RANDOM MATRICES AND FREE PROBABILITY

JACOB CAMPBELL

These are notes for a graduate topics course at the University of Virginia in Spring 2026. The main aim of the course is to learn about recent developments in strong convergence and its applications. See the table of contents for more details.

Contents

1. GUE and genus expansion

1.1. Moments of gaussians.

Recall the following distribution:

Definition 1.1. A random variable X has a standard *gaussian* distribution if it has density

$$f_X(x) = \frac{1}{\sqrt{2\pi}} e^{-\frac{x^2}{2}}$$

for $x \in \mathbb{R}$. This is the case of mean 0 and variance 1.

Actually, we care about all the moments:

Proposition 1.2. *If X is standard gaussian, then*

$$\mathbb{E}(X^{2k}) = (2k-1)!! \text{ and } \mathbb{E}(X^{2k-1}) = 0$$

for $k \geq 1$.

Proof. Exercise. □

Definition 1.3 (Set partitions)**.** A *partition* of the set $[n] := \{1, \ldots, n\}$ is a collection $\{V_1, \ldots, V_l\}$ of *blocks*, which are disjoint subsets of $[n]$, with $[n] = \bigcup_{i=1}^{l} V_i$. The set of partitions of $[n]$ will be denoted by $P(n)$. A *pair* partition is a partition whose blocks all have size 2; the set of pair partitions of $[n]$ will be denoted by $P_2(n)$. Note that $P_2(n) = \emptyset$ when n is odd.

Let $\phi : P(n) \to S_n$ be the map which turns blocks into cycles, with the usual order inherited from $[n]$. This is obviously injective, and the range of $P_2(n)$ is the set of permutations in S_n with order 2 and no fixed points. We will refer interchangeably to $P_2(n)$ and its image in S_n; notice that in the case of $P_2(n)$, the arbitrary choice of order in the definition of ϕ does not actually matter.

Example 1.4.

$$P_2(4) = \{\{\{1,2\},\{3,4\}\},\{\{1,3\},\{2,4\}\},\{\{1,4\},\{2,3\}\}\}$$

Proposition 1.5. *We have $|P_2(2k)| = (2k-1)!!$ for $k \geq 1$.*

Idea of proof. When you choose what gets paired with 1, you have $2k-1$ choices. Next, you have $2k-3$ choices. This goes on to give you $(2k-1)!!$ choices in total. Exercise: formalize this idea. □

Theorem 1.6 (Wick formula)**.** *Let $X_1, \ldots, X_n$ be gaussian with covariance matrix Σ. Then for $\mathbf{i} : [k] \to [n]$, we have*

$$\mathbb{E}(X_{\mathbf{i}(1)} \cdots X_{\mathbf{i}(k)}) = \sum_{\pi \in P_2(k)} \prod_{(r,s) \in \pi} \mathbb{E}(X_{\mathbf{i}(r)} X_{\mathbf{i}(s)}).$$

Proof. Exercise. □

Definition 1.7 (Complex gaussian)**.** A standard *complex gaussian* variable Z is obtained by letting X and Y be independent standard real gaussians and letting $Z = \frac{1}{\sqrt{2}}(X + iY)$. This has mean 0 and variance 1:

$$\mathbb{E}(Z) = \frac{1}{\sqrt{2}}(\mathbb{E}(X) + i\mathbb{E}(Y)) = 0$$

and

$$\mathbb{E}(Z\overline{Z}) = \frac{1}{2}\mathbb{E}((X+iY)(X-iY)) = \frac{1}{2}(\mathbb{E}(X^2) + \mathbb{E}(Y^2)) = 1.$$

Proposition 1.8. *Let Z be a standard complex gaussian variable. Then*

$$\mathbb{E}(Z^m \overline{Z}^n) = \begin{cases} m! & \text{if } m = n \\ 0 & \text{otherwise} \end{cases}$$

for $m, n \geq 0$.

Proof. Exercise. □

Remark 1.9. By multilinearity, the structure of the Wick formula is retained when one replaces some of the real gaussians with complex gaussians and/or their adjoints. We will use this observation freely.

1.2. Self-adjoint gaussian matrix.

Definition 1.10 (Gaussian unitary ensemble)**.** Let $A = (a_{ij})_{1\le i,j\le N}$ be a matrix where

- $\{a_{ii} : 1 \le i \le N\}$ are iid real gaussian with mean 0 and variance $\frac{1}{N}$,
- $\{a_{ij} : 1 \le i < j \le N\}$ are iid complex gaussian with mean 0, variance $\frac{1}{N}$, and
- $a_{ij} = \overline{a_{ji}}$ for $1 \le j < i \le N$.

The point of this definition is that A is self-adjoint with independent gaussian entries, except as required by the self-adjointness. The choice of variance $\frac{1}{N}$ is for normalization and will play an important role when we make $N \to \infty$.

Definition 1.11. Let $(\Omega, \mathcal{F}, P)$ be a probability space and for $1 \le i, j \le N$, let $a_{ij} : \Omega \to \mathbb{C}$ be a random variable. Assume that $A = (a_{ij})_{i,j}$ is self-adjoint. This random matrix produces a random probability measure

$$\nu_A := \frac{1}{N}\sum_{i=1}^{N} \delta_{\lambda_i}$$

on $\mathbb{R}$, where $\lambda_1, \dots, \lambda_N$ are the eigenvalues of A. This is called the *empirical spectral distribution* (or *ESD*) of A.

The *average eigenvalue distribution* of A, denoted by μ_A, is simply the mean of ν_A: define μ_A by

$$\int_{\mathbb{R}} f(x)\, d\mu_A(x) = \mathbb{E}\left(\int_{\mathbb{R}} f(x)\, d\nu_A(x)\right)$$

for measurable f. This gives us a nice way to access the moments:

$$\int_{\mathbb{R}} x^m\, d\mu_A(x) = \mathbb{E}\left(\int_{\mathbb{R}} x^m\, d\nu_A(x)\right) = \mathbb{E}\left(\frac{1}{N}\sum_{i=1}^{N}\lambda_i^m\right) = \mathbb{E}\mathrm{tr}_N(A^m).$$

Theorem 1.12 (Wigner's semicircle law)**.** *Let A be the random matrix from Definition 1.10. Then $\mu_A \to \mu$ weakly as $N \to \infty$, where $d\mu = f\, dx$ with*

$$f(x) = \begin{cases} \frac{1}{2\pi}\sqrt{4 - x^2} & \textit{if } x \in [-2, 2] \\ 0 & \textit{otherwise} \end{cases}.$$

Remark 1.13. The mode of convergence in Theorem 1.12 can be strengthened. Namely, one can show $\nu_A \to \mu$ weakly in probability or weakly almost surely. This could be a good starting point for your project.

In this class and next, we will prove Theorem 1.12 using moments. The moments of the average eigenvalue distribution turn out to be encoded by a combinatorially rich sequence of polynomials – related to topological genus of certain surfaces – evaluated at $\frac{1}{N}$. We will come back to the latter connection later on; for now, we will only be concerned with the leading order.

Notation 1.14. Let $\gamma_n = (1, \ldots, n)$. We will use the notation $\#(\cdot)$ for the number of disjoint cycles in a permutation (including singletons/fixed points).

Theorem 1.15 (Genus expansion)**.** *We have*

$$\mathbb{E}(\operatorname{tr}_N(A^m)) = \sum_{\pi \in P_2(m)} \left(\frac{1}{N}\right)^{\frac{m}{2}+1-\#(\gamma_m \pi)}$$

for $m \geq 1$. When m is odd, the formula above should be read as an empty sum, i.e. as 0.

