Lecture 3: April 1, 2011

Last time, we saw that the notion of algebraic freeness could be encapsulated in a combinatorial way using the "identity-component" linear functional on a group algebra. But when we calculated moments, the origins of this functional were unimportant. By analogy: a perfect model for independence in classical probability is afforded by orthogonal "cylinder sets" in a product probability space; but the definition of independence does not require this underlying structure to be known.

So, from here on, we work in the more general setting:

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

a $*$-algebra over $\mathbb{C}$ — a positive, faithful state on $\mathfrak{A}$.

In this general setting, we employ the combinatorial definition of freeness derived from algebraic freeness in $\mathbb{C}F$ w.r.t. φ_F.

<u>Def</u>: Two subalgebras $A, B < \mathfrak{A}$ are <u>free</u> if, for all $n \geq 2$, and all $a_1, \ldots, a_n \in A$ and $b_1, \ldots, b_n \in B$,

$$\varphi(a_i) = \varphi(b_i) = 0 \;\; \forall i = 1, \ldots, n \implies \varphi(a_1 b_1 \cdots a_n b_n) = 0$$
$$\& \; \varphi(b_1 a_2 \cdots a_n b_n) = 0$$
$$\& \; \varphi(a_1 b_1 \cdots b_{n-1} a_n) = 0.$$

<u>Remark</u>: Thinking of φ as a generalization of $\mathbb{E}$ for classical random variables, an element $a \in \mathfrak{A}$ with $\varphi(a) = 0$ is said to be <u>centered</u>.

In general, we will often use the operation $\mathring{a} \equiv a - \varphi(a)$, which is the <u>centering</u> of a.

Actually, we should state the definition for freeness of a collection of (possibly more than two) subalgebras.

<u>Def</u>: Let $A_1, \ldots, A_k < \mathfrak{A}$. They are <u>free</u> if, for any n and $i_1, \ldots, i_n$ such that $i_1 \neq i_2, i_2 \neq i_3, \ldots, i_{n-1} \neq i_n$, and any <u>centered</u> elements $a_1 \in A_{i_1}, \ldots, a_n \in A_{i_n}$,

$$\varphi(a_1 a_2 \cdots a_n) = 0.$$

Subsets $X_1,\ldots,X_k \subseteq \mathfrak{A}$ are free iff the subalgebras $\langle X_i\rangle_{\mathfrak{A}}$ they generate are free. In particular: elements $a_1,a_2,\ldots,a_k$ are free iff for any n, any $i_1\neq i_2\neq\cdots\neq i_n$ with $i_j\in\{1,\ldots,k\}$, and polynomials $P_1,\ldots,P_n$,

$$\varphi(P_j(a_{i_j}))=0 \;\forall j=1,\ldots,n \implies \varphi[P_1(a_{i_1})\cdots P_n(a_{i_n})]=0.$$

We have already explored the consequences of freeness. We can restate some of them here.

Eg. If $A,B<\mathfrak{A}$ are free and $a\in A, b\in B$, then $\varphi(ab)=\varphi(a)\varphi(b)$.
(In particular, if $a_0\in A, b_0\in B$ are fixed, then $a_0^n\in A$ and $b_0^m\in B$ $\forall n,m\in\mathbb{N}$; hence, $\varphi(a_0^n b_0^m)=\varphi(a_0^n)\varphi(b_0^m)$, as we saw before.

Eg. If $\{a_1,a_2\}$ and $\{b\}$ are free, then $\varphi(a_1ba_2)=\varphi(a_1a_2)\varphi(b)$.
This is an easy generalization of the calculation from the end of the previous lecture. Combining with the first example, this means that if $a_1,a_2,\ldots,a_n$ are all free, then $\varphi(a_1\cdots a_n)=\varphi(a_1)\cdots\varphi(a_n)$.

