitions.

**Case II-a.** All nonempty preimages of $s$ in $V_{\gamma}$ are of size at least 2. Then it is possible that all the preimages of $s \circ \gamma$ appear to be a subset of $[0..\ell_{\gamma} - 1]$ with totally consecutive elements (indices are treated modulo $\ell$—we say such preimage is consecutive for short). In this case there are precisely $N_{s,\gamma}$ transitions, and we have
\[
\omega_{\gamma}(s) = O\left(n^{-\frac{N_{s,\gamma}}{2}}\right).
\]

**Case II-b.** There exists at least one preimage of $s$ in $V_{\gamma}$ of size 1. From the definition of reduced, the single point in this preimage should be traversed at least twice by $\gamma$ and cannot be consecutive. Due to its single nature, each inner product containing this preimage is $O(n^{-\frac{1}{2}})$. In the worst case, for those preimages of $s$ in $V_{\gamma}$ of size at least 2, the corresponding preimages of $s \circ \gamma$ appear to be consecutive, and the remaining consecutive part corresponds to the union of all the singleton preimages. If $c_{s,\gamma}$ denotes the number of singleton preimages of $s$ in $V_{\gamma}$, then this remaining part consists of at least $2c_{s,\gamma}$ inner products, so that we have
\[
\omega_{\gamma}(s) = O\left(n^{-\frac{N_{s,\gamma} - c_{s,\gamma} + 2c_{s,\gamma}}{2}}\right) = O\left(n^{-\frac{N_{s,\gamma} + c_{s,\gamma}}{2}}\right).
\]
Note that the quantity $c_{s,\gamma}$ satisfies the inequality

$$v_{\gamma} - c_{s,\gamma} \geq 2(N_{s,\gamma} - c_{s,\gamma}),$$

which implies

$$c_{s,\gamma} \geq 2N_{s,\gamma} - v_{\gamma}.$$ 

Hence **Case II-a** may happen only if $2 \leq N_{s,\gamma} \leq \frac{v_{\gamma}}{2}$. For $\frac{v_{\gamma}}{2} < N_{s,\gamma} \leq v_{\gamma}$, we must be in **Case II-b** and we have

$$\omega_{\gamma}(s) = O\left(n^{-\frac{3N_{s,\gamma} - v_{s,\gamma}}{2}}\right).$$

Combining all above cases, we conclude that

$$W_{\gamma} = \frac{1}{(mn)^{v_{\gamma}}} \sum_{i=1}^{v_{\gamma}} \sum_{s \in \Omega(V_{\gamma})} \omega_{\gamma}(s) \leq v_{\gamma} \left( \frac{mn}{(mn)^{v_{\gamma}}} + \sum_{i=2}^{\frac{v_{\gamma}}{2}} (mn)^{i} n^{-\frac{i}{2}} + \sum_{i > \frac{v_{\gamma}}{2}} (mn)^{i} n^{-\frac{2i - v_{\gamma}}{2}} \right)$$

$$\leq v_{\gamma} \left( \frac{mn}{(mn)^{v_{\gamma}}} + \sum_{i=2}^{\frac{v_{\gamma}}{2}} (m\sqrt{n})^{i} n^{-\frac{v_{\gamma}}{2}} + \sum_{i > \frac{v_{\gamma}}{2}} (m\sqrt{n})^{i} \left( \frac{m}{\sqrt{n}} \right)^{v_{\gamma}} \right)$$

$$\leq v_{\gamma} (mn)^{1-v_{\gamma}} + m^{-\frac{v_{\gamma}}{2}} n^{-\frac{3v_{\gamma}}{2}} + n^{-v_{\gamma}}$$

$$\ll v_{\gamma} n^{1-v_{\gamma}} \left( \frac{1}{m} + \frac{1}{n} \right)$$

where we use the assumption $m \geq \sqrt{n}$ in the third and fifth inequalities.

Now denote $\Gamma_{\ell}$ to be the set of all closed paths $\gamma \in \Pi_{p}/\Sigma_p$ such that its corresponding reduced path $\tilde{\gamma}$ is a single loop on a single point. Then we have $\ell_{\tilde{\gamma}} = v_{\tilde{\gamma}} = W_{\tilde{\gamma}} = 1$, and the last two equations of (**16**) gives $W_{\gamma} = n^{1-v_{\gamma}}$.