Remark 1.16. For $\pi \in P_2(2k)$, there are at least two ways to interpret the exponent $k+1-\#(\gamma_{2k}\pi)$. It is $2g_\pi$, where g_π is defined in either of the following two ways:

(1) g_π is the genus of the surface obtained from a polygon with $2k$ sides by gluing the sides together in pairs according to π;
(2) g_π is the smallest possible genus for which the following can be done: put the elements of $[2k]$ on a circle clockwise, make that circle the boundary of a surface with genus g_π, and draw π on the surface without crossings.

This is where the phrase "genus expansion" comes from.

Proof of Theorem 1.15. We have

$$\begin{aligned}
\mathbb{E}(\operatorname{tr}_N(A^m)) &= \frac{1}{N} \sum_{\mathbf{i}:[m]\to[N]} \mathbb{E}(a_{\mathbf{i}(1)\mathbf{i}(2)} \cdots a_{\mathbf{i}(m)\mathbf{i}(1)}) \\
&= \frac{1}{N} \sum_{\mathbf{i}:[m]\to[N]} \sum_{\pi \in P_2(m)} \prod_{(r,s)\in\pi} \mathbb{E}(a_{\mathbf{i}(r)\mathbf{i}(r+1)} a_{\mathbf{i}(s)\mathbf{i}(s+1)}) \\
&= \frac{1}{N} \sum_{\mathbf{i}:[m]\to[N]} \sum_{\pi \in P_2(m)} \prod_{(r,s)\in\pi} \delta_{\mathbf{i}(r)=\mathbf{i}(s+1)} \delta_{\mathbf{i}(r+1)=\mathbf{i}(s)} \frac{1}{N} \\
&= \frac{1}{N} \sum_{\mathbf{i}:[m]\to[N]} \sum_{\substack{\pi \in P_2(m) \\ \mathbf{i}=\mathbf{i}\circ\gamma_m\circ\pi}} \left(\frac{1}{N}\right)^{\frac{m}{2}} \\
&= \left(\frac{1}{N}\right)^{\frac{m}{2}+1} \sum_{\pi \in P_2(m)} |\{\mathbf{i} : [m] \to [N] : \mathbf{i} = \mathbf{i} \circ \gamma_m \circ \pi\}| \\
&= \left(\frac{1}{N}\right)^{\frac{m}{2}+1} \sum_{\pi \in P_2(m)} N^{\#(\gamma_m \pi)} \\
&= \sum_{\pi \in P_2(m)} \left(\frac{1}{N}\right)^{k+1-\#(\gamma_m \pi)}
\end{aligned}$$

since a map $\mathbf{i} : [m] \to [N]$ with $\mathbf{i} = \mathbf{i} \circ \gamma_m \circ \pi$ amounts to a choice of label from $[N]$ for each cycle in $\gamma_m \pi$. $\square$

1.3. **Exercises.**

Exercise 1.17. In this exercise, you will show that the moments of a standard gaussian variable count pair partitions.

(1) Let X be a standard gaussian variable. Prove that
$$\mathbb{E}(X^{2k}) = (2k-1)!! \text{ and } \mathbb{E}(X^{2k-1}) = 0$$
for all $k \geq 1$. *Use integration by parts to find a recursion.*

(2) Prove that $|P_2(2k)| = (2k-1)!!$ by putting $P_2(2k)$ in bijection with a set of cardinality $(2k-1)|P_2(2k-2)|$.

Exercise 1.18. In this exercise, you will prove the Wick formula: if $X_1, \ldots, X_n$ are gaussian with mean 0 and covariance matrix Σ, then
$$\mathbb{E}(X_{\mathbf{i}(1)} \cdots X_{\mathbf{i}(k)}) = \sum_{\pi \in P_2(k)} \prod_{(r,s) \in \pi} \mathbb{E}(X_{\mathbf{i}(r)} X_{\mathbf{i}(s)})$$
for all $\mathbf{i} : [k] \to [n]$.

(1) Assume Σ is diagonal and prove the claim.

(2) Prove the claim in general by diagonalizing Σ and using the multilinearity of the claimed formula.

Exercise 1.19 ([3, Exercise 1.6])**.** Let Z be a standard complex gaussian variable. Show that the moments are
$$\mathbb{E}(Z^m \overline{Z}^n) = \begin{cases} m! & \text{if } m = n \\ 0 & \text{otherwise} \end{cases}.$$

Hint: start by showing that
$$\mathbb{E}(Z^m \overline{Z}^n) = \frac{1}{\pi} \int_{\mathbb{R}^2} (t_1 + it_2)^m (t_1 - it_2)^n e^{-(t_1^2 + t_2^2)}\, dt_1\, dt_1$$
and then switch to polar coordinates to show that
$$\mathbb{E}(Z^m \overline{Z}^n) = \frac{1}{\pi} \int_0^{2\pi} \int_0^{\infty} r^{m+n+1} e^{i\theta(m-n)} e^{-r^2}\, dr\, d\theta.$$
Use this to prove the claim.

2. Semicircle law and noncommutative probability spaces

Recall the theorem from last class:

Theorem 1.15 (Genus expansion)**.** *We have*
$$\mathbb{E}(\mathrm{tr}_N(A^m)) = \sum_{\pi \in P_2(m)} \left(\frac{1}{N}\right)^{\frac{m}{2}+1-\#(\gamma_m \pi)}$$
for $m \geq 1$. When m is odd, the formula above should be read as an empty sum, i.e. as 0.

What happens when we send $N \to \infty$? Clearly, for the RHS of Theorem 1.15 to converge, the exponents have to be non-negative; if this is indeed the case, the only summands that will survive are the ones with $\frac{m}{2} + 1 - \#(\gamma\pi) = 0$.

Definition 2.1. A partition $\pi \in P(n)$ is said to be *noncrossing* if the following situation never occurs: there are some blocks $V, W \in \pi$ with $V \neq W$, and some $a, c \in V$ and $b, d \in W$ with $a < b < c < d$. The set of noncrossing partitions of $[n]$ is denoted by $NC(n)$.

Theorem 2.2 ([1])**.** *We have $\#(\gamma\pi) \leq k+1$ for all $\pi \in P_2(2k)$. Moreover, we have equality if and only if π is noncrossing.*

We will come back to this in a moment. First, let's use it to find the limiting moments of μ_A.

Notation 2.3. Write $NC_2(m)$ for the non-crossing pair partitions of $[m]$. When m is odd, $NC_2(m)$ is of course empty.

Proposition 2.4. *We have*

$$|NC_2(2k)| = \frac{1}{k+1}\binom{2k}{k} \text{ and } |NC_2(2k-1)| = 0$$

for all $k \geq 1$.

Proof. Exercise. □

Definition 2.5. The k-th *Catalan number* is $\mathrm{Cat}(k) := \frac{1}{k+1}\binom{2k}{k}$.

Corollary 2.6. *We have*

$$\lim_{N\to\infty} \mathbb{E}(\mathrm{tr}_N(A^{2k})) = \mathrm{Cat}(k) \text{ and } \lim_{N\to\infty} \mathbb{E}(\mathrm{tr}_N(A^{2k-1})) = 0$$

for $k \geq 1$.

2.1. **Which pairings survive in the limit?**

Recall the core combinatorial theorem:

Theorem 2.2 ([1])**.** *We have $\#(\gamma\pi) \leq k+1$ for all $\pi \in P_2(2k)$. Moreover, we have equality if and only if π is noncrossing.*

To see the inequality, we can make a simple observation about permutations:

Lemma 2.7. *Let $\alpha \in S_n$ and let $\tau = (i, j)$ be a transposition. Then*

$$\#(\alpha\tau) = \begin{cases} \#(\alpha)+1 & \text{if } i \text{ and } j \text{ are in the same cycle of } \alpha \\ \#(\alpha)-1 & \text{if } i \text{ and } j \text{ are in different cycles of } \alpha \end{cases}.$$

Remark 2.8. The permutation $\gamma_{2k}\pi$ can be thought of in terms of a building process: each pair in π is a transposition, which bumps the cycle count up or down by 1. We start with the one cycle of γ_{2k}, and the maximal situation is that each of the k pairs in π increases the number of cycles. This makes $\#(\gamma_{2k}\pi) \leq k+1$.

