Free Probability

GOALS 2020

Operator Algebras $\rightsquigarrow$ Function Algebras

Unital C^*-Algebras $\rightsquigarrow$ $\mathcal{C}(X)$ for X compact, Hausdorff

von Neumann Algebras $\rightsquigarrow$ $L^\infty(X, \mu)$

A concrete example:

$$\mathcal{A} = \mathcal{C}([0,1]) \subset B(L^2([0,1], d\lambda))$$

$$\mathcal{A}'' = \overline{\mathcal{A}}^{WOT} = \overline{\mathcal{A}}^{SOT} = L^\infty([0,1], d\lambda) \subset B(L^2([0,1], d\lambda))$$

So we should be thinking measure theory or probability.

Probability Crash Course

A probability space is a triple $(\Omega, \mathcal{F}, \mathbb{P})$ where:

- Ω is a set;
- $\mathcal{F}$ is a σ-algebra; and
- $\mathbb{P}$ is a positive measure on $(\Omega, \mathcal{F})$ with $\mathbb{P}(\Omega) = 1$

These give rise to an expectation

$$\begin{aligned} \mathbb{E} : L^1(\Omega, \mathbb{P}) &\longrightarrow \mathbb{C} \\ X &\longmapsto \int_\Omega X(\omega)\, d\mathbb{P}(\omega) \end{aligned}$$

We have the space of essentially bounded random variables $L^\infty(\Omega, \mathbb{P})$ which give bounded operators on $L^2(\Omega, \mathbb{P})$ by multiplication.

Probability Crash Course

Let's record some properties:

- $L^\infty(\Omega, \mathbb{P}) = L^\infty(\Omega, \mathbb{P})'$ is a von Neumann algebra
- $\mathbb{E}[1] = 1$
- If $X \geq 0$ in $L^\infty(\Omega, \mathbb{P})$ then $\mathbb{E}[X] \geq 0$
- If $0 \leq X_1 \leq X_2 \leq \cdots \leq \infty$, then $\lim_{n\to\infty} \mathbb{E}[X_n] = \mathbb{E}[\lim_{n\to\infty} X_n]$

  (Monotone convergence theorem)
- $\mathbb{E}[XY] = \mathbb{E}[YX]$

A key property is independence:

(unital) subalgebras $(\mathcal{A}_i)_{i\in I}$ of $L^\infty(\Omega, \mathbb{P})$ are independent if

whenever $n \in \mathbb{N}$, $i_1, \ldots, i_n \in I$ are distinct,

and $X_1 \in \mathcal{A}_{i_1}, \ldots, X_n \in \mathcal{A}_{i_n}$ with $\mathbb{E}[X_{i_1}] = \cdots = \mathbb{E}[X_{i_n}] = 0$

we have $\mathbb{E}[X_{i_1} \cdots X_{i_n}] = 0$.

Variables are independent if the von Neumann algebras they generate are.

Wait, what? That isn't the usual definition!

Well, suppose X_1, X_2 are independent variables and f_1, f_2 are measurable functions. Write $a_1 = \mathbb{E}[f_1(X_1)]$, $a_2 = \mathbb{E}[f_2(X_2)]$.

Then

$$
\begin{aligned}
0 &= \mathbb{E}\left[\left(f_1(X_1) - a_1\right)\left(f_2(X_2) - a_2\right)\right] \\
&= \mathbb{E}\left[f_1(X_1) f_2(X_2)\right] - a_1 \mathbb{E}\left[f_2(X_2)\right] - a_2 \mathbb{E}\left[f_1(X_1)\right] + a_1 a_2
\end{aligned}
$$

$$
\mathbb{E}\left[f_1(X_1) f_2(X_2)\right] = a_1 a_2
$$

Using similar tricks, independence prescribes all mixed moments in terms of pure moments.

Theorem: The (Weakened) Central Limit Theorem

Suppose $(X_n)_{n\in\mathbb{N}}$ are independent random variables in $L^\infty(\Omega, \mathbb{P})$, so that:

- $\mathbb{E}[X_n^k] = \mathbb{E}[X_1^k]$ $\forall k$ (they are identically distributed)
- $\mathbb{E}[X_1] = 0$
- $\mathbb{E}[X_1^2] = 1$.

Let $S_N = \frac{1}{\sqrt{N}} \sum_{i=1}^{N} X_i$.

