Introduction to Free Probability

* Office hours: Tues 9am (check this works for most people)
* Poll the class about background:
  - Probability: Undergrad ____ Grad ____
  - Real Analysis: Undergrad ____ Grad ____
  - Complex Analysis: Undergrad ____ Grad ____
  - Functional Analysis ____
  - Combinatorics ____

Lecture 1: March 28, 2011

Free Probability is a beautiful new subject that incorporate ideas and tools from a wide range of mathematical areas. Here is a sampling:

* measure theory / probability
* free products of groups / group algebras
* operator algebras — notably Von Neumann algebras
* Complex analysis — notably analytic functions $G: \mathbb{C}_+ \to \mathbb{C}_-$ (from the upper-half-plane to the lower) satisfying $\lim_{|z|\to\infty} z \cdot G(z) = 1$.
* enumerative combinatorics:
  - generating functions
  - the lattices $NC(n)$ of non-crossing partitions on $[n] = \{1, \ldots, n\}$.
  - Möbius inversion on these lattices

There are also significant connections/applications to

* random matrix theory
* representation theory of symmetric groups
* structure theory of von Neumann algebras
* other combinatorial structures (e.g. parking functions)

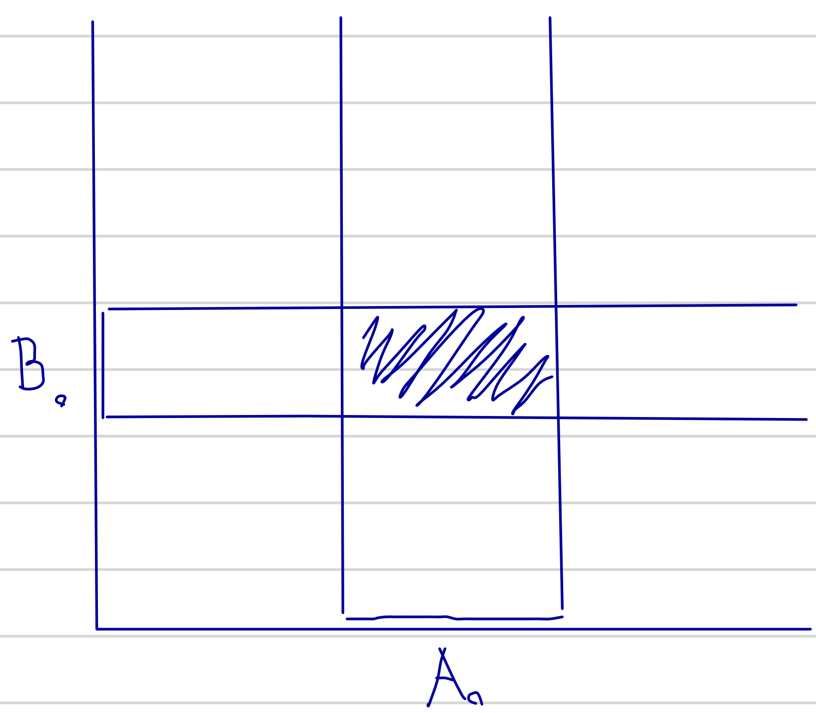
Basic Constructs of Classical Probability:

* fundamental objects are <u>events</u>: subsets of a "universe" Ω.
* the set $\mathcal{F}$ of admissible events is closed under countable $\cup$ and ^{c}.
* there is a "probability" function $\mathbb{P}: \mathcal{F} \to [0,1]$ with nice properties:
    - $\mathbb{P}(A \sqcup B) = \mathbb{P}(A) + \mathbb{P}(B)$
    - $\mathbb{P}$ is "continuous": if $A_n \uparrow A$, then $\mathbb{P}(A_n) \uparrow \mathbb{P}(A)$.
* from this and basics of $\cup, \cap$ get properties like

$$\mathbb{P}(A \cup B) = \mathbb{P}(A) + \mathbb{P}(B) - \mathbb{P}(A \cap B).$$

* Events A, B are called <u>independent</u> if $\mathbb{P}(A \cap B) = \mathbb{P}(A)\mathbb{P}(B)$.

(standard example: $\Omega = [0,1]^2$ with $\mathbb{P}$ = Lebesgue measure dx
then if $A = A_0 \times [0,1]$ & $B = [0,1] \times B_0$, then $\mathbb{P}(A \cap B) = \mathbb{P}(A)\mathbb{P}(B)$)



Can equally formulate everything in terms of functions

$$X : \Omega \to \mathbb{R} \ (\text{or } \mathbb{C})$$

Such functions are known as <u>random variables</u>. The set of such functions forms an <u>algebra</u> over $\mathbb{R}$ or $\mathbb{C}$. Moreover, it has a natural <u>involution</u> or <u>star</u> operation:

$$X^* = \overline{X}$$

(complex conjugation)

The set $\mathcal{F}$ of admissible subsets $\mathcal{F}$ of Ω is easily encoded in the algebra of random variables:

$$A \in \vec{\mathcal{F}} \iff \mathbb{1}_A : \Omega \to \mathbb{R}$$
$$\mathbb{1}_A(\omega) = \begin{cases} 0, & \omega \notin A \\ 1, & \omega \in A \end{cases}$$