Eg. If $\{a_1,a_2\},\{b_1,b_2\}$ are free, then (generalizing Ex. 2.3) we have

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

In all these examples, the key feature is this: if A,B are free, then any joint moment <u>across</u> A and B separates into combinations of moments <u>within</u> A and B separately. Let's state and prove this as a proposition.

<u>Prop</u>: Let $A_1,\ldots,A_k<\mathfrak{A}$ be free subalgebras, and let $B=\langle A_1\cup\cdots\cup A_k\rangle_{\mathfrak{A}}$. Then $\varphi|_B$ is uniquely determined by $\varphi|_{A_1},\ldots,\varphi|_{A_k}$.

<u>Pf</u>. A general element of B is a linear combination of terms of the form $a_1a_2\cdots a_n$, where we may assume wlog that $a_j\in A_{i_j}$ for $i_1\neq i_2\neq\cdots\neq i_n$ (if two adjacent elements are in the same subalgebra, just multiply them and consider the product as a single element. So, it suffices to show that the joint moment

$$\varphi(a_1\cdots a_n)$$

is determined by $\varphi|_{A_1},\ldots,\varphi|_{A_k}$.

To see this, we proceed inductively on n. If $n=1$, since a_1 is in A_{i_1}, the moment is obviously determined by $\varphi|A_{i_1}$. Assume, therefore, that we know any moment of length $n-1$ is determined by the separate restrictions $\varphi|A_i$, $i=1..k$. Consider the centerings: $\mathring{a}_i = a_i - \varphi(a_i)$. Then

$$a_1 \cdots a_n = (\mathring{a}_1 + \varphi(a_1)) \cdots (\mathring{a}_n + \varphi(a_n))$$

$$= \mathring{a}_1 \cdots \mathring{a}_n + \sum \text{terms of length} \leq n-1.$$

Since $A_1, \ldots, A_k$ are free and $a_1, \ldots, a_n$ come from successively distinct subalgebras, it follows that $\varphi(\mathring{a}_1 \cdots \mathring{a}_n) = 0$. Therefore, by the linearity of φ, $\varphi(a_1 \cdots a_n)$ is equal to a linear combination of moments of length $\leq n-1$, and so, by the inductive hypothesis, is determined by $\varphi|A_1, \ldots, \varphi|A_k$. ▨

So far, the $*$-structure of the algebra $\mathcal{A}$ has not played an observable role in freeness. Let's explore how it comes into play.

<u>Def</u>: Subsets $X_1, \ldots, X_k \subseteq \mathcal{A}$ are called $*$-free if $X_1 \cup X_1^*, \ldots, X_k \cup X_k^*$ are free. (Note: $X^* \equiv \{x^* : x \in X\}$.) In particular, if $A_1, \ldots, A_k < \mathcal{A}$ are $*$-subalgebras (meaning closed under $*$) then they are free iff they are $*$-free.

<u>Prop</u>: If $A_1, A_2 < \mathcal{A}$ are $*$-free subalgebras, then $A_1 \cap A_2 = \mathbb{C} \cdot 1$.

<u>Pf</u>. Suppose $a \in A_1 \cap A_2$. Then $a^* \in A_1^* \cap A_2^*$, and so the two elements

$$b = (a + a^*)/2, \quad c = (a - a^*)/2i$$

are both in $A_1 \cup A_1^*$ and in $A_2 \cup A_2^*$. These two subsets are free, and so b is free from itself, as is c. Now, working with b, this means

$$\varphi(b) = \varphi(b \cdot b) = \varphi(b)^2.$$

But then $\varphi(\mathring{b}^2) = \varphi[(b - \varphi(b))^2] = \varphi(b^2 - 2\varphi(b) \cdot b + \varphi(b)^2]$
$= \varphi(b^2) - \varphi(b)^2 = 0.$ b/c φ is faithful

