Lecture 4: April 4, 2011

Examples of NCPS's (non-commutative probability spaces)

Ex 1. $L^\infty(\Omega,\mathcal{F},\mathbb{P})$, $\mathbb{E}$. The $*$ is complex conjugation.
↑
a commutative example (in some sense, the only kind)

Ex 2. $M_n(\mathbb{C}) \leftarrow$ $n\times n$ complex matrices. The $*$ is Hermitian conjugate – i.e. conjugate transpose. There are many possible states. All have the form

$$\varphi(A) = \mathrm{Tr}(A\Psi)$$

where Ψ is a positive-definite $n\times n$ matrix with $\mathrm{Tr}(\Psi)=1$. The study of this family of NCPS's (particularly how they combine under $\otimes$) is called <u>quantum information theory</u>.

The nicest example is $\Psi = \frac{1}{n}I$, so $\varphi = \frac{1}{n}\mathrm{Tr}$ ← normalized trace. Because of the tracial/cyclic property that Tr has, this example has the property $\varphi(AB)=\varphi(BA)$. It is the <u>only</u> such example.

Ex 3. Combine examples 1, 2. Let $\mathcal{A} = L^\infty(\Omega,\mathcal{F},\mathbb{P};M_n(\mathbb{C}))$ – random matrices, or (more precisely) matrix-valued bounded random variables. (We could alternatively view the elements of $\mathcal{A}$ as matrices with entries taken from the algebra L^∞. Still alternately, $\mathcal{A} \simeq L^\infty \otimes M_n(\mathbb{C})$.) The $*$ is conjugate transpose (transpose in the matrix, conjugate of the random variable). Here, the standard state is

$$\varphi(A) = \frac{1}{n}\mathbb{E}\,\mathrm{Tr}(A).$$

(i.e. the tensor product of the states on L^∞ and M_n). We could be fancier and define it as

$$\varphi_P(A) = \mathbb{E}\,\mathrm{Tr}(AP)$$

where the entries of P are $L^1(\Omega,\mathcal{F},\mathbb{P})$, and P is a.s. positive definite. But the case $P=\frac{1}{n}I$ has enough structure to be as interesting as we need.

Ex 4. $\mathcal{A} = \mathbb{C}G$ for a group G, $f^*(x) = \overline{f(x^{-1})}$, and $\varphi(f) = f(1_G)$.
This class of examples is the arena from which we derived the concept of freeness.

Ex 5. Let H be a Hilbert space. Let $\mathcal{A} \subset \mathcal{B}(H)$ be a $*$-subalgebra of the set of all bounded operators on H. (The $*$ on $\mathcal{B}(H)$ is the ∞-dim version of transpose; it is determined by the relation

$$\langle Ah, k \rangle_H = \langle h, A^*k \rangle_H \quad \forall h, k \in H.)$$

Let $\xi \in H$ be a unit vector: $\|\xi\|_H = 1$. Then define, for $A \in \mathcal{A}$,

$$\varphi_\xi(A) = \langle A\xi, \xi \rangle_H$$

This is called a <u>vector state</u>.

Exercise 4.1: verify that φ_ξ is a positive state. Give an example where φ_ξ is not faithful. (Hint: this can be accomplished in a finite-dimensional H.)

In fact, essentially every NCPS takes this form. This is called the GNS construction

Gelfand Naimark Segal $\Rightarrow$ Gross $\Rightarrow$ Driver, Kemp

mathematical genealogy aside.

<u>GNS construction:</u>
Let $(\mathcal{A}, \varphi)$ be a NCPS. First, we have the inner-product

$$\langle a, b \rangle_\varphi = \varphi(b^* a)$$

on the vector space $\mathcal{A}$. This is typically not complete (unless $\mathcal{A}$ is finite-dimensional), so we set H = the completion of $\mathcal{A}$ in $\langle \, , \rangle_\varphi$.