These indicator functions are characterized (algebraically) as the <u>Idempotent elements</u> in the algebra: $\mathbb{1}_A^2 = \mathbb{1}_A$. The operations ^{c}, $\cup$ and $\cap$ can easily be identified on the level of r.v.'s as well:

$$\mathbb{1}_{A\cap B} = \mathbb{1}_A \mathbb{1}_B$$
$$\mathbb{1}_{A^c} = 1 - \mathbb{1}_A$$
$$\mathbb{1}_{A\cup B} = \mathbb{1}_{(A^c\cap B^c)^c} = \mathbb{1}_A + \mathbb{1}_B - \mathbb{1}_A \mathbb{1}_B$$

The probability measure also boosts to the level of random var's: by integration. This gives rise to the <u>Expectation</u> functional.

$$\mathbb{E}(X) = \int_\Omega X \, d\mathbb{P}$$

This recovers $\mathbb{P}$ since
$\mathbb{E}(\mathbb{1}_A) = \int_A d\mathbb{P} = \mathbb{P}(A)$.

think of this in terms of $d\mathbb{P} = dx$ on $\Omega = [0,1]^k$; nothing is lost in this restriction.

This brings up a technical issue: not every function can be integrated. The set of <u>integrable</u> functions is denoted $L^1(\Omega, \mathbb{P})$. The trouble is: this vector space is not closed under product – it is not an algebra.

One way to fix this is to restrict to the subset $L^\infty(\Omega,\mathbb{P}) \subset L^1(\Omega,\mathbb{P})$ of <u>bounded</u> random variables. This algebra has a natural norm topology on it: $\|X\|_\infty = \sup_\omega |X(\omega)|$.

The $\mathbb{E}$ linear functional has nice properties on $L^\infty(\Omega,\mathbb{P})$:

- $\mathbb{E}(1) = 1$ (<u>state</u>)
- $\mathbb{E}(|X|^2) = \mathbb{E}(\bar{X}X) \geq 0$ and $= 0$ iff $X = 0$ (<u>positive</u>, <u>faithful</u>)
- $\mathbb{E}$ is <u>continuous</u> w.r.t. the topology of $L^\infty(\Omega,\mathbb{P})$

actually contin. in a stronger sense – w^*.

Independence of random variables

We know what it means for events A, B to be independent; for random variables X, Y the usual definition is:

X, Y are <u>independent</u> if $X^{-1}(U), Y^{-1}(V)$ are independent events for any subsets U, V of (a class of measurable sets in) $\mathbb{R}$ or $\mathbb{C}$.

It is a standard exercise in a first graduate course in probability to show that this is equivalent to the following:

$\forall$ bounded, continuous functions $f, g : \mathbb{R} \to \mathbb{R}$

$$(*) \qquad \mathbb{E}(f(X)g(Y)) = \mathbb{E}(f(X))\,\mathbb{E}(g(Y)).$$

If $X, Y \in L^\infty$ are bounded to start with, then the Weierstrass approx. theorem shows we can take f, g to be restricted to <u>polynomials</u> in $(*)$.
Then the linearity of $\mathbb{E}$ shows that:

$$X, Y \in L^\infty \text{ are independent iff } \mathbb{E}(X^n Y^m) = \mathbb{E}(X^n)\mathbb{E}(Y^m) \ \forall n, m \in \mathbb{N}.$$

The moral is: all of the constructs of probability theory can be encoded (in algebraic language) in terms of a pair

$$(L^\infty, \mathbb{E})$$

(nice) algebra — (nice) linear functional

particularly important are <u>moments</u>:

$$\{\mathbb{E}(X^n) : n \in \mathbb{N}\} \leftarrow \text{moments of } X$$

$$\{\mathbb{E}(X^n Y^m) ; n, m \in \mathbb{N}\} \leftarrow \text{joint moments of } (X, Y).$$

Independence, in this format, is a (very simple) algorithm for computing the <u>joint</u> moments of (X, Y) from the <u>individual</u> moments of X and Y separately.

So, broadly speaking, a probability space can be identified as a pair

$$(\mathfrak{A}, \varphi)$$

where $\mathfrak{A}$ is a (complete normed) $*$-algebra, and $\varphi : \mathfrak{A} \to \mathbb{C}$ is a positive faithful continuous state on $\mathfrak{A}$.

Moreover, an independence rule is an algorithm for determining the joint moments of elements $x, y \in \mathfrak{A}$ from their individual moments $\varphi(x^n)$, $\varphi(y^n)$, $n = 1, 2, 3, \ldots$

The setup of classical probability uses a commutative algebra $\mathfrak{A}$. Next time we will explore what happens when we look at the same structure built on a non-commutative algebra $\mathfrak{A}$ — the group algebra $\mathbb{C}\mathbb{F}_k$ over a free group $\mathbb{F}_k$ $(k \geq 2)$.