For example, let $k = 3$ and $\pi = (1,4)(2,3)(5,6)$. Then we start at $(1,2,3,4,5,6)$ with 1 cycle. Next, we multiply by $(1,4)$:

$$(1,2,3,4,5,6)(1,4) = (1,5,6)(2,3,4)$$

which has two cycles. Next,

$$(1,2,3,4,5,6)(1,4)(2,3) = (1,5,6)(2,4)(3)$$

which has three cycles. Finally,

$$(1,2,3,4,5,6)(1,4)(2,3)(5,6) = (1,5)(2,4)(3)(6)$$

which has four cycles. This is the maximal situation: each pair split a cycle in two.

On the other hand, now consider $\pi = (1,5)(2,3)(4,6)$. Then we again start at $(1,2,3,4,5,6)$ with 1 cycle. Then

$$(1,2,3,4,5,6)(1,5) = (1,6)(2,3,4,5)$$

has two cycles, as before. Next,

$$(1,2,3,4,5,6)(1,5)(2,3) = (1,6)(2,4,5)(3)$$

which is another splitting step (notice we haven't arrived at the crossing yet) giving us three cycles. The last step is different:

$$(1,2,3,4,5,6)(1,5)(2,3)(4,6) = (1,6,5,2,4)(3)$$

which is back down to two cycles. This is the generic situation: we can have both splits and merges.

Analyzing the case of equality can probably be done directly, but it is really more insightful to put all this in a proper algebraic framework. Let's work with general partitions and permutations, with size n; the results we need for pairings will fall out as special cases.

Definition 2.9. For $\alpha \in S_n$, let $|\alpha|$ be the *length* of α: the minimal number of transpositions needed to factor α. For $\alpha, \beta \in S_n$, write $d(\alpha, \beta) := |\alpha^{-1}\beta|$.

Proposition 2.10. *Notation as above. Then*

(1) $|\alpha| = n - \#(\alpha)$ *for all* $\alpha \in S_n$*;*
(2) (S_n, d) *is a metric space.*

Proof. For (1), use Lemma 2.7. (2) is a very direct and straightforward verification of axioms. □

Proposition 2.11 ([1])**.** *Let* $\phi : P(n) \to S_n$ *be the injective map which turns blocks into cycles. Let*

$$S_{NC}(\gamma_n) := \{\alpha \in S_n : d(e, \alpha) + d(\alpha, \gamma_n) = d(e, \gamma_n)\}.$$

Then $S_{NC}(\gamma_n)$ *is the range of* $\phi|_{NC(n)}$*.*

Proof. Finicky induction but elementary. See [1, Theorem 1]. □

Proof of Theorem 2.2. In (S_{2k}, d), for $\pi \in P_2(2k)$, the triangle inequality gives

$$d(e, \gamma_{2k}) \le d(e, \pi) + d(\pi, \gamma_{2k}).$$

Unpacking notation, this translates to

$$2k - 1 \le (2k - k) + (2k - \#(\gamma_{2k}\pi))$$

which simplifies to $\#(\gamma_{2k}\pi) \le k + 1$. The case of equality, i.e.

$$d(e, \gamma_{2k}) = d(e, \pi) + d(\pi, \gamma_{2k}),$$

corresponds to π being noncrossing due to Proposition 2.11. □

2.2. **Moment problem.**

Question 2.12. We just showed that the moments of the average eigenvalue distribution of a GUE converge to the Catalan numbers. How do we know this is a moment sequence, and how do we know this determines the weak limit of the average eigenvalue distribution?

The Catalan numbers appear as the moments of a particular distribution:

Proposition 2.13. *Let $d\mu = f(x)\,dx$ where*

$$f(x) = \begin{cases} \frac{1}{2\pi}\sqrt{4-x^2} & \textit{if } x \in [-2,2] \\ 0 & \textit{otherwise} \end{cases}.$$

Then

$$\int_{\mathbb{R}} x^{2k}\,d\mu(x) = \frac{1}{k+1}\binom{2k}{k} \quad \textit{and} \quad \int_{\mathbb{R}} x^{2k-1}\,d\mu(x) = 0$$

for all $k \geq 1$.

Proof. Exercise. □

Okay, so we can guess that maybe the average eigenvalue distribution of a GUE converges to the semicircle distribution. But we just found the moments match – *a priori* this could just be a funny coincidence. So we can refocus Question 2.12:

Question 2.12′. If $(\mu_n)_{n\geq 1}$ is a sequence in $\mathrm{Prob}(\mathbb{R})$ and $\mu \in \mathrm{Prob}(\mathbb{R})$ has

$$\lim_{n\to\infty} \int_{\mathbb{R}} x^m\,d\mu_n(x) = \int_{\mathbb{R}} x^m\,d\mu(x)$$

for all $m \geq 1$, then does μ_n converge to μ in some meaningful sense at the level of measures?

The answer to Question 2.12′ is a qualified "yes":

Theorem 2.14. *Let μ be a probability measure on $\mathbb{R}$ with compact support.*

(1) *If ν is another probability measure on $\mathbb{R}$ with*

$$\int_{\mathbb{R}} x^m\,d\mu(x) = \int_{\mathbb{R}} x^m\,d\nu(x)$$

for all $m \geq 1$, then $\mu = \nu$.

(2) *If $(\mu_n)_{n\geq 1}$ is a sequence of probability measures on $\mathbb{R}$ with*

$$\lim_{n\to\infty} \int_{\mathbb{R}} x^m\,d\mu_n(x) = \int_{\mathbb{R}} x^{,}\,d\mu(x)$$

for all $m \geq 1$, then $\mu_n \to \mu$ weakly as $n \to \infty$.

Proof. Big exercise. See [2, Theorems 30.1 & 30.2]. □

Proof of Theorem 1.12. Let μ_N be the average eigenvalue distribution of an $N \times N$ GUE, and let μ be the semicircle distribution with radius 2. We have already proved that

$$\lim_{N\to\infty} \int_{\mathbb{R}} x^m\,d\mu_N(x) = \int_{\mathbb{R}} x^m\,d\mu(x)$$

for all $m \geq 1$. Since μ has compact support, Theorem 2.14 shows that $\mu_A \to \mu$ weakly as $N \to \infty$. $\square$

2.3. **Noncommutative probability spaces.**

Definition 2.15. A $*$-*algebra* is a unital associative algebra over $\mathbb{C}$ with an operation $\mathcal{A} \to \mathcal{A} : a \mapsto a^*$ which is conjugate-linear and has $(a^*)^* = a$ and $(ab)^* = b^*a^*$ for all $a, b \in \mathcal{A}$. An element $a \in \mathcal{A}$ is said to be *positive* if $a = b^*b$ for some $b \in \mathcal{A}$.

Definition 2.16. A $*$-*probability space* is a pair $(\mathcal{A}, \varphi)$ where $\mathcal{A}$ is a $*$-algebra and φ is a linear functional on $\mathcal{A}$ with $\varphi(a^*a) \geq 0$ for all $a \in \mathcal{A}$, and $\varphi(1) = 1$.

Remark 2.17. The point of Definition 2.16 is to view the elements of $\mathcal{A}$ as "random variables" and the linear functional φ as the "expectation". This abstraction becomes useful when one needs to consider noncommutative objects as random variables.

