Lecture 2: March 30, 2011

Let F be a group. (Usually, we think of discrete groups here).
Let $H, K < F$ be subgroups.

Def: H, K are *free* in F if there are no non-trivial relations between them. To be precise:

$$\forall n \geq 2,\ h_1, \dots, h_n \in H - \{1\} \ \& \ k_1, \dots, k_n \in K - \{1\}$$

$$h_1 k_1 \cdots h_n k_n \neq 1$$
$$k_1 h_2 \cdots h_n k_n \neq 1$$
$$h_1 k_1 \cdots k_{n-1} h_n \neq 1$$

Given subsets $A, B \subseteq F$ (in particular singletons), say they are *free* if the subgroups $\langle A \rangle_F$, $\langle B \rangle_F$ they generate are free.

The canonical examples are given by free groups: $\mathbb{F}_k = \langle u_1, \dots, u_k \rangle$. In $\mathbb{F}_k$, $\langle u_1, \dots u_m \rangle$ and $\langle u_{m+1}, \dots u_k \rangle$ are free. This should be thought of in analogy to the canonical example of independence via Cartesian product in $[0,1]^2$. But freeness is much more malleable than orthogonality, as the following exercise demonstrates.

Ex 2.1: Let $\mathbb{F}_2 = \langle u, v \rangle$. Show that the subsets

$$\{u, v^{-1}uv\}, \{v^{-2}uv^2\}$$

are free. Use this observation to show that the subgroup $\langle u, v^{-1}uv^{-1}, v^{-2}uv^2 \rangle_{\mathbb{F}_2}$ is isomorphic to $\mathbb{F}_3$.

(Indeed, continuing in the manner of Ex. 2.1, one can show that $\mathbb{F}_2$ contains free subgroups of all countable orders.

The analogy with independence becomes clearer when we look at the *group algebra*.

Def. Let F be a group. The group algebra $\mathbb{C}F$ over the complex field is the abstract vector space with F as a basis. The scalar product is given by

$$\lambda\cdot(\alpha_1 x_1+\cdots+\alpha_n x_n)=\lambda\alpha_1\cdot x_1+\cdots+\lambda\alpha_n\cdot x_n,\quad \lambda,\alpha_i\in\mathbb{C},\ x_i\in F.$$

(product in $\mathbb{C}$)

The algebra product is the linear extension of the group product

$$(\alpha_1 x_1+\cdots+\alpha_n x_n)\cdot(\beta_1 y_1+\cdots+\beta_m y_m)=\sum_{\substack{1\le i\le n\\ 1\le j\le m}}\alpha_i\beta_j\cdot x_i y_j$$

(product in F; product in $\mathbb{C}$)

That's how an algebraist thinks about the group algebra. Analysts think of it this way instead.

Def. The group algebra $\mathbb{C}F$ of F over $\mathbb{C}$ is the set of finitely supported functions

$$f: F\to\mathbb{C}\quad (\text{ie. } f(x)=0 \text{ for all but finitely many } x\in F)$$

The scalar product on this vector space is the usual one, but the algebra product is convolution on the group F:

$$(f\cdot g)(x)=\sum_{y\in F} f(xy^{-1})g(y).$$

(This is a finite sum since f,g are finitely-supported.)

Ex. 2.2: Show that the two definitions of "group algebra" are isomorphic.

In the group algebra, most elements are not merely group elements, but rather linear combinations of them. So, to extend the notion of freeness to this setting, it is too weak to ask only that non-unity elements multiply to a non-unity element. We must contend with the unity-component.

Def: Let F be a group. Let $\varphi_F:\mathbb{C}F\to\mathbb{C}$ denote the unity-component of an element of $\mathbb{C}F$. That is,

$$\varphi_F(\alpha_1 1+\alpha_2 x_2+\alpha_3 x_3+\cdots)=\alpha_1.$$

in terms of the other picture of $\mathbb{C}F$:

$$\varphi_F(f)=f(1).$$

When restricted to the group $F \subset \mathbb{C}F$, φ_F is just the indicator function

$$\varphi_F|_F = \mathbb{1}_{\{1\}}.$$

So, in the group, we can rephrase freeness as follows:

$H, K < F$ are free if, given $h_1, \dots, h_n \in H$ & $k_1, \dots, k_n \in K$,

$$\varphi_F(h_i) = \varphi_F(k_i) = 0 \ \forall i \implies \varphi_F(h_1 k_1 \cdots h_n k_n) = 0$$
$$\& \ \varphi_F(h_1 k_1 \cdots h_n) = 0$$
$$\& \ \varphi_F(k_1 h_2 \cdots k_n) = 0.$$