Then for all k, $\lim_{N\to\infty} \mathbb{E}[S_N^k] = \begin{cases} (k-1)!! & \text{if } k \text{ is even} \\ 0 & \text{else} \end{cases}$.

Note: The Gaussian distribution $\mathcal{N}(0,1)$ is the unique distribution with these moments, but it is not bounded and so doesn't quite fit in this simplified framework. $\blacksquare$

Proof: Write $m_b = \mathbb{E}[X_1^b]$.

$$\mathbb{E}[S_N^k] = N^{-k/2}\, \mathbb{E}\left[\left(\sum_{i=1}^{N} X_i\right)^k\right]$$

$$= N^{-k/2} \sum_{\alpha:[k]\to[N]} \mathbb{E}[X_{\alpha(1)} \cdots X_{\alpha(k)}]$$

A partition of $[k]$ is a set $\{B_1, \dots, B_m\}$ of disjoint subsets of $[k]$ with $[k] = B_1 \cup \dots \cup B_m$. The set of such is denoted by $\mathcal{P}(k)$.

A choice of $\alpha : [k] \to [N]$ is equivalent to choosing $\pi \in \mathcal{P}(k)$ and $\tilde{\alpha} : \pi \hookrightarrow [N]$.

$$= N^{-k/2} \sum_{\pi \in \mathcal{P}(k)} \sum_{\tilde{\alpha}: \pi \to [N]} \mathbb{E}[X_{\tilde{\alpha}([1]_\pi)} \cdots X_{\tilde{\alpha}([k]_\pi)}]$$

But this expectation depends only on π! Let us write m_π for shorthand.

$$= N^{-k/2} \sum_{\pi \in \mathcal{P}(k)} m_\pi\, N(N-1)\cdots(N-\#\pi+1)$$

$$= N^{-k/2} \sum_{\pi \in \mathcal{P}_2(k)} N^{k/2} + o(1)$$

$$\longrightarrow \#\mathcal{P}_2(k) = \begin{cases} (k-1)!! & \text{if } k \text{ is even} \\ 0 & \text{if } k \text{ is odd.} \end{cases}$$

If $\#\pi < k/2$, the contribution vanishes as $N \to \infty$.

But what is m_π? By independence, if π has blocks of sizes $\beta_1, \dots, \beta_m$, then

$$m_\pi = \mathbb{E}[X_1^{\beta_1} \cdots X_m^{\beta_m}] = \mathbb{E}[X_1^{\beta_1}] \cdots \mathbb{E}[X_1^{\beta_m}] = m_{\beta_1} \cdots m_{\beta_m}$$

In particular, if $\beta_j = 1$ ever, $m_\pi = 0$.

The only π satisfying both must have only blocks of size 2; the set of such is denoted $\mathcal{P}_2(k)$.

If $\pi \in \mathcal{P}_2(k)$, $m_\pi = \mathbb{E}[X_1^2]^{k/2} = 1$.

Free Probability Crash Course

- Suppose $\mathcal{M}$ is a von Neumann algebra with trace τ.
- $\tau[1] = 1$
- If $X \geq 0$ in $\mathcal{M}$ then $\tau[X] \geq 0$
- If $X_\lambda \nearrow X$, then $\lim_\lambda E[X_\lambda] = E[\lim_\lambda X_\lambda]$

  (τ is normal)
- $\tau[XY] = \tau[YX]$

A key property is free independence:

(unital) subalgebras $(\mathcal{A}_i)_{i \in I}$ of $\mathcal{M}$ are freely independent if

whenever $n \in \mathbb{N}$, $i_1, \dots, i_n \in I$ with $i_1 \neq i_2 \neq \cdots \neq i_n$

and $X_1 \in \mathcal{A}_{i_1}, \dots, X_n \in \mathcal{A}_{i_n}$ with $\tau[X_{i_1}] = \cdots = \tau[X_{i_n}] = 0$

we have $\tau[X_{i_1} \cdots X_{i_n}] = 0$.

Variables are freely independent if the von Neumann algebras they generate are.

Why do we need a new definition of independence?

The commutative one doesn't tell us how to evaluate products with repeated terms, since they can always be reduced in that setting, e.g. $X_1 X_2 X_1 X_2 = X_1^2 X_2^2$.

Why not try a simpler rule, like factor τ across independent algebras or just group variables by algebra? E.g., ask for $\tau(X_1 X_2 X_1 X_2) = \tau(X_1)\tau(X_2)\tau(X_1)\tau(X_2)$ or

$$= \tau(X_1^2)\,\tau(X_2^2)\,?$$

In the first case, the constants won't be independent from most algebras; in the second, things are only independent if they commute under τ, which isn't great.