Example 2.18 (Commutative case)**.** Let $(\Omega, \mathcal{F}, P)$ be a (classical) probability space, i.e. a measure space with total measure 1. Let $\mathcal{A} := L^\infty(\Omega, \mathcal{F}, P)$ be the algebra of essentially bounded functions, and let φ be the linear functional defined by

$$\varphi(f) = \int_\Omega f(\omega)\, dP(\omega)$$

for $f \in \mathcal{A}$. This is a $*$-probability space, where the $*$-operation is complex conjugation – in fact, it has a lot of analytic structure that we will put aside for now.

Example 2.19 (Finite moments)**.** Major objection to Example 2.18: many random variables we care about are not bounded. We can set up a similar example that will actually be more relevant for us: let $\mathcal{A} = L^{\infty-}(\Omega, \mathcal{F}, P)$ where $L^{\infty-}(\Omega, \mathcal{F}, P) := \bigcap_{p \geq 1} L^p(\Omega, \mathcal{F}, P)$, i.e. the algebra of random variables with all moments finite. (Use Hölder's inequality to show $\mathcal{A}$ is a $*$-algebra: once to show $L^p \supseteq L^q$ for $p \leq q$, and once to show $fg \in L^1$ for $f, g \in \mathcal{A}$.) The expectation φ is defined in the same way, by integrating functions against P. This is again a $*$-probability space.

Example 2.20 (Scalar matrices)**.** Let $\mathcal{A} = M_N$ be the algebra of $N \times N$ matrices and let $\varphi(A) = \frac{1}{N}\mathrm{Tr}(A)$. This is a $*$-probability space which is not commutative.

Example 2.21 (Random matrices)**.** Let $\mathcal{A} = M_N(L^{\infty-}(\Omega, \mathcal{F}, P))$ be the $*$-algebra of matrices with entries that are RVs with finite moments, and let φ be the expected trace: $\varphi(A) = \mathbb{E}\mathrm{tr}(A)$. For example, our GUE random matrix lives here.

So far, we haven't seen anything new. The real reason for making this abstraction is to include genuinely noncommutative situations – where there is no hope of identifying an underlying classical probability space – and view them as essentially probabilistic in nature. The best example comes from groups and their group rings.

Example 2.22 (Group algebra)**.** Let G be a group and let $\mathcal{A} := \mathbb{C}[G]$. The expectation is defined by

$$\varphi\left(\sum_{g \in G} a_g g\right) = a_e.$$

This is a $*$-probability space.

Next class, we will use group algebras and group-theoretical freeness to motivate Voiculescu's highly influential notion of *free independence*. Then, we will use it to construct a concrete operator model for the asymptotics of multiple GUEs.

2.4. **Exercises.**

Exercise 2.23. In this exercise, you will enumerate the noncrossing pairings and show that they are counted by the moments of the semicircle distribution. *(1) and (2) are classic textbook combinatorics. (3) is a somewhat involved calculus problem.*

(1) Find a recursion for $|NC_2(2k)|$. *Think back to the enumeration of* $P_2(2k)$.
(2) Show that $\mathrm{Cat}(k) := \frac{1}{k+1}\binom{2k}{k}$ satisfy the same recursion that you found in (1). *To do this, first show that with* $C(z) := \sum_{k=0}^{\infty} \mathrm{Cat}(k) z^k$, *we have* $C(z) = \frac{1-\sqrt{1-4z}}{2z}$, *and derive the functional equation* $C(z) = 1 + zC(z)^2$. *Recover the recursion from this functional equation.*
(3) Let $d\mu = f(x)\,dx$ where

$$f(x) = \begin{cases} \frac{1}{2\pi}\sqrt{1-4x} & \text{if } x \in [-2,2] \\ 0 & \text{otherwise} \end{cases}.$$

Show that

$$\int_{\mathbb{R}} x^{2k}\,d\mu(x) = \mathrm{Cat}(k) \text{ and } \int_{\mathbb{R}} x^{2k-1}\,d\mu(x)$$

for $k \geq 1$. *To do this, make the substitution* $x = 2\cos\theta$. *You can use the following identity without proof:*

$$\int_0^{\pi} \cos^{2m}\theta\,d\theta = \frac{(2m-1)!!}{(2m)!!}\pi.$$

Exercise 2.24. In this exercise, you will fill in the details of why convergence in moments implies weak convergence in the case of the semicircular law. In both parts, let μ be a probability measure on $\mathbb{R}$ with compact support. *This is part genuine exercise, part "book report". Both parts require some knowledge of measure theory.*

(1) Let ν be a probability measure on $\mathbb{R}$ with

$$\int_{\mathbb{R}} x^m\,d\mu(x) = \int_{\mathbb{R}} x^m\,d\nu(x)$$

for all $m \geq 1$. Prove that $\mu = \nu$. *Note: there is no assumption that* ν *has compact support! Be careful and think about how to get around this issue.*
(2) Let $(\mu_n)_{n\geq 1}$ be a sequence of probability measures on $\mathbb{R}$ with

$$\lim_{n\to\infty} \int_{\mathbb{R}} x^m\,d\mu_n(x) = \int_{\mathbb{R}} x^m\,d\mu(x)$$

for all $m \geq 1$. Prove that $\mu_n \to \mu$ weakly. *This is standard textbook material (Billingsley P&M Theorems 30.1 and 30.2). What I'm looking for is a concise summary of the argument that addresses its various subtleties: for example, how exactly is (1) being used, how do you establish tightness,* *etc. You don't need to reproduce proofs of basic classical theorems, like Markov inequality or Helly selection theorem/Prokhorov's theorem.*

3. Free independence

3.1. Motivation and definition.

Definition 3.1 (Group-theoretical freeness)**.** Let G be a group and let $\{G_i : i \in I\}$ be a family of subgroups. The subgroups are *free* if for all $k \geq 1$, for all $i_1, \ldots, i_k \in I$ with $i_j \neq i_{j+1}$, and for all $g_j \in G_{i_j}$ with $g_j \neq e$, we have $g_1 \cdots g_k \neq e$.

How does this look in terms of the $*$-probability space $(\mathbb{C}[G], \varphi)$? Well, the condition that

$$g_j \neq e \implies g_1 \cdots g_k \neq e \text{ translates to } \varphi(g_j) = 0 \implies \varphi(g_1 \cdots g_k) = 0.$$

Definition 3.2 (Freeness of subalgebras)**.** Let $(\mathcal{A}, \varphi)$ be a $*$-probability space, and let $\{\mathcal{A}_i : i \in I\}$ be a family of unital $*$-subalgebras. The family $\{\mathcal{A}_i : i \in I\}$ is said to be *freely independent* (or *free*) if for all $k \geq 1$, for all $i_1, \ldots, i_k \in I$ with $i_j \neq i_{j+1}$, and for all $a_j \in \mathcal{A}_{i_j}$ with $\varphi(a_j) = 0$, we have $\varphi(a_1 \cdots a_k) = 0$.

Proposition 3.3. *Let G be a group and let $\{G_i : i \in I\}$ be a family of subgroups. Then the subgroups are free in the group-theoretical sense if and only if the subalgebras $\mathbb{C}[G_i]$ of $\mathbb{C}[G]$ are freely independent with respect to φ.*

Proof. Exercise. I think this is an essential one. □

Definition 3.4 (Freeness of variables)**.** Let $(\mathcal{A}, \varphi)$ be a $*$-probability space and let $\{a_i : i \in I\}$ be a family in $\mathcal{A}$. For $i \in I$, let $\mathcal{A}_i$ be the $*$-subalgebra of $\mathcal{A}$ generated by a_i. The family $\{a_i : i \in I\}$ is said to be *freely independent* (or *free*) if the family $\{\mathcal{A}_i : i \in I\}$ is freely independent.

3.2. What does freeness actually do?

To understand what freeness means, let's look at some examples. This section is entirely based on [4, Lecture 5].