If $\gamma \notin \Gamma_{\ell}$, then applying (**17**) to $\gamma$ and combining with the last two equations of (**16**) yields the same result as (**17**). This completes the proof of Lemma 5.

3 Proof of Theorem 2

Let the notations be the same as in Section 2. In order to choose $p$ distinct elements from $\mathfrak{B}$, we introduce the probability space $\Omega_{p,1}$, which is the subspace of $\Omega_{p}$ consisting only of those maps $s$ that are injective, endowed with uniform probability. For each such map $s$, we construct the corresponding $\Phi(s)$ and $\mathcal{G}(s)$ as defined in (2) and (3) respectively. Furthermore, define

$$\mathcal{M}(s) := \sqrt{\frac{n}{p}} (\mathcal{G}(s) - I_p).$$


Note that $\mathcal{M}(s)$ is a $p \times p$ matrix whose $(j,k)$-th entries are given by

$$
\sqrt{\frac{n}{p}} \left( \langle s(j), s(k) \rangle - \delta_{j,k} \right).
$$

In particular if $j = k$, then since all the vectors in $\mathcal{B}$ are normal, this quantity is zero.

Then the $\ell$-th moment of the empirical spectral distribution of $\mathcal{M}(s)$ is given by

$$
A_{\ell,I}(s) = \frac{1}{p} \text{Tr} \left( \mathcal{M}(s)^\ell \right).
$$

In order to prove Theorem 2, it suffices to prove the following two statements (see [4]):

(i) $E(A_{\ell,I}(s), \Omega_{p,I}) \to A_{\ell,\text{SC}}$ as $n \to \infty$, where $A_{\ell,\text{SC}}$ is the $\ell$-th moment of the Wigner’s semicircle law given explicitly by

$$
A_{\ell,\text{SC}} = \begin{cases} 
0 & (\ell \text{ is odd}) \\
\frac{2}{\pi} \left( \frac{\ell}{\ell/2} \right) & (\ell \text{ is even}) 
\end{cases}.
$$

(ii) $\text{Var}(A_{\ell,I}(s), \Omega_{p,I}) \to 0$ as $n \to \infty$.

More precisely, we have the following two estimates:

**Theorem 6.** For any fixed positive integer $\ell$,

$$
E(A_{\ell,I}(s), \Omega_{p,I}) = \begin{cases} 
O_{\ell} \left( \frac{1}{\sqrt{p}} + \sqrt{\frac{p}{n}} \right) & (\ell \text{ is odd}) \\
O_{\ell} \left( \frac{2}{\pi} \left( \frac{\ell}{\ell/2} \right) + \frac{1}{m} + \frac{p}{n} \right) & (\ell \text{ is even}) 
\end{cases}.
$$

**Theorem 7.** For any fixed positive integer $\ell$,

$$
\text{Var}(A_{\ell,I}(s), \Omega_{p,I}) = O_{\ell} \left( \frac{1}{p^2} + \frac{1}{pm} \right).
$$

The rest of this section will be devoted to the proofs of these two theorems.

### 3.1 Problem Set-up

First, noting that the diagonal entries of $\mathcal{M}(s)$ are all 0, to compute $A_{\ell,I}(s)$, we only need to consider those closed paths $\gamma \in \Pi_{\ell,p}$ such that $\gamma(u) \neq \gamma(u + 1)$ for any $u$. For this purpose we introduce the subset

$$
\Pi'_{\ell,p} := \{ \gamma \in \Pi_{\ell,p} : \gamma(u) \neq \gamma(u + 1) \quad \forall u \in [0..\ell - 1] \}.
$$

Then we have

$$
A_{\ell,I}(s) = \frac{1}{p} \left( \frac{n}{p} \right) \frac{\ell}{2} \sum_{\gamma \in \Pi'_{\ell,p}} \omega_\gamma(s).
$$