Using the same centring trick, we can compute for X_1, X_2 free, that

$$\tau[X_1 X_2 X_1 X_2] = \tau[X_1^2]\,\tau[X_2]^2 + \tau[X_1]^2\,\tau[X_2^2] - \tau[X_1]^2\,\tau[X_2]^2$$

Where does this definition come from?

If Γ, Λ are groups, this is precisely the relation between $L(\Gamma)$ and $L(\Lambda)$ in $L(\Gamma * \Lambda)$ with respect to usual trace.

Also describes the state on an arbitrary free product of von Neumann algebras.

Theorem: The (Weakened) Free Central Limit Theorem

Suppose $(X_n)_{n\in\mathbb{N}}$ are freely independent random variables in $\mathcal{M}$, so that:

- $\tau[X_n^k] = \tau[X_1^k]$ $\forall k$ (they are identically distributed)
- $\tau[X_1] = 0$
- $\tau[X_1^2] = 1$.

Let $S_N = \frac{1}{\sqrt{N}} \sum_{i=1}^{N} X_i$.

Then for all k, $\lim_{N\to\infty} \tau[S_N^k] = \begin{cases} C_{k/2} & \text{if } k \text{ is even} \\ 0 & \text{else} \end{cases}$

where $C_b = \frac{1}{b+1}\binom{2b}{b}$ is the b-th Catalan number.

Proof: Write $m_b = \mathbb{E}[X_1^b]$.

$$\mathbb{E}[S_N^k] = N^{-k/2}\, \mathbb{E}\left[\left(\sum_{i=1}^N X_i\right)^k\right]$$

$$= N^{-k/2} \sum_{\alpha:[k]\to[N]} \mathbb{E}[X_{\alpha(1)} \cdots X_{\alpha(k)}]$$

A partition of $[k]$ is a set $\{B_1, \dots, B_m\}$ of disjoint subsets of $[k]$ with $[k] = B_1 \cup \dots \cup B_m$. The set of such is denoted by $P(k)$.

A choice of $\alpha : [k] \to [N]$ is equivalent to choosing $\pi \in P(k)$ and $\tilde{\alpha} : \pi \hookrightarrow [N]$.

$$= N^{-k/2} \sum_{\pi \in P(k)} \sum_{\tilde{\alpha}: \pi \to [N]} \mathbb{E}\left[X_{\tilde{\alpha}([1]_\pi)} \cdots X_{\tilde{\alpha}([k]_\pi)}\right]$$

But this expectation depends only on π! Let us write m_π for shorthand.

$$= N^{-k/2} \sum_{\pi \in P(k)} m_\pi\, N(N-1) \cdots (N - \#\pi + 1)$$

If $\#\pi < k/2$, the contribution vanishes as $N \to \infty$.

But what is m_π?

If π has a singleton, we still get a factor of $m_1 = \mathbb{E}[X_1] = 0$.

So only pair partitions contribute as $N \to \infty$.

But not all the same!

Notice $\tau[X_1 X_2 X_1 X_2] = 0$

$$\neq$$

$$\tau[X_1^2 X_2^2] = \tau[X_1^2]\,\tau[X_2^2] = 1.$$

If $\pi \in P_2(k)$, we can compute m_π recursively.

If $k = 0$, $\pi = \emptyset$, then $m_\pi = 1$

If π has a block $\{d, d+1\}$, then

$$m_\pi = \mathbb{E}\Big[\underbrace{\cdots\;}_{\text{free from } X_{\alpha(d)}} X_{\alpha(d)}^2 \underbrace{\;\cdots}_{\text{free from } X_{\alpha(d)}}\Big] = \mathbb{E}\left[X_{\alpha(d)}^2\right] m_{\pi \setminus \{\{d, d+1\}\}}$$

If π has no such block, $m_\pi = 0$

So $m_\pi = 1$ precisely when π can be reduced to the empty partition by removing blocks of consecutive elements.

Combinatorial fact: these are precisely the non-crossing partitions.

A partition $\pi \in \mathcal{P}(k)$ is non-crossing if whenever $1 \le w < x < y < z \le k$ with $w \sim y$, $x \sim z$, we have $w \sim x$.

The set of such is denoted $NC(k)$.