Example 3.5. Suppose that $\mathcal{A}$ and $\mathcal{B}$ are freely independent subalgebras of some ambient algebra. Let's look at some words with mixtures between $\mathcal{A}$ and $\mathcal{B}$.

Length two: for $a \in \mathcal{A}$ and $b \in \mathcal{B}$, freeness says

$$0 = \varphi((a - \varphi(a))(b - \varphi(b))) = \varphi(ab) - \varphi(a)\varphi(b)$$

so $\varphi(ab) = \varphi(a)\varphi(b)$.

Length three: for $a_1, a_2 \in \mathcal{A}$ and $b \in \mathcal{B}$, freeness says

$$\varphi((a - \varphi(a))(b - \varphi(b))(a - \varphi(a))) = 0.$$

Expanding and using the length two factorization, this says

$$\begin{aligned}
0 &= \varphi(a_1 b a_2) - \varphi(a_2)\varphi(a_1 b) - \varphi(b)\varphi(a_1 a_2) + \varphi(a_1)\varphi(a_2)\varphi(b) \\
&\quad - \varphi(a_1)\varphi(b a_2) + \varphi(a_1)\varphi(a_2)\varphi(b) + \varphi(a_1)\varphi(b)\varphi(a_2) - \varphi(a_1)\varphi(a_2)\varphi(b) \\
&= \varphi(a_1 b a_2) - \varphi(a_2)\varphi(a_1)\varphi(b) - \varphi(b)\varphi(a_1 a_2) + \varphi(a_1)\varphi(a_2)\varphi(b) \\
&\quad - \varphi(a_1)\varphi(b)\varphi(a_2) + \varphi(a_1)\varphi(a_2)\varphi(b) + \varphi(a_1)\varphi(b)\varphi(a_2) - \varphi(a_1)\varphi(a_2)\varphi(b)
\end{aligned}$$

$$= \varphi(a_1ba_2) - \varphi(a_1a_2)\varphi(b)$$

so $\varphi(a_1ba_2) = \varphi(a_1a_2)\varphi(b)$.

IMPORTANT: this factorization pattern does not continue. The same kind of calculation, with $a_1, a_2 \in \mathcal{A}$ and $b_1, b_2 \in \mathcal{B}$, shows that

$$\varphi(a_1b_1a_2b_2) = \varphi(a_1a_2)\varphi(b_1)\varphi(b_2) + \varphi(a_1)\varphi(a_2)\varphi(b_1b_2) - \varphi(a_1)\varphi(b_1)\varphi(a_2)\varphi(b_2).$$

The point of all this is that mixed moments only depend on mixed moments from the same subalgebra, via some complicated pattern.

Proposition 3.6. *Let $(\mathcal{A}, \varphi)$ be a $*$-probability space and let $\{\mathcal{A}_i : i \in I\}$ be freely independent $*$-subalgebras. Let $\mathcal{B}$ be the $*$-subalgebra of $\mathcal{A}$ generated by $\{\mathcal{A}_i : i \in I\}$. Then $\varphi|_{\mathcal{B}}$ is uniquely determined by $\{\varphi|_{\mathcal{A}_i} : i \in I\}$.*

Proof. See [4, Lemma 5.13]. □

3.3. **Free central limit theorem.** Similar to the last section, this one is entirely based on [4, Lecture 8]. From now on, fix a $*$-probability space $(\mathcal{A}, \varphi)$ and a sequence $(a_n)_{n\geq 1}$ in $\mathcal{A}$ with $a_n^* = a_n$, $\varphi(a_n) = 0$, and $\varphi(a_n^2) = 1$ for all $n \geq 1$. Also assume all the a_n have the same moment sequence and they are freely independent.

Theorem 3.7 ([5]). *We have*

$$\lim_{N\to\infty} \varphi\left(\left(\frac{a_1 + \cdots + a_N}{\sqrt{N}}\right)^m\right) = \begin{cases} \mathrm{Cat}(k) & \text{if } m = 2k \\ 0 & \text{otherwise} \end{cases}$$

for $m \geq 1$.

The first step is to simply unpack the LHS:

$$\varphi\left(\left(\frac{a_1 + \cdots + a_N}{\sqrt{N}}\right)^m\right) = \frac{1}{N^{m/2}} \sum_{\mathbf{i}:[m]\to[N]} \varphi(a_{\mathbf{i}(1)} \cdots a_{\mathbf{i}(m)}).$$

Notation 3.8. For $\mathbf{i} : [m] \to \mathbb{N}$, let $\ker(\mathbf{i})$ be the partition of $[m]$ defined by letting p and q be in the same block if and only if $\mathbf{i}(p) = \mathbf{i}(q)$.

Lemma 3.9. *If $\mathbf{i}, \mathbf{j} : [m] \to \mathbb{N}$ have $\ker(\mathbf{i}) = \ker(\mathbf{j})$, then*

$$\varphi(a_{\mathbf{i}(1)} \cdots a_{\mathbf{i}(m)}) = \varphi(a_{\mathbf{j}(1)} \cdots a_{\mathbf{j}(m)}).$$

Idea of proof. This follows from the assumption that the a_n all have the same distribution, plus the fact that free independence means mixed moments are determined by the individual distributions.

For example, suppose the common partition is $\{\{1, 3\}, \{2, 4\}\}$, and $\mathbf{i} = (1, 2, 1, 2)$ and $\mathbf{j} = (5, 3, 5, 3)$. Then, using the computations from Example 3.5, we have

$$\varphi(a_1a_2a_1a_2) = \varphi(a_1^2)\varphi(a_2)^2 + \varphi(a_1)^2\varphi(a_2^2) - \varphi(a_1)^2\varphi(a_2)^2$$

and

$$\varphi(a_5a_3a_5a_3) = \varphi(a_5^2)\varphi(a_3)^2 + \varphi(a_5)^2\varphi(a_3^2) - \varphi(a_5)^2\varphi(a_3)^2.$$

Since we assume the a_n all have the same moment sequence, these are the same. □

Notation 3.10. In light of Lemma 3.9, for $\pi \in P(m)$, write $\varphi(\pi)$ for the common value of $\varphi(a_{\mathbf{i}(1)} \cdots a_{\mathbf{i}(m)})$ where $\mathbf{i} : [m] \to [N]$ has $\ker(\mathbf{i}) = \pi$. Let A_π^N be the number of maps $\mathbf{i} : [m] \to [N]$ with $\ker(\mathbf{i}) = \pi$.

So we have

$$\varphi\left(\left(\frac{a_1 + \cdots + a_N}{\sqrt{N}}\right)^m\right) = \frac{1}{N^{m/2}} \sum_{\pi \in P(m)} A_\pi^N \varphi(\pi)$$

and the task is to see what happens to A_π^N as $N \to \infty$. We can immediately dispense with any π that has a singleton block:

Lemma 3.11. *If $\pi \in P(m)$ and there is some $V \in \pi$ with $|V| = 1$, then $\varphi(\pi) = 0$.*

Proof. Suppose that $\mathbf{i}(j) = r$ and $\{j\} \in \pi$. Then

$$\begin{aligned} \varphi(\pi) &= \varphi(a_{\mathbf{i}(1)} \cdots a_{\mathbf{i}(j-1)} a_r a_{\mathbf{i}(j+1)} \cdots a_{\mathbf{i}(m)}) \\ &= \varphi(a_{\mathbf{i}(1)} \cdots a_{\mathbf{i}(j-1)} a_{\mathbf{i}(j+1)} \cdots a_{\mathbf{i}(m)}) \varphi(a_r) \end{aligned}$$

using freeness and one of the computations in Example 3.5. We have $\varphi(a_r) = 0$, so $\varphi(\pi) = 0$. □

Now, we need to understand the limit of A_π^N where $\pi \in P(m)$ has $|V| \geq 2$ for all $V \in \pi$. This is straightforward: a map $\mathbf{i} : [m] \to [N]$ with $\pi = \ker(\mathbf{i})$ amounts to a choice of label from $[N]$ for each block of π, where we do not allow duplicate labels. There are

$$N(N-1) \cdots (N - |\pi| + 1)$$

choices, so we have

$$\varphi\left(\left(\frac{a_1 + \cdots + a_N}{\sqrt{N}}\right)^m\right) = \sum_{\substack{\pi \in P(m) \\ |V| \geq 2 \forall V \in \pi}} \frac{N(N-1) \cdots (N - |\pi| + 1)}{N^{m/2}} \varphi(\pi).$$

The condition on π makes $|\pi| \leq m/2$, and when $N \to \infty$, the fraction involving N goes to 1 if $|\pi| = m/2$, and goes to 0 otherwise. The only way we can have $|\pi| = 1$ is if $\pi \in P_2(m)$. So we have

$$\lim_{N \to \infty} \varphi\left(\left(\frac{a_1 + \cdots + a_N}{\sqrt{N}}\right)^m\right) = \sum_{\pi \in P_2(m)} \varphi(\pi).$$

Of course, if m is odd, this is 0.