After taking expectation over $\Omega_{p,I}$ in both sides and adopting further ideas similar to [10] Section III-A, we obtain

$$
E(A_{\ell,I}(s), \Omega_{p,I}) = \frac{1}{p} \left( \frac{n}{p} \right) \frac{\ell}{2} \sum_{\gamma \in \Pi'_{\ell,p} / \Sigma_p} \frac{p!}{(p - v_\gamma)!} E(\omega_\gamma(s), \Omega_I(V_\gamma)),
$$

where $\Omega_I(V_\gamma) := \{ s \in \Omega(V_\gamma) : s \text{ is injective} \}$ with uniform probability.
3.2 Proof of Theorem 6

For any $\gamma \in \Pi_{\ell, p}/\Sigma_p$ and $s \in \Omega_I(V_\gamma)$, $s \circ \gamma(j) \neq s \circ \gamma(j + 1)$ $\forall j$, so from (1), we have

$$E(\omega_\gamma(s), \Omega_I(V_\gamma)) = O(n^{-\frac{\ell}{2}}).$$

(19)

On the other hand, we also have the following estimate, whose proof is quite technical and will be postponed to Section 3.3.

Lemma 8. We have

$$E(\omega_\gamma(s), \Omega_I(V_\gamma)) = W_\gamma + O(\ell \left( \frac{n^{1-v_\gamma}}{m} \right)),
$$

where $W_\gamma$ is defined as in (6).

Define

$$\beta_\gamma := \frac{1}{p} \left( \frac{n}{p} \right)^{\frac{\ell}{2}} \frac{p!}{(p-v_\gamma)!} E(\omega_\gamma(s), \Omega_I(V_\gamma)),
$$

hence we have

$$E(A_{\ell, I}(s), \Omega_{p, I}) = \sum_{\gamma \in \Pi_{\ell, p}/\Sigma_p} \beta_\gamma.$$

From (19), Lemmas 5 and 8 we can summarize the estimates of $\beta_\gamma$ as follows:

(a). $\beta_\gamma \ll \frac{1}{\sqrt{p}}$ : $v_\gamma < 1 + \frac{\ell}{2},$

(b). $\beta_\gamma \ll \sqrt{n}$ : $v_\gamma > 1 + \frac{\ell}{2},$

(c). $\beta_\gamma \ll \frac{1}{m} + \frac{1}{n}$ : $v_\gamma = 1 + \frac{\ell}{2}, \gamma \notin \Gamma_\ell,$

(d). $\beta_\gamma = 1 + O(\ell \left( \frac{1}{p} + \frac{1}{m} \right))$ : $v_\gamma = 1 + \frac{\ell}{2}, \gamma \in \Gamma_\ell.$

Note that (c) and (d) may appear only when $\ell$ is even, and in this case the square root symbols in (a) and (b) can be dropped too. Using the identity (see [4, Lemma 2.4])

$$\sum_{\gamma \in \Gamma_\ell \atop v_\gamma = 1 + \frac{\ell}{2}} 1 = \frac{2}{\ell + 2} \left( \frac{\ell}{2} \right),
$$

we obtain the desired estimates on $E(A_{\ell, I}(s), \Omega_{p, I})$. This completes the proof of Theorem 6. \qed

3.3 Proof of Theorem 7

Now we proceed to prove Theorem 7.

First, we expand the quantity $\text{Var}(A_{\ell, I}(s), \Omega_{p, I})$ as

$$\text{Var}(A_{\ell, I}(s), \Omega_{p, I}) = E(|A_{\ell, I}(s)|^2, \Omega_{p, I}) - |E(A_{\ell, I}(s), \Omega_{p, I})|^2.$$

Similar to the first main step in Section 2.3, we can write

$$\text{Var}(A_{\ell, I}(s), \Omega_{p, I}) = \sum_{(\gamma_1, \gamma_2) \in \Pi_{\ell, p}/\Sigma_p} \frac{1}{p^2} \left( \frac{n}{p} \right)^{\ell} \frac{p!}{(p-v_{\gamma_1, \gamma_2})!} \beta_{\gamma_1, \gamma_2},
$$

(20)
where
\[ \beta_{\gamma_1, \gamma_2} := E \left( \omega_{\gamma_1}(s) \omega_{\gamma_2}(s), \Omega_f(V_{\gamma_1, \gamma_2}) \right) - E \left( \omega_{\gamma_1}(s), \Omega_f(V_{\gamma_1}) \right) E \left( \omega_{\gamma_2}(s), \Omega_f(V_{\gamma_2}) \right). \]