Def: Let $A, B < \mathbb{C}F$ be subalgebras. Say they are free if, $\forall n \geq 2$, $a_1, \dots, a_n \in A$ & $b_1, \dots, b_n \in B$,

$$\varphi(a_i) = \varphi(b_i) = 0 \ \forall i \implies \varphi_F(a_1 b_1 \cdots a_n b_n) = 0, \text{ etc.}$$

Subsets $X, Y \subseteq \mathbb{C}F$ are free if the subalgebras $\langle X \rangle_{\mathbb{C}F}$ and $\langle Y \rangle_{\mathbb{C}F}$ are free. In particular, elements $a, b \in \mathbb{C}F$ are free if $\forall$ polynomials $p_1, \dots, p_n$ and $q_1, \dots, q_n$ (in one variable),

$$\varphi_F(p_i(a_i)) = \varphi_F(q_i(b_i)) = 0 \ \forall i$$
$$\implies \varphi_F(p_1(a_1) q_1(b_1) \cdots p_n(a_n) q_n(a_n)) = 0$$
$$\text{etc.}$$

Canonical example: in $\mathbb{C}F_2$ (F_2 generated by $\{u, v\}$), the generators u, v are free. As in the group case, it is also true that $\{u, v^{-1}uv\}$ and $\{v^2 u v^{-2}\}$ are free.

So, algebraic freeness (in a group algebra) can be described in the setting of a linear functional on the group algebra. Actually, φ_F is just the kind of nice linear functional we were describing in the previous lecture.

Indeed, any group algebra is a $*$-algebra via the standard involution

$$(\lambda_1 x_1 \cdots \lambda_n x_n)^* = \bar{\lambda}_1 x_1^{-1} + \cdots + \bar{\lambda}_n x_n^{-1}.$$

In terms of the other picture of a group algebra, this is

$$f^*(x) = \bar{f}(x^{-1}).$$

Why should this be the $*$? It is the unique involution on $\mathbb{C}F$ such that $x^* = x^{-1}$ for all group elements $x \in F$. This is desirable from a representation theory perspective — more on this next week.

Prop: the linear functional φ_F on $\mathbb{C}F$ is a positive faithful state.

Pf. $\varphi_F(1) = 1$ by definition. For the other properties, it is easiest to work in the analyst's picture.

$$f \cdot f^*(x) = \sum_{y \in F} f(xy^{-1}) f^*(y) = \sum_{y \in F} f(xy^{-1}) \bar{f}(y^{-1})$$

$$\therefore \varphi_F(f \cdot f^*) = f \cdot f^*(1) = \sum_{y \in F} f(y^{-1}) \bar{f}(y^{-1}) = \sum_{y \in F} |f(y^{-1})|^2.$$

This is a sum of squares, so is ≥ 0 and $= 0$ iff all the terms are 0. In the latter case, $f(y^{-1}) = 0$ for all y s.t. $y^{-1} \in \operatorname{supp} f$. Thus, $f = 0$ on its support, which means $f = 0$. ▨

Remark: It is also true that φ_F is continuous in an appropriate sense — but to make this claim requires a topology on $\mathbb{C}F$. We will discuss this topology a little later.

Thus, $(\mathbb{C}F, \varphi_F)$ is just the kind of arena we identified as a (generalized) probability space. However, unlike L^∞, $\mathbb{C}F$ is a non-commutative algebra (unless F is abelian). As we will see, this means that the naïve "independence" rule (factorization of moments) doesn't make sense. But freeness does. Let's look at some examples.

In the following examples, we assume $a, b \in \mathbb{C}\langle F \rangle$ are free.

Eg. Fix $n, m \in \mathbb{N}$. Let $p(x) = x^n - \varphi_F(a^n)$, and $q(x) = x^m - \varphi_F(b^m)$.