Now let us compute $\varphi(\pi)$ for $\pi \in P_2(2k)$. Pick $\mathbf{i} : [m] \to \mathbb{N}$ with $\pi = \ker(\mathbf{i})$. If $\mathbf{i}(j) \neq \mathbf{i}(j+1)$ for all $1 \leq j \leq m-1$, then $\varphi(\pi) = 0$ by freeness; otherwise, there is some $1 \leq j \leq m-1$ with $\mathbf{i}(j) = \mathbf{j}(j+1)$. Using the computations from Example 3.5, we have

$$\begin{aligned} \varphi(\pi) &= \varphi(a_{\mathbf{i}(1)} \cdots a_{\mathbf{i}(j-1)} (a_{\mathbf{i}(j)} a_{\mathbf{i}(j+1)}) a_{\mathbf{j}(j+2)} \cdots a_{\mathbf{i}(m)}) \\ &= \varphi(a_{\mathbf{i}(1)} \cdots a_{\mathbf{i}(j-1)} a_{\mathbf{i}(j+2)} \cdots a_{\mathbf{i}(m)}) \varphi(a_{\mathbf{i}(j)} a_{\mathbf{i}(j+1)}) \\ &= \varphi(a_{\mathbf{i}(1)} \cdots a_{\mathbf{i}(j-1)} a_{\mathbf{i}(j+2)} \cdots a_{\mathbf{i}(m)}). \end{aligned}$$

The pairings where we can keep doing this k times are exactly the ones that are noncrossing, so we have

$$\varphi(\pi) = \begin{cases} 1 & \text{if } \pi \in NC_2(2k) \\ 0 & \text{if } \pi \in P_2(2k) \setminus NC_2(2k) \end{cases}.$$

This shows that

$$\lim_{N\to\infty} \varphi\left(\left(\frac{a_1 + \cdots + a_N}{\sqrt{N}}\right)^m\right) = \begin{cases} \mathrm{Cat}(k) & \text{if } m = 2k \\ 0 & \text{otherwise} \end{cases}$$

which is the claim of Theorem 3.7.

3.4. **Exercises.**

Exercise 3.12. Let G be a group and let $\mathcal{A} = \mathbb{C}[G]$. Let φ be the linear functional on $\mathcal{A}$ defined by

$$\varphi\left(\sum_{g\in G} a_g g\right) = a_e.$$

I would say (3) is essential for understanding the concept of free independence. I strongly suggest you do it, even if you don't hand it in.

(1) Prove that φ is positive by directly using the definition above.
(2) Find a Hilbert space H, a $*$-homomorphism $\pi : \mathcal{A} \to \mathcal{B}(H)$, and a vector $\xi \in H$ such that $\varphi(a) = \langle \pi(a)\xi, \xi\rangle$ for all $a \in \mathcal{A}$. Use the fact that such a thing exists to prove that φ is positive.
(3) Let $\{G_i : i \in I\}$ be a family of subgroups of G, and for $i \in I$, let $\mathcal{A}_i := \mathbb{C}[G_i]$. Prove that $\{G_i :\in I\}$ are free in the group-theoretical sense if and only if $\{\mathcal{A}_i : i \in I\}$ are freely independent.

4. Asymptotic freeness of multiple GUEs

4.1. **Free semicircular families.** The example of freeness in the last section will become relevant when we talk about random unitary matrices, but for now, we are looking for some noncommutative data that captures the asymptotics of multiple GUEs. The answer is that when $N \to \infty$, they become freely independent families of semicircular variables.

Definition 4.1 (Semicircular family)**.** Let $(\mathcal{A}, \varphi)$ be a $*$-probability space. A *free semicircular family* in $(\mathcal{A}, \varphi)$ consists of some elements $s_1, \ldots, s_r \in \mathcal{A}$ such that

- s_j is self-adjoint and semicircular, and
- $\{s_1, \ldots, s_r\}$ is freely independent.

Theorem 4.2. *For each $r \geq 1$, there is a $*$-probability space $(\mathcal{A}, \varphi)$ and some elements $s_1, \ldots, s_r \in \mathcal{A}$ such that*

(1) *$\{s_1, \ldots, s_r\}$ is a free semicircular family, and*
(2) *$\mathcal{A}$ is generated by $\{s_1, \ldots, s_r\}$.*

In this section, we will construct a concrete instance of a free semicircular family using creation and annihilation operators on the so-called *full Fock space*. This model will allow for very concrete calculations involving certain lattice paths which are in obvious bijection with NC_2.

Definition 4.3 (Full Fock space)**.** Fix a Hilbert space H. The *full Fock space* on H is the Hilbert space

$$\mathcal{F}(H) := \mathbb{C}\Omega \oplus \bigoplus_{n=1}^{\infty} H^{\otimes n}.$$

Here, the inner product of $H^{\otimes n}$ is given on elementary tensors by

$$\langle \xi_1 \otimes \ldots \otimes \xi_n, \eta_1 \otimes \cdots \otimes \eta_n \rangle = \langle \xi_1, \eta_1 \rangle \cdots \langle \xi_n, \eta_n \rangle$$

and the direct sum is the set of sequences $(\xi_n)_{n\geq 0}$ where $\xi_0 \in \mathbb{C}\Omega$ and $\xi_n \in H^{\otimes n}$ for $n \geq 1$, with $\sum_{n=1}^{\infty} \|\xi_n\|^2 < \infty$. The inner product is given by

$$\langle (\xi_n)_{n\geq 0}, (\eta_n)_{n\geq 0} \rangle = \sum_{n=0}^{\infty} \langle \xi_n, \eta_n \rangle.$$

The $*$-algebra $\mathcal{B}(\mathcal{F}(H))$ carries a canonical *vacuum state*:

$$\varphi(T) = \langle T\Omega, \Omega \rangle.$$

Then $(\mathcal{B}(\mathcal{F}(H))), \varphi)$ is a $*$-probability space.

Proposition 4.4. *For $\xi \in H$, there is an operator $c(\xi) \in \mathcal{B}(\mathcal{F}(H))$ defined by $c(\xi)\Omega = \xi$ and*

$$c(\xi)\xi_1 \otimes \cdots \otimes \xi_n = \xi \otimes \xi_1 \otimes \cdots \otimes \xi_n.$$

The adjoint is given by

$$c(\xi)^*\Omega = 0,\ c(\xi)^*\xi_1 = \langle \xi_1, \xi \rangle \Omega,$$

and

$$c(\xi)^*\xi_1 \otimes \cdots \otimes \xi_n = \langle \xi_1, \xi \rangle \xi_2 \otimes \cdots \otimes \xi_n$$

and has the following useful property:

$$c(\xi)^* c(\eta) = \langle \eta, \xi \rangle \cdot 1.$$

Specifically, $c(\xi)$ is a scalar multiple of an isometry, and $\|c(\xi)\| = \|\xi\|$.