### 3.4 Study of \( \beta_{\gamma_1, \gamma_2} \)

First, by the condition in (1), we easily obtain
\[ |\beta_{\gamma_1, \gamma_2}| \leq 2n^{-\ell}. \tag{21} \]

Next, we have the following estimation:

**Lemma 9.**
\[ \beta_{\gamma_1, \gamma_2} \ll \ell n^{1-v_{\gamma_1, \gamma_2}} \left( \frac{1}{m} + \frac{1}{n} \right). \tag{22} \]

To prove this, we need the following technical lemma, whose proof is postponed to Section 3.5:

**Lemma 10.** Let \( v_{\gamma_1 \cap \gamma_2} \geq 1 \). Then
\[ E \left( \omega_{\gamma_1}(s) \omega_{\gamma_2}(s), \Omega_f(V_{\gamma_1, \gamma_2}) \right) = W_{\gamma_1, \gamma_2} + O \ell \left( \frac{n^{1-v_{\gamma_1, \gamma_2}}}{m} \right), \]

where \( W_{\gamma_1, \gamma_2} \) is defined in (9).

If \( v_{\gamma_1 \cap \gamma_2} = 0 \), then the same statement holds with an extra factor of \( n \) in the numerator of the error term.

**Proof of Lemma 9.** If \( v_{\gamma_1 \cap \gamma_2} \geq 1 \), applying Lemmas 8 and Lemma 10 directly to the terms \( E(\omega_{\gamma_i}(s), \Omega_f(V_{\gamma_i})) \) \( (i = 1, 2) \) and \( E \left( \omega_{\gamma_1}(s) \omega_{\gamma_2}(s), \Omega_f(V_{\gamma_1}) \right) \) respectively, then using Lemma 5 and Equation (11) in Section 2, also observing that \( v_{\gamma_1} + v_{\gamma_2} = v_{\gamma_1, \gamma_2} + v_{\gamma_1 \cap \gamma_2} \geq v_{\gamma_1, \gamma_2} + 1 \), we obtain the desired result by a straightforward computation.

Now assume \( v_{\gamma_1 \cap \gamma_2} = 0 \). We remark that if we use the above approach, we can only obtain
\[ \beta_{\gamma_1, \gamma_2} \ll \ell \frac{n^{2-v_{\gamma_1, \gamma_2}}}{m}, \]
which falls short of our expectation (22). So we adopt a different method.

Denote
\[ N_i = \# \Omega_f(V_{\gamma_i}) = \frac{(mn)!}{(mn - v_{\gamma_i})!}, \quad i = 1, 2, \]
and
\[ N_0 = \# \Omega_f(V_{\gamma_1, \gamma_2}) = \frac{(mn)!}{(mn - v_{\gamma_1, \gamma_2})!}. \]

By using its definition, we can rewrite \( \beta_{\gamma_1, \gamma_2} \) as
\[ \beta_{\gamma_1, \gamma_2} = A - B, \]
where

\[
A = \left(1 - \frac{N_0}{N_1 N_2}\right) E \left(\omega_{\gamma_1}(s)\omega_{\gamma_2}(s), \Omega_I(V_{\gamma_1, \gamma_2})\right)
\]

\[
B = \frac{1}{N_1 N_2} \left(\sum_{s \in \Omega_I(V_{\gamma_1, \gamma_2})} \omega_{\gamma_1}(s)\omega_{\gamma_2}(s) - \sum_{s \in \Omega_I(V_{\gamma_1, \gamma_2})} \omega_{\gamma_1}(s)\omega_{\gamma_2}(s)\right).
\]