Since $b^* = \left(\frac{a+a^*}{2}\right)^* = \frac{a^*+a}{2} = b$, also $\mathring{b}^* = \mathring{b}$; so $0 = \varphi(\mathring{b}^2) = \varphi(\mathring{b}\mathring{b}^*) \Rightarrow \mathring{b} = 0$

So $0 = \mathring{b} = b - \varphi(b)\cdot 1$, and hence $b = \varphi(b)\cdot 1 \in \mathbb{C}\cdot 1$. Since $c^* = c$ as well, an analogous argument proves that $c = \varphi(c)\cdot 1 \in \mathbb{C}\cdot 1$. Thus,

$$a = \frac{a+a^*}{2} + i\cdot\frac{a-a^*}{2i} = b + ic \in \mathbb{C}\cdot 1.$$

$\blacksquare$

A Note on Non-Commutativity

We started with a model for freeness (freeness in groups) that is maximally non-commutative: no relations at all. But now we've abstracted to a combinatorial definition of freeness that, a priori, could make sense for commuting random variables. The next result shows this is not the case — freeness is an intrinsically non-commutative concept.

Prop: Suppose a, b are self-adjoint: $a = a^*$, $b = b^*$. If a, b are free and also commute ($ab = ba$) then at least one of a, b is constant.

Pf. Since $ab = ba$, $a^2b^2 = abab$. By freeness, on the one hand $\varphi(a^2b^2) = \varphi(a^2)\varphi(b^2)$. But also, appealing again to Ex. 2.3,

$$\varphi(a^2b^2) = \varphi(abab) = \varphi(a^2)\varphi(b)^2 + \varphi(a)^2\varphi(b^2) - \varphi(a)^2\varphi(b)^2.$$

Combining, this gives

$$\varphi(a^2)\varphi(b^2) = \varphi(a^2)\varphi(b)^2 + \varphi(a)^2\varphi(b^2) - \varphi(a)^2\varphi(b)^2$$

which simplifies to

$$\begin{aligned} 0 &= \varphi(a^2)\varphi(b^2) - \varphi(a^2)\varphi(b)^2 - \varphi(a)^2\varphi(b^2) + \varphi(a)^2\varphi(b)^2 \\ &= [\varphi(a^2) - \varphi(a)^2][\varphi(b^2) - \varphi(b)^2]. \end{aligned}$$

Hence, at least one of these two quantities is 0; wlog say $\varphi(a^2) - \varphi(a)^2 = 0$. As above, this shows that

$$\varphi[(a - \varphi(a))^2] = \varphi(a^2) - \varphi(a)^2 = 0.$$

Since $a = a^*$, $(a-\varphi(a))^2 = (a-\varphi(a))(a-\varphi(a))^*$ and so since φ is faithful we have $a - \varphi(a)\cdot 1 = 0$, as required. $\blacksquare$

Remark: The self-adjointness condition is very natural. In the context of classical random variables in $(L^\infty, \mathbb{E})$, where everything commutes, $X = X^*$ means $X = \overline{X}$ — i.e. X is real-valued. So, if two classical real-valued r.v.'s are free, one of them is constant. (Indeed, it is easy to check that this also holds true for $\mathbb{C}$-valued r.v.'s.

Remark: It is easy to check the (vacuously) true statement that constants are always free from everything.

Relation to Orthogonality

Since φ is positive and faithful, it is easy to check that the bilinear form

$$(a,b) \longmapsto \varphi(b^* a)$$

is an inner product on $\mathfrak{A}$. In the classical setting, this is the usual L^2-inner-product wrt which we define orthogonality. Indeed, if X, Y are (real-valued) classical r.v.'s that are independent, then

$$\mathbb{E}(\mathring{X}\mathring{Y}) = \mathbb{E}(\mathring{X})\mathbb{E}(\mathring{Y}) = 0.$$

So independence implies orthogonality (after centering). The following is a souped up version of this for free random variables (which is a very useful tool for computation.