Proof: Write $m_b = \mathbb{E}[X_1^b]$.

$$\mathbb{E}[S_N^k] = N^{-k/2}\,\mathbb{E}\left[\left(\sum_{i=1}^N X_i\right)^k\right]$$

$$= N^{-k/2} \sum_{\alpha:[k]\to[N]} \mathbb{E}[X_{\alpha(1)} \cdots X_{\alpha(k)}]$$

A partition of $[k]$ is a set $\{B_1, \dots, B_m\}$ of disjoint subsets of $[k]$ with $[k] = B_1 \cup \dots \cup B_m$. The set of such is denoted by $P(k)$.

A choice of $\alpha : [k] \to [N]$ is equivalent to choosing $\pi \in P(k)$ and $\tilde{\alpha} : \pi \hookrightarrow [N]$.

$$= N^{-k/2} \sum_{\pi \in P(k)} \sum_{\tilde{\alpha}:\pi \to [N]} \mathbb{E}[X_{\tilde{\alpha}([1]_\pi)} \cdots X_{\tilde{\alpha}([k]_\pi)}]$$

But this expectation depends only on π! Let us write m_π for shorthand.

$$= N^{-k/2} \sum_{\pi \in P(k)} m_\pi\, N(N-1)\cdots(N-\#\pi+1)$$

If $\#\pi < k/2$, the contribution vanishes as $N \to \infty$.

But what is m_π?

If π has a singleton, we still get a factor of $m_1 = \mathbb{E}[X_1] = 0$.

So only pair partitions contribute as $N \to \infty$.

But not all the same!

$$= N^{-k/2} \sum_{\pi \in NC_2(k)} N^{k/2} + o(1)$$

$$\longrightarrow \#NC_2(k)$$

$$= \begin{cases} C_{k/2} & \text{if } k \text{ is even} \\ 0 & \text{else} \end{cases}.$$

Is this the distribution of some random variable?

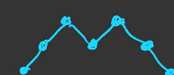
Consider $\mathcal{H} = \ell^2(\mathbb{N})$ and let $a \in B(\mathcal{H})$ be the unilateral shift, so $a\delta_j = \delta_{j+1}$. Note that $a^*\delta_j = \begin{cases} 0 & \text{if } j=1 \\ \delta_{j-1} & \text{else} \end{cases}$

Then $a^*a = 1$ and $aa^* = 1 - \mathrm{Proj}_{\delta_1}$.

Set $S = a + a^*$.

What is $\langle \delta_1, S^k \delta_1 \rangle$?

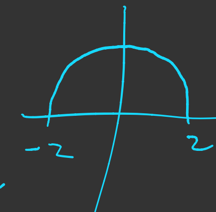
A term in the expansion of S^k corresponds to a path stepping up at each a^* and down at each a,

e.g. $a^* a^* a a^* a a$ $\rightsquigarrow$ 

To contribute, it must begin and end at the same level, and never cross below where it started. These are the Dyck paths, which are counted by $C_{k/2}$.

So $S \in B(\mathcal{H})$ with state $\langle \delta_1, \cdot\, \delta_1 \rangle$ is a central limit variable.

It has density $\frac{1}{2\pi}\sqrt{4-t^2}\, 1_{[-2,2]}$



and is called the semicircular distribution.

Fact: The von Neumann algebra generated by n independent Gaussians is isomorphic to the algebra generated by $1 : L^\infty(\mathbb{R}^n, d\gamma^n) \cong L^\infty(\mathbb{R}, d\gamma)$

Question: What about for free semicircular variables?

$$\left(L^\infty(\Omega, d\mathbb{P}),\ \mathbb{E}\right) \longleftrightarrow (\mathcal{A}, \tau)$$

Gaussian distribution $\longleftrightarrow$ Semicircular distribution

Independence $\longleftrightarrow$ Free independence

Partitions $\longleftrightarrow$ Non-crossing partitions

Log Fourier transform $\longleftrightarrow$ R transform

Conditional expectation $\longleftrightarrow$ Conditional expectation

Entropy / information theory $\longleftrightarrow$ Free entropy

Brownian motion (Lévy process with ind. stationary Gaussian increments) $\longleftrightarrow$ Free Brownian motion (free Lévy process with free ind. stationary $\cap$ increments)

Fact: if u is uniformly distributed on $\mathbb{T}$ (a Haar unitary) and X is freely independent from u, then $(u^k X u^{-k})_{k \in \mathbb{Z}}$ are free and identically distributed.

There isn't a way to do this in the commutative world.