Proof. Exercise. □

Proposition 4.5 (Semicircular)**.** *Let H be a Hilbert space and let $\xi \in H$. Then $c(\xi) + c(\xi)^* \in \mathcal{B}(\mathcal{F}(H))$ is a semicircular element with radius $2\|\xi\|$.*

The combinatorics of noncrossing pairings are directly built into this model, but in a slightly different form.

Definition 4.6. A *Dyck path* with m steps is a path in $\mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0}$ which

- starts at $(0, 0)$,
- takes steps of $(1, 1)$ or $(1, -1)$, and
- ends at $(m, 0)$.

Note that this definition includes the requirement that the path never goes below the x-axis. Let $D(m)$ be the set of Dyck paths with m steps; when m is odd, $D(m) = \emptyset$.

Lemma 4.7. *There is a canonical bijection $NC_2(m) \simeq D(m)$.*

Proof of Proposition 4.5. To clean up notation, let $a = c(\xi)$. We will compute moments:

$$\varphi((a+a^*)^m) = \sum_{\epsilon_1,\ldots,\epsilon_m \in \{1,*\}} \varphi(a^{\epsilon_1} \cdots a^{\epsilon_m}).$$

The key observation is that $\varphi(a^{\epsilon_1} \cdots a^{\epsilon_m})$ is just an indicator of a certain combinatorial property of the sequence $(\epsilon_1, \ldots, \epsilon_m)$: the sequence determines a lattice path with NE and SE steps, and the indicator detects whether or not it is a Dyck path.

To see this, for $\epsilon_1, \ldots, \epsilon_m \in \{1, *\}$, let

$$\lambda_j = \begin{cases} 1 & \text{if } \epsilon_{m-j+1} = 1 \\ -1 & \text{if } \epsilon_{m-j+1} = * \end{cases}$$

for $1 \leq j \leq m$. Then, if we read the expression $\xi^{\otimes 0}$ as Ω, we have

$$a^{\epsilon_1} \cdots a^{\epsilon_m} \Omega = \begin{cases} \xi^{\otimes(\lambda_1 + \cdots + \lambda_m)} & \text{if } \lambda_1 + \cdots + \lambda_k \geq 0 \, \forall \, 1 \leq k \leq m \\ 0 & \text{otherwise} \end{cases}$$

and

$$\begin{aligned} \varphi(a^{\epsilon_1} \cdots a^{\epsilon_m}) &= \langle a^{\epsilon_1} \cdots a^{\epsilon_m} \Omega, \Omega \rangle \\ &= \begin{cases} \langle \xi^{\otimes(\lambda_1 + \cdots + \lambda_m)}, \Omega \rangle & \text{if } \lambda_1 + \cdots + \lambda_k \geq 0 \, \forall \, 1 \leq k \leq m \\ 0 & \text{otherwise} \end{cases} \end{aligned}$$

The inner product in the last line is 1 if $\lambda_1 + \cdots + \lambda_m = 0$, and 0 otherwise. The condition $\lambda_1 + \cdots + \lambda_k \geq 0$ for all $1 \leq k \leq m$ means the path doesn't go below the x-axis, and the condition that $\lambda_1 + \cdots + \lambda_m = 0$ means it does return to the x-axis, i.e. it's a Dyck path. So $\varphi((a+a^*)^m)$ is the number of Dyck paths with m steps. By Lemma 4.7, this shows that $a + a^*$ is semicircular. $\square$

Proposition 4.8 (Freeness)**.** *Let H be a Hilbert space and let $H_1, \ldots, H_r$ be mutually orthogonal subspaces of H. For $1 \leq i \leq r$, let $\mathcal{A}_i$ be the $*$-subalgebra of $\mathcal{B}(\mathcal{F}(H))$ generated by $\{c(\xi) : \xi \in H_i\}$. Then $\mathcal{A}_1, \ldots, \mathcal{A}_r$ are freely independent.*

Proof. Let $1 \leq i_1, \ldots, i_k \leq r$ with $i_j \neq i_{j+1}$, and pick $T_j \in \mathcal{A}_{i_j}$ with $\varphi(T_j) = 0$. Assume without loss of generality that

$$T_j = c(\xi_1^j) \cdots c(\xi_{m_j}^j) c(\eta_1^j)^* \cdots c(\eta_{n_j}^j)^*$$

with $m_j + n_j \geq 1$ and all vectors in H_{i_j}. The reason we can do this, and ignore contributions from 1, is that any non-zero contribution from 1 will make φ non-zero.

If there is some $1 \leq j \leq k-1$ with $n_j \neq 0$ and $m_{j+1} \neq 0$, then the product $T_j T_{j+1}$ includes the product $c(\eta_{n_j}^j)^* c(\xi_1^{j+1}) = \langle \xi_1^{j+1}, \eta_{n_j}^j \rangle 1$. Since $H_j \perp H_{j+1}$, this is 0 and then $\varphi(T_1 \cdots T_k) = 0$.

Otherwise, for all $1 \le j \le k-1$, we have either $n_j = 0$ or $m_{j+1} = 0$. Then

$$T_1 \cdots T_k = c(\xi_1) \cdots c(\xi_m) c(\eta_1)^* \cdots c(\eta_n)^*$$

for some $\xi_1, \ldots, \xi_m, \eta_1, \ldots, \eta_n \in H$ with $m + n \ge 1$, and

$$\begin{aligned}\varphi(T_1 \cdots T_k) &= \langle c(\xi_1) \cdots c(\xi_m) c(\eta_1)^* \cdots c(\eta_n)^* \Omega, \Omega\rangle \\ &= \langle c(\eta_1)^* \cdots c(\eta_n)^* \Omega, c(\xi_m)^* \cdots c(\xi_1)^* \Omega\rangle.\end{aligned}$$

Since at least one of m or n is ≥ 1, one of the two arguments in the inner product is of the form $c(\xi)^*\Omega = 0$, so $\varphi(T_1 \cdots T_k) = 0$. □

Proof of Theorem 4.2. Let $\{e_1, \ldots, e_r\}$ be the standard orthonormal basis of $\mathbb{C}^r$, and let $s_j = c(e_j) \in \mathcal{B}(\mathcal{F}(\mathbb{C}^r))$ for $1 \le j \le r$. Let $\mathcal{A}$ be the $*$-algebra in $\mathcal{B}(\mathcal{F}(\mathbb{C}^r))$ generated by $\{s_1, \ldots, s_r\}$, and let $\varphi(T) = \langle T\Omega, \Omega\rangle$ for $T \in \mathcal{A}$. □

Remark 4.9. Theorem 4.2 is a bit artificially weak, because I don't want to assume any background in operator algebras. If we let $\mathcal{A}$ be the C^*-subalgebra of $\mathcal{B}(\mathcal{F}(\mathbb{C}^r))$ generated by $\{c(e_1)+c(e_1)^*, \ldots, c(e_r)+c(e_r)^*\}$ and let $\varphi(T) = \langle T\Omega, \Omega\rangle$ for $T \in \mathcal{A}$, then

(1) Ω is a cyclic vector for $\mathcal{A}$, meaning that $\{T\Omega : T \in \mathcal{A}\}$ is dense in $\mathcal{F}(H)$;
(2) φ is a faithful trace;
(3) for any C^*-algebra $\mathcal{B}$ with a faithful state ψ, if $\mathcal{B}$ is generated by a free semicircular family of size r, then there is a state-preserving $*$-isomorphism $\mathcal{A} \simeq \mathcal{B}$.

This is a very nice object and in light of (3), it is referred to as *the* semicircular C^*-algebra with r generators. See [4, Lecture 7] for details.