Prop: Let $A_1, \ldots, A_k < \mathfrak{A}$ be free subalgebras. Consider centered elements $a_1, \ldots, a_n$ and $b_1, \ldots, b_m$ with $a_\ell \in A_{i_\ell}$ and $b_\ell \in A_{j_\ell}$, where the indices $i_1, \ldots, i_n$ and $j_1, \ldots, j_m$ satisfy $i_1 \neq i_2 \neq \cdots \neq i_n$ and $j_1 \neq \cdots \neq j_m$. Then

$$\varphi(a_1 \cdots a_n b_m \cdots b_1) = \begin{cases} \varphi(a_1 b_1) \cdots \varphi(a_n b_n) & \text{if } n = m \text{ \& } i_\ell = j_\ell \ \forall \ell \\ 0 & \text{otherwise} \end{cases}$$

Pf. Since the a_ℓ's are from consecutively-distinct algebras, as are the b_ℓ's, if $i_n \neq j_m$ then the whole list is consecutively-distinct, and since all elements are centered, by definition of freeness it follows that $\varphi(a_1 \cdots a_n b_m \cdots b_1) = 0$.

Suppose, instead, that $i_n = j_m$, so a_n, b_m are in the same algebra. Set $c = a_n b_m$. Then the product $a_1 \cdots a_{n-1} c b_{m-1} \cdots b_1$ consists of elements sampled from consecutively-distinct algebras.

The only catch is that c is not necessarily centered. Thus

$$\varphi(a_1\cdots a_{n-1} c\, b_{m-1}\cdots b_1) = \varphi[a_1\cdots a_{n-1}(\mathring{c}+\varphi(c))b_{m-1}\cdots b_1]$$

$$= \underbrace{\varphi[a_1\cdots a_{n-1}\mathring{c}\, b_{m-1}\cdots b_1]}_{0 \text{ by freeness}} + \varphi(c)\varphi(a_1\cdots a_{n-1}b_{m-1}\cdots b_1)$$

So, if $i_n = j_m$, we have $\varphi(a_1\cdots a_n b_m\cdots b_1) = \varphi(a_n b_m)\varphi(a_1\cdots a_{n-1}b_{m-1}\cdots b_1)$. Now iterate this observation $\min(n,m)$ times. If $n\neq m$, say $n>m$, the result will be

$$\varphi(a_n b_m)\varphi(a_{n-1}b_{m-1})\cdots\varphi(a_{n-m+1}b_1)\underbrace{\varphi(a_1\cdots a_{n-m})}_{0 \text{ by freeness}}$$

Thus, we only get $\neq 0$ when $n=m$ and $(i_1,\dots,i_n)=(j_1,\dots,j_m)$, resulting in the claimed equation.

∎

These orthogonality relations will come in handy in following lectures.

So, in general terms, we have seen that freeness is/provides an algorithm for computing joint moments from separate individual moments. But thus far, this is an "algorithm" in name only. If a,b are free, what is $\varphi(a^3b^7a^2bab)$ in terms of $\{\varphi(a^k),\varphi(b^k);\ 1\le k\le 7\}$? This could be worked out iteratively by hand, but would be very time-consuming.

A lot of this course will be devoted to understanding the combinatorics underlying freeness. This will involve lattices of non-crossing partitions, and Möbius inversion.

Before we get there, we should see a little more clearly why freeness is an interesting, important concept.

The first step en route is <u>distributions of non-commutative random variables</u>. That's next week's topic.

<u>Exercise</u>: at several points in the above proofs, we used (implicitly) the fact that if $a=a^*$, $\varphi(a)\in\mathbb{R}$. Show that this is true. As a consequence, show that, in general, $\varphi(a^*)=\overline{\varphi(a)}$.
<u>Hint</u>: Any selfadjoint can be decomposed as $a = \left(\frac{1+a}{2}\right)^2 - \left(\frac{1-a}{2}\right)^2$.