As for the first term \(A\), since \(0 \leq v_{\gamma_1, \gamma_2} = v_{\gamma_1} + v_{\gamma_2} \leq 2\ell\), we have \(1 - \frac{N_0}{N_1 N_2} \ll \ell = \frac{1}{mn}\) By Lemma 10 and noting that

\[
W_{\gamma_1, \gamma_2} = W_{\gamma_1} W_{\gamma_2} \ll \ell^{n_{1-v_{\gamma_1}} n_{1-v_{\gamma_2}}} = n^{2-v_{\gamma_1, \gamma_2}},
\]

we can obtain easily

\[
A \ll \ell \frac{1}{mn} \left(n^{2-v_{\gamma_1, \gamma_2}} + \frac{n^{2-v_{\gamma_1, \gamma_2}}}{m}\right) \ll \ell \frac{n^{1-v_{\gamma_1, \gamma_2}}}{m}.
\]

As for \(B\), first, we can rewrite it as

\[
B = \frac{1}{N_1 N_2} \sum_{s \in \Omega_I(V_{\gamma_1}) \times \Omega_I(V_{\gamma_2})} \omega_{\gamma_1}(s)\omega_{\gamma_2}(s).
\]

Here the subscript means that we sum over all \(s \in \Omega_I(V_{\gamma_1}) \times \Omega_I(V_{\gamma_2})\) such that there are \(a \in V_{\gamma_1}\) and \(b \in V_{\gamma_2}\) with \(s(a) = s(b)\).

Let \(Q = \{(a, b) : a \in V_{\gamma_1}, b \in V_{\gamma_2}\}\). For any non-empty subset \(U \subset Q\), we can define corresponding new maps \(\gamma_{1U}\) and \(\gamma_{2U}\) by identifying the vertices corresponding to \(a_k\) and \(b_k\) whenever \((a_k, b_k) \in U\). For these new maps, clearly we have

\[
v_{\gamma_{1U}, \gamma_{2U}} \leq v_{\gamma_1, \gamma_2} - 1.
\]

Moreover, since \(\gamma_{1U}\) and \(\gamma_{2U}\) share the new vertex formed by identifying \(a_k\) with \(b_k\), we also have \(v_{\gamma_{1U}, \gamma_{2U}} \geq 1\). Hence we can apply Lemma 10 to obtain

\[
\left|\sum_{s \in \Omega_I(V_{\gamma_{1U}, \gamma_{2U}})} \omega_{\gamma_{1U}}(s)\omega_{\gamma_{2U}}(s)\right| \ll \ell^{(mn)^{v_{\gamma_{1U}, \gamma_{2U}}}} \left|E \left(\omega_{\gamma_{1U}}(s)\omega_{\gamma_{2U}}(s), \Omega_I(V_{\gamma_{1U}, \gamma_{2U}})\right)\right| \ll \ell \ m^{v_{\gamma_{1U}, \gamma_{2U}}-1} n.
\]

Then by the inclusion-exclusion principle, we conclude that

\[
\left|\sum_{s \in \Omega_I(V_{\gamma_1}) \times \Omega_I(V_{\gamma_2}) \setminus \Omega_I(V_{\gamma_{1U}, \gamma_{2U}})} \omega_{\gamma_1}(s)\omega_{\gamma_2}(s)\right| \leq \sum_U \left|\sum_{s \in \Omega_I(V_{\gamma_{1U}, \gamma_{2U}})} \omega_{\gamma_{1U}}(s)\omega_{\gamma_{2U}}(s)\right| \ll \ell \ m^{v_{\gamma_{1U}, \gamma_{2U}}-1} n.
\]

From this we obtain

\[
B \ll \ell \frac{n^{1-v_{\gamma_1, \gamma_2}}}{m}.
\]

Combining the estimates of \(A\) and \(B\) yields the desired result for \(\beta_{\gamma_1, \gamma_2}\). This completes the proof of Lemma 9. \(\square\)
Now define
\[ \alpha_{\gamma_1, \gamma_2} = \frac{1}{p^2} \left( \frac{n}{p} \right) \frac{p!}{(p - v_{\gamma_1, \gamma_2})!} \beta_{\gamma_1, \gamma_2}. \]

From (21) and Lemma 9 we summarize the estimates of \( \alpha_{\gamma_1, \gamma_2} \) as follows:
\begin{align*}
\alpha_{\gamma_1, \gamma_2} &\ll \ell \, p^{v_{\gamma_1, \gamma_2} - \ell - 2}, \\
\alpha_{\gamma_1, \gamma_2} &\ll \ell \, \left( \frac{p}{n} \right)^{v_{\gamma_1, \gamma_2} - \ell - 1} \left( \frac{1}{pm} + \frac{1}{pm} \right).
\end{align*}