4.2. **Asymptotic freeness of GUEs.**

Theorem 4.10 ([6])**.** *Let $\{A_1, \ldots, A_r\}$ be an independent family of $N \times N$ GUEs, and let $\{s_1, \ldots, s_r\}$ be a free semicircular family. Then $(A_1, \ldots, A_r)$ converges in distribution to $(s_1, \ldots, s_r)$, in the following sense: for all $m \ge 1$ and $\mathbf{i} : [m] \to [r]$, we have*

$$\lim_{N\to\infty} \mathbb{E}\mathrm{tr}(A_{\mathbf{i}(1)} \cdots A_{\mathbf{i}(m)}) = \varphi(s_{\mathbf{i}(1)} \cdots s_{\mathbf{i}(m)}).$$

This theorem follows from an easy multivariate generalization of the genus expansion:

Theorem 1.15′. *Let $m \ge 1$ and $\mathbf{i} : [m] \to [r]$. Then*

$$\mathbb{E}(\mathrm{tr}_N(A_{\mathbf{i}(1)} \cdots A_{\mathbf{i}(m)})) = \sum_{\substack{\pi \in P_2(m) \\ \pi \le \ker(\mathbf{i})}} \left(\frac{1}{N}\right)^{\frac{m}{2}+1-\#(\gamma_m \pi)}.$$

When m is odd, the formula should be read as an empty sum, i.e. as 0.

Proof of Theorem 4.10. When $N \to \infty$ in the formula above, the only summands that survive are the ones with $\frac{m}{2} + 1 - \#(\gamma_m\pi) = 0$. These are the ones with π noncrossing, so

$$\mathbb{E}(\mathrm{tr}_N(A_{\mathbf{i}(1)} \cdots A_{\mathbf{i}(m)})) = |\{\pi \in NC_2(m) : \pi \le \ker(\mathbf{i})\}| + O(N^{-2})$$

and we need to show that

$$\varphi(s_{\mathbf{i}(1)} \cdots s_{\mathbf{i}(m)}) = |\{\pi \in NC_2(m) : \pi \leq \ker(\mathbf{i})\}|.$$

This is similar to Proposition 4.5: in the proof there, the words $a^{\epsilon_1} \cdots a^{\epsilon_m}$ which contribute to the count $|NC_2(m)|$ correspond to Dyck paths. There is a similar constraint here, but we also need pairs (r, s) of up and down steps to have $\mathbf{i}(r) = \mathbf{i}(s)$. In terms of $NC_2(m)$, this amounts to $\pi \leq \ker(\mathbf{i})$.

Here is an example of how this works: consider the path which makes two up steps and then two down steps, or in other words the noncrossing pairing $\{\{1, 4\}, \{2, 3\}\}$. This corresponds to

$$\begin{aligned} a^*_{\mathbf{i}(1)} a^*_{\mathbf{i}(2)} a_{\mathbf{i}(3)} a_{\mathbf{i}(4)} \Omega &= a^*_{\mathbf{i}(1)} a^*_{\mathbf{i}(2)} (e_{\mathbf{i}(3)} \otimes e_{\mathbf{i}(4)}) \\ &= a^*_{\mathbf{i}(1)} \langle e_{\mathbf{i}(3)}, e_{\mathbf{i}(2)} \rangle e_{\mathbf{i}(4)} \\ &= \langle e_{\mathbf{i}(3)}, e_{\mathbf{i}(2)} \rangle \langle e_{\mathbf{i}(1)}, e_{\mathbf{i}(4)} \rangle \Omega \end{aligned}$$

so we have the additional requirement that $\mathbf{i}(2) = \mathbf{i}(3)$ and $\mathbf{i}(1) = \mathbf{i}(4)$, i.e. the pairing is compatible with $\mathbf{i}$. $\square$

4.3. **Exercises.**

Exercise 4.11. Let H be a Hilbert space, let $\mathcal{F}(H)$ be its full Fock space, and let $\mathcal{F}_0(H)$ be the dense subspace of finite linear combinations of elementary tensors. In this exercise, you will fill in the details of the construction of creation and annihilation operators on $\mathcal{F}(H)$.

(1) For $\xi \in H$, define $c(\xi) : \mathcal{F}_0(H) \to \mathcal{F}(H)$ by letting

$$c(\xi)(\xi_1 \otimes \cdots \otimes \xi_n) = \xi \otimes \xi_1 \otimes \cdots \otimes \xi_n$$

and extending by linearity. Prove that $c(\xi)$ is bounded and extends to an element $c(\xi) \in \mathcal{B}(H)$ with $\|c(\xi)\| = \|\xi\|$. *Try to do it in a way that implies $c(\xi)$ is a scalar multiple of an isometry.*

(2) Prove that

$$c(\xi)^*\Omega = 0, \; c(\xi)^*\xi_1 = \langle \xi_1, \xi \rangle \Omega,$$

and

$$c(\xi)^*(\xi_1 \otimes \cdots \otimes \xi_n) = \langle \xi_1, \xi \rangle \xi_2 \otimes \cdots \otimes \xi_n$$

for $n \geq 2$.

(3) Prove that $c(\xi)^* c(\eta) = \langle \eta, \xi \rangle \cdot 1$.

Exercise 4.12. A *C^*-probability space* is a $*$-probability space $(\mathcal{A}, \varphi)$ where $\mathcal{A}$ is equipped with a norm, with respect to which it is complete, which has the properties

- $\|ab\| \leq \|a\| \|b\|$ for all $a, b \in \mathcal{A}$, and
- $\|a^* a\| = \|a\|^2$ for all $a \in \mathcal{A}$.

This might be familiar to you as a C^*-algebra equipped with a state. As usual in this course, we consider all algebras and related structures to be unital. *This exercise requires some knowledge of functional analysis beyond the prerequisites.*

(1) Let $(\mathcal{A}, \varphi)$ be a C^*-probability space and let $a \in \mathcal{A}$ be normal (meaning that $a^*a = aa^*$). Prove that there is a unique compactly supported measure on $\mathbb{C}$ such that

$$\varphi(a^p a^{*q}) = \int_{\mathbb{C}} z^p \overline{z}^q \, d\mu(z)$$

for all $p, q \geq 0$. *This is called the* $*$-distribution*, or simply the* distribution*, of a.*

(2) Let $(\mathcal{A}, \varphi)$ be a C^*-probability space and let $\{\mathcal{A}_i : i \in I\}$ be a freely independent family of $*$-subalgebras of $\mathcal{A}$. For $i \in I$, let $\mathcal{B}_i$ be the norm-closure of $\mathcal{A}_i$. Prove that $\{\mathcal{B}_i : i \in I\}$ are freely independent.

References

1. Philippe Biane, *Some properties of crossings and partitions*, Discrete Math. **175** (1997), no. 1-3, 41–53.
2. Patrick Billingsley, *Probability and measure*, third ed., Wiley Series in Probability and Mathematical Statistics, John Wiley & Sons, Inc., New York, 1995.
3. James A. Mingo and Roland Speicher, *Free probability and random matrices*, Fields Institute Monographs, vol. 35, Springer, New York; Fields Institute for Research in Mathematical Sciences, Toronto, ON, 2017.
4. Alexandru Nica and Roland Speicher, *Lectures on the combinatorics of free probability*, London Mathematical Society Lecture Note Series, vol. 335, Cambridge University Press, Cambridge, 2006.
5. Dan Voiculescu, *Symmetries of some reduced free product C^*-algebras*, Operator algebras and their connections with topology and ergodic theory (Buşteni, 1983), Lecture Notes in Math., vol. 1132, Springer, Berlin, 1985, pp. 556–588.
6. ———, *Limit laws for random matrices and free products*, Invent. Math. **104** (1991), no. 1, 201–220.