Then
$$\varphi_F[p(a)] = \varphi_F[a^n - \varphi_F(a^n)\cdot 1] = \varphi_F(a^n) - \varphi_F(a^n)\cdot\varphi_F(1)$$
(by linearity of φ_F)
$$= \varphi_F(a^n) - \varphi_F(a^n)\cdot 1 = 0.$$

Similarly, $\varphi_F[q(b)] = 0$. Thus, by freeness,

$$0 = \varphi_F[p(a)q(b)] = \varphi_F[(a^n - \varphi_F(a^n))(b^m - \varphi_F(b^m))]$$
$$= \varphi_F[a^n b^m - \varphi_F(a^n)b^m - \varphi_F(b^m)a^n + \varphi_F(a^n)\varphi_F(b^m)]$$
$$= \varphi_F(a^n b^m) - \varphi_F(a^n)\varphi_F(b^m) - \varphi_F(b^m)\varphi_F(b^m) + \varphi_F(a^n)\varphi_F(b^m)$$
$$= \varphi_F(a^n b^m) - \varphi_F(a^n)\varphi_F(b^m).$$

Thus, $\varphi_F(a^n b^m) = \varphi_F(a^n)\varphi_F(b^m)$. ← compare to $\mathbb{E}(X^n Y^m) = \mathbb{E}(X^n)\mathbb{E}(Y^m)$ for independent rv's $X, Y \in (L^\infty, \mathbb{E})$.

Eg. Since $\mathbb{C}\langle F \rangle$ is not generally abelian, aba is not typically of the form $a^n b^m$ for any n, m. But we can compute: using ideas like the previous example, set $\mathring{a} = a - \varphi_F(a)$ and $\mathring{b} = b - \varphi_F(b)$. Then $\varphi_F(\mathring{a}) = \varphi_F(\mathring{b}) = 0$, and so $\varphi_F(\mathring{a}\mathring{b}\mathring{a}) = 0$. Well,

$$\mathring{a}\mathring{b}\mathring{a} = (a - \varphi_F(a))(b - \varphi_F(b))(a - \varphi_F(a))$$
$$= aba - \varphi_F(a)ba - \varphi_F(b)a^2 - \varphi_F(a)ab$$
$$+ \varphi_F(a)\varphi_F(b)a + \varphi_F(a)^2 b + \varphi_F(a)\varphi_F(b)a$$
$$- \varphi_F(a)^2\varphi_F(b).$$

$$\therefore\quad 0 = \varphi_F(\mathring{a}\mathring{b}\mathring{a}) = \varphi_F(aba) - \varphi_F(a)\varphi_F(ba) - \varphi_F(b)\varphi_F(a^2) - \varphi_F(a)\varphi_F(ba)$$
$$+ \varphi_F(a)^2\varphi_F(b) + \varphi_F(a^2)\varphi_F(b) + \varphi_F(a)^2\varphi_F(b)$$
$$- \varphi_F(a)^2\varphi_F(b)$$

Using the result from the first exercise, $\varphi_F(ba) = \varphi_F(ab) = \varphi_F(a)\varphi_F(b)$.
Thus, we have

$$0 = \varphi_F(aba) - 2\varphi_F(a)^2\varphi_F(b) - \varphi_F(b)\varphi_F(a^2)$$
$$+ 2\varphi_F(a)^2\varphi_F(b) + \varphi_F(a^2)\varphi_F(b).$$

Hence, we conclude that $\varphi_F(aba) = \varphi_F(a^2)\varphi_F(b)$.

Similarly, $\varphi_F(a^l b^m a^n) = \varphi_F(a^{l+n})\varphi_F(b^m)$. This suggests a pattern... but that impression is misleading.

Eg. Let's look at abab. Again using $\mathring{a}, \mathring{b}$, we do the big calculation; the result is

Ex. 2.3: Show that, if a,b are free in $\mathbb{C}F$, then

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

So, the natural conjecture that freeness should mean $\varphi_F(a^{n_1}b^{m_1}\cdots a^{n_k}b^{m_k}) = \varphi_F(a^{n_1+\cdots+n_k})\varphi_F(b^{m_1+\cdots+m_k})$ is <u>false</u>. This only becomes apparent with at least two repetitions of each variable — as we will see later, this is because all set partitions of ≤ 3 elements are non-crossing.

What is apparent, however, is that if a,b are free in $\mathbb{C}F$, then the "joint moments" of $\{a,b\}$ are determined by the individual moments of a and b separately — i.e. $\varphi_F(a^{n_1}b^{m_1}\cdots a^{n_k}b^{m_k})$ is a polynomial in the moments

$$\{\varphi_F(a), \ldots, \varphi_F(a^{n_1+\cdots+n_k}), \varphi_F(b), \ldots, \varphi_F(b^{m_1+\cdots+m_k})\}.$$

We will prove this in the next lecture. The point is: freeness is an independence rule — it provides an algorithm for determining joint moments from individual ones.