We split \( \text{Var}(A_{\ell, I}(s), \Omega_{p, I}) \) in (20) into two terms
\[ \text{Var}(A_{\ell, I}(s), \Omega_{p, I}) = \sum_{(\gamma_1, \gamma_2) \in \Pi_{p}^{2}/\Sigma_{p}} \alpha_{\gamma_1, \gamma_2} + \sum_{(\gamma_1, \gamma_2) \in \Pi_{p}^{2}/\Sigma_{p}} \alpha_{\gamma_1, \gamma_2}. \]

For the first term, using (23) and the trivial bound (12) we easily obtain
\[ \sum_{(\gamma_1, \gamma_2) \in \Pi_{p}^{2}/\Sigma_{p}, v_{\gamma_1, \gamma_2} \leq \ell} \alpha_{\gamma_1, \gamma_2} \ll \ell \frac{1}{p^2}. \]

For the second term of (25), using (24) we can also obtain
\[ \sum_{(\gamma_1, \gamma_2) \in \Pi_{p}^{2}/\Sigma_{p}, v_{\gamma_1, \gamma_2} \geq \ell + 1} \alpha_{\gamma_1, \gamma_2} \ll \ell \frac{1}{pm} + \frac{1}{pm}. \]

Putting (26) and (27) into (25) gives the desired result for \( \text{Var}(A_{\ell, I}(s), \Omega_{p, I}) \). This completes the proof of Theorem 7.

3.5 Proof of Lemmas 8 and 10

Now we prove Lemmas 8 and 10.

**Proof of Lemma 8.** First, define
\[ \tilde{\mathbb{E}}(\omega_{\gamma}(s), \Omega_{I}(V_{\gamma})) := \frac{\sum_{s \in \Omega_{I}(V_{\gamma})} \omega_{\gamma}(s)}{(mn)^{v_{\gamma}}}. \]

Noting that
\[ \mathbb{E}(\omega_{\gamma}(s), \Omega_{I}(V_{\gamma})) = \tilde{\mathbb{E}}(\omega_{\gamma}(s), \Omega_{I}(V_{\gamma})) \frac{(mn)^{v_{\gamma}}}{mn(mn - 1)(mn - 2) \cdots (mn - v_{\gamma} + 1)} = \tilde{\mathbb{E}}(\omega_{\gamma}(s), \Omega_{I}(V_{\gamma})) \left( 1 + O_{\ell} \left( \frac{1}{mn} \right) \right), \]

we prove Lemma 8 it suffices to study \( \tilde{\mathbb{E}}(\omega_{\gamma}(s), \Omega_{I}(V_{\gamma})) \). We write
\[ \tilde{\mathbb{E}}(\omega_{\gamma}(s), \Omega_{I}(V_{\gamma})) = \frac{\sum_{s \in \Omega(V_{\gamma})} \omega_{\gamma}(s) - \sum_{s \in \Omega(V_{\gamma}) \setminus \Omega_{I}(V_{\gamma})} \omega_{\gamma}(s)}{(mn)^{v_{\gamma}}}. \]

The first term is precisely \( W_{\gamma} \) defined in (6). As for the second term, the condition \( s \in \Omega(V_{\gamma}) \setminus \Omega_{I}(V_{\gamma}) \)
is equivalent to \( s \) being not injective, that is, there exist \( a \neq b \in V_\gamma \) such that \( s(a) = s(b) \). Denote by \( \Omega_{(a,b)} \) the set of all \( s \in \Omega(V_\gamma) \) such that \( s(a) = s(b) \). We may order the set \( v_\gamma \) as \( v_\gamma = \{ z_i : 1 \leq i \leq v_\gamma \} \) and define \( P = \{(z_i, z_j) : 1 \leq i < j \leq v_\gamma \} \). Using

\[
\Omega(V_\gamma) \setminus \Omega_I(V_\gamma) = \bigcup_{(a,b) \in P} \Omega_{(a,b)},
\]

and the inclusion-exclusion principle, we have

\[
\left| \sum_{s \in \Omega(V_\gamma) \setminus \Omega_I(V_\gamma)} \omega_\gamma(s) \right| \leq |P| \sum_{t=1} |(a_1, b_1), \ldots, (a_t, b_t) \in P| \sum_{s \in \cap_{m=1}^{t} \Omega_{(a_m, b_m)}} \omega_\gamma(s).
\]