Now, $\mathcal{A}$ can be identified as an algebra of bounded operators on H: for a vector $v \in \mathcal{A} \subseteq H$, the action of $a \in \mathcal{A}$ on v is $a(v) = a \cdot v \in \mathcal{A}$.
We need to check this is a bounded operator:

$$\|a(v)\|^2 = \langle a(v), a(v) \rangle_\varphi = \langle a \cdot v, a \cdot v \rangle_\varphi = \varphi((av)^* av) = \varphi(v^* a^* a v).$$

The one bit of structure we need: the algebra $\mathfrak{A}$ must be such that, for every $a \in \mathfrak{A}$, there is a constant $\lambda_a > 0$ s.t.

Eg. if $a \in M_n(\mathbb{C})$, take $\lambda_a = \|a^* a\| = \|a\|^2$.

$$\lambda_a 1_{\mathfrak{A}} - a^* a \geq 0$$

$$\uparrow$$

i.e. $\lambda_a - a^* a = bb^*$ for some $b \in \mathfrak{A}$.

Morally, we are asking that "$a^* a \leq \lambda_a$." The kinds of algebras where this always happens are called <u>C^*-algebras</u>; we'll look more closely at them later.

So, assuming this is the case, we then have

$$\varphi(v^* bb^* v) = \varphi((v^* b) \cdot (v^* b)^*) \geq 0 \quad \text{as } \varphi \text{ is positive.}$$

$$\|$$

$$\varphi(v^* (\lambda_a - a^* a) v) = \lambda_a \cdot \varphi(v^* v) - \varphi(v^* a^* a v)$$
$$= \lambda_a \cdot \|v\|^2 - \|a(v)\|^2.$$

I.e. $\|a(v)\| \leq \sqrt{\lambda_a} \|v\|$, so $a(\cdot)$ is a bounded operator on $\mathfrak{A} \subset H$; since $\mathfrak{A}$ is dense in H, it follows that $a(\cdot)$ extends uniquely to a bounded operator on H.

Moreover, if $a, b \in \mathfrak{A}$ and $a(\cdot) = b(\cdot)$, this means $(a-b) \cdot v$ is 0 in H for all $v \in H$. In particular, $0 = \|(a-b) \cdot 1\|^2$
$= \varphi((a-b)(a-b)^*)$
$\Longrightarrow a - b = 0$.

So we have represented $\mathfrak{A}$ as an algebra of bounded operators on a Hilbert space H. (This H is often referred to as

$$H = L^2(\mathfrak{A}, \varphi).)$$

Finally, note that for any $a \in \mathfrak{A}$,

$$\varphi(a) = \varphi(a(1) \cdot 1) = \langle a(1), 1 \rangle_\varphi$$

So φ <u>is</u> a vector state, with unit vector $1 \in \mathfrak{A} \subset H$.

So every (C^*-)NCPS has this form. In particular, examples 1–4 are special cases of example 5.

Remark: it is not easy to see directly that the group algebra $\mathbb{C}G$ has the positive-dominance property. That is: given $f \in \mathbb{C}G$, $f = f^*$, it is true (Exercise) that there is a constant $\lambda_f > 0$ and a function $g: G \to \mathbb{C}$ such that $\lambda_f 1_{\mathbb{C}G} - f = g \cdot g^*$, that g may not have finite support. Ie. the definition of "positive" may need to be extended to include elements in an extension of the algebra. In the case of $\mathbb{C}G$ for discrete G, it is actually easy to realize the algebra as a $*$-subalgebra of $\mathcal{B}(H)$ for a particular Hilbert space H directly. We'll take a look at this next time.

Freeness in different NCPS's:

- we saw last time that freeness basically does not occur in Ex 1: if two classical r.v.'s are freely-independent, then one of them is constant.
- on the other hand, freeness is modeled after group-theoretic freeness in Ex. 4, so we know it readily occurs there.
- what about examples 2 and 3? It turns out that freeness never occurs here either. This is really an algebraic fact: given two matrices $A, B \in M_n(\mathbb{C})$ (random or not), there always exists a non-commutative polynomial $P(x,y)$ (a linear combination of words in x, y such as $x^2y^3xy^4x^7y$) such that $P(A,B) = 0$. Ie. ANY two matrices satisfy some non-trivial algebraic relation.

However, the degree of the required polynomial P grows (logarithmically) with n. In fact, matrices often exhibit asymptotic freeness. We will discuss this in detail later.