A little thought reveals that the inner summand \( \sum_{s \in \cap_{m=1}^{t} \Omega_{(a_m, b_m)}} \omega_\gamma(s) \) corresponds to the quantity \( W_{\gamma T} \), where the closed path \( \gamma T \) is obtained from \( \gamma \) by identifying the vertices \( a \) and \( b \) for all pairs \((a, b)\) inside the set \( T = \{(a_m, b_m) : 1 \leq m \leq t \} \). More precisely, let \( v_{\gamma T} \) be the number of vertices of \( \gamma T \), then

\[
\frac{1}{(mn)^v_{\gamma T}} \left| \sum_{s \in \cap_{m=1}^{t} \Omega_{(a_m, b_m)}} \omega_\gamma(s) \right| = W_{\gamma T}.
\]

Obviously \( v_{\gamma T} \leq v_\gamma - 1 \). Applying Lemma 5 on \( W_{\gamma T} \) directly, we obtain

\[
\left| \sum_{s \in \Omega(V_\gamma) \setminus \Omega_I(V_\gamma)} \omega_\gamma(s) \right| \ll \ell m^{\nu_\gamma - 1} n.
\]

Inserting this into (29), we obtain

\[
\tilde{E}(\omega_\gamma(s), \Omega_I(V_\gamma)) = W_\gamma + O_\ell \left( \frac{n^{1-\nu}}{m} \right).
\]

Noting the relation (28) and the estimate of \( W_\gamma \) in Lemma 6 we obtain the desired estimate on \( E(\omega_\gamma(s), \Omega_I(V_\gamma)) \). This completes the proof of Lemma 8. \( \square \)

**Proof of Lemma 7**. Let \( v_{\gamma_1 \gamma_2} \geq 1 \). We can identify the pair \( (\gamma_1, \gamma_2) \) with the closed path \( \gamma_{1,2} \) as defined in (10). Then the desired statement is simply Lemma 8 applied to \( \gamma_{1,2} \).

Now consider the case \( v_{\gamma_1 \gamma_2} = 0 \). In this case when we apply the proof of Lemma 8 we should do it on the pair \( (\gamma_1, \gamma_2) \), and the resulting pair is \( (\gamma_{1T}, \gamma_{2T}) \). If \( T \) contains at least one pair such that one vertex is from \( \gamma_1 \) and another one from \( \gamma_2 \), then the resulting pair \( (\gamma_{1T}, \gamma_{2T}) \) share a common vertex and therefore the full argument of Lemma 8 still applies. Otherwise \( (\gamma_{1T}, \gamma_{2T}) \) is still totally disjoint and \( W_{\gamma_{1T} \gamma_{2T}} = W_{\gamma_{1T}} W_{\gamma_{2T}} \ll \ell n^{1-\nu_{\gamma_{1T}}} n^{1-\nu_{\gamma_{2T}}} \ll \ell n^{2-\nu_{\gamma_{1T}}} n^{2-\nu_{\gamma_{2T}}} \). Therefore the desired error bound should have an extra factor of \( n \) in the numerator.

Combining both completes the proof of Lemma 10. \( \square \)

**Acknowledgements**

The research of M. Xiong was supported by RGC grant number 16303615 from Hong Kong.
References

[1] B. Babadi, S. S. Ghassemzadeh and V. Tarokh, “Group randomness properties of pseudo-noise and Gold sequences,” Proc. 12th Can. Workshop Inform. Theory (CWIT), pp. 42–46, 2011.

[2] B. Babadi and V. Tarokh, “Spectral distribution of random matrices from binary linear block codes,” IEEE Trans. Inform. Theory 57 (2011), no. 6, 3955–3962.

[3] B. Babadi and V. Tarokh, “Spectral distribution of product of pseudorandom matrices formed from binary block codes,” IEEE Trans. Inform. Theory 59 (2013), no. 2, 970–978.

[4] Z. Bai, J. W. Silverstein, Spectral Analysis of Large Dimensional Random Matrices, 2nd ed. New York, NY, USA: Springer Series in Statistics, 2010.

[5] S. Bandyopadhyay, P. O. Boykin, V. Roychowdhury, F. Vatan, “A New Proof for the Existence of Mutually Unbiased Bases,” Algorithmica 34 (2002), no. 4, 512–528.

[6] H. Bechmann-Pasquinucci, W. Tittel, “Quantum cryptography using larger alphabets,” Phys. Rev. A 61 (2000), 062308.

[7] C. H. Bennett, G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” Theoret. Comput. Sci. 560 (2014), 7–11.

[8] D. Bruss, “Optimal eavesdropping in quantum cryptography with six states,” Phys. Rev. Lett. 84 (1998), 3018–3021.

[9] X. Cao, W. Chou, More constructions of approximately mutually unbiased bases, Bull. Aust. Math. Soc. 93 (2016), no. 2, 211–222.

[10] C. H. Chan, E. Kung and M. Xiong, “Random Matrices from Linear Codes and Wigner’s Semicircle Law,” IEEE Trans. Inf. Theory 65 (2019), no. 10, 6001–6009.

[11] C. H. Chan and M. Xiong, “Random Matrices from Linear Codes and Wigner’s Semicircle Law II,” The 9th International Workshop on Signal Design and its Applications (IWSDA), 2019.

[12] P. Delsarte, J. M. Goethals, J. J. Seidel, “Bounds for Systems of Lines, and Jacobi Polynomials,” Geometry and Combinatorics (1991), 193–207.

[13] S. G. Hoggar, “t-Designs in Projective Spaces,” Europ. J. Combinatorics 3 (1982), 233–254.

[14] I. D. Ivonovic, “Geometrical description of quantal state determination,” J. Phys. A 14 (1981), no. 12, 3241–3245.

[15] G. A. Kabatiansky, V. I. Levenshtein, “On Bounds for Packings on a Sphere and in Space,” Probl. Peredachi Inf. 14 (1978), no. 1, 3–25.

[16] A. Klappenecker, M. Rötteler, “Constructions of Mutually Unbiased Bases,” International Conference on Finite Fields and Applications, 137–144, 2003.

[17] M. L. Mehta, Random Matrices (Pure and Applied Mathematics), vol. 142, 3rd ed. San Francisco, CA, USA: Academic, 2004.
[18] S. Pafka, M. Potters, and I. Kondor, “Exponential weighting and random-matrix-theory-based filtering of financial covariance matrices for portfolio optimization.” (2004) Available at: http://arxiv.org/abs/cond-mat/0402573

[19] J. Schwinger, “Unitary Operator Bases,” Proc. Nat. Acad. Sci. U.S.A. 46 (196), 570–579.

[20] I. E. Shparlinski, A. Winterhof, Constructions of approximately mutually unbiased bases, LATIN 2006: Theoretical informatics, 793–799, Lecture Notes in Comput. Sci., 3887, Springer, Berlin, 2006.

[21] A. M. Tulino and S. Verdú, “Random matrix theory and wireless communications,” Commun. Inf. Theory 1 (2004), no. 1, 1–182.

[22] G. Wang, M. Niu, F. Fu, Two new constructions of approximately mutually unbiased bases, Int. J. Quantum Inf. 16 (2018), no. 4, 1850038, 10 pp.

[23] E. P. Wigner, “Characteristic vectors of bordered matrices with infinite dimensions,” Ann. of Math. 62 (1955), no. 2, 548–564.

[24] J. Wishart, “The generalised product moment distribution in samples from a normal multivariate population,” Biometrika 20A (1928), no. 1/2, 32–52.

[25] W. K. Wootters, B. D. Fields, “Optimal state-determination by mutually unbiased measurements,” Ann. Physics 191 (1989), no. 2, 363–381.

[26] J. Xia and M. Xiong, “On a Question of Babadi and Tarokh,” IEEE Trans. Inform. Theory 60 (2014), no. 11, 7355–7367.