David Thomas, 18.312 Lecture 3

Announcements:

Office hours changed to Tuesday 12-1pm and Wednesday 1-2pm.

Today:

(1) Möbius Inversion Example

(2) Multiplicative Functions, Dirichlet Series

(3) Permutations, Stirling Numbers

Möbius Inversion Example

Recall Möbius Inversion from last lecture. Let f, g be functions on $\mathbb{N}$, then $f(n) = \sum_{d|n} g(d)$ if and only if $g(n) = \sum_{d|n} \mu(d) f(\frac{n}{d})$ where $\mu(d)$ is the Mobius inversion function.

Fix $n \in \mathbb{N}$ and let

$$P(d) = \#\{\text{Primitive necklaces } (a_1, \ldots, a_d) | a_i \in [n]\}$$

Primitive means that all rotations are distinct ie. $r^i(\underline{a}) \neq r^j(\underline{a})$, for $i \neq j$ and $i, j \in [d]$. Fix $k \in \mathbb{N}$, let

$$\begin{aligned} N(k) &= \#\{\text{all necklaces } (a_1, \ldots, a_k) | a_i \in [n]\} \\ &= n^k \\ &= \sum_{d|k} P(d) \end{aligned}$$

Now using Möbius inversion we have

$$\begin{aligned} P(k) &= \sum_{d|k} \mu(d) N(\frac{k}{d}) \\ &= \sum_{d|k} \mu(d) n^{k/d} \end{aligned}$$

where $P(k)$ is divisible by k. Now we can reduce this to Fermats little theorem by setting $k = p$, then

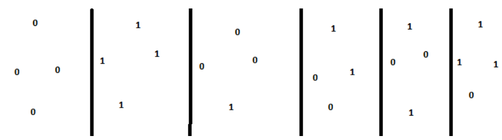
$$\begin{aligned} P(p) &= \mu(1) n^p + \mu(p) n \\ &= n^p - n \end{aligned}$$

Now fix $n \in \mathbb{N}$, let

$M(k) = \#\{\text{equivalence classes of necklaces } (a_1, \ldots, a_k), a_i \in [n], \text{up to rotations}\}$

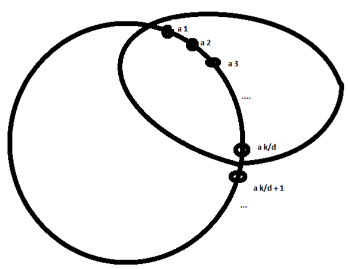
For example if $n = 2, k = 4$ then

$$M(4) = 6$$



Any necklace $\underline{a}$ has a stabilizer $stab(a) \subseteq C_k =< r >$ and $stab(a) = C_d =< r^{k/d} >$ for some divisor $d|k$. I will show that

$$\#\{\underline{a}|stab(\underline{a}) = C_d\} = \frac{P(k/d)}{k/d}$$



Since the stabilizer of $\underline{a}$ is C_d we have blocks of length k/d of the necklace that are repeated d times. $P(k/d)$ counts the different kinds of blocks. We must divide by k/d to correct for overcounting blocks that are rotations of each other, and hence are the same. Combining these into $\frac{P(k/d)}{k/d}$ counts the number of unique necklaces up to rotation with stabilizer C_d.

Hence

$$M(k) = \sum_{d|k} \frac{P(k/d)}{k/d}$$
$$= \sum_{d|k} \frac{P(d)}{d}$$

and substituting P(d) from earlier result yields

$$M(k) = \sum_{d|k} \frac{1}{d} \sum_{l|d} \mu(l) n^{d/l}$$
$$= \sum_{d|k} \frac{1}{d} \sum_{l|d} \mu(\frac{d}{l}) n^{l}$$
$$= \sum_{l|k} n^{l} \sum_{l|d|k} \frac{1}{d} \mu(\frac{d}{l})$$

letting $m = \frac{d}{l}$, we have

$$M(k) = \sum_{l|k} n^{l} \sum_{m|\frac{k}{l}} \frac{\mu(m)}{ml}$$
$$= \sum_{l|k} \frac{n^{l}}{l} \sum_{m|\frac{k}{l}} \frac{\mu(m)}{m}$$

and $\sum_{m|\frac{k}{l}} \frac{\mu(m)}{m} = \frac{\phi(k/l)}{k/l}$

$$M(k) = \sum_{l|k} \frac{n^{l}}{l} \frac{\phi(k/l)}{k/l}$$
$$= \frac{1}{k} \sum_{l|k} \phi(k/l) n^{l}$$

Now for a quick review of Burnside's Lemma before we show how to use it for a more concise proof of our result.

Lemma. *Group Action $G \times X \to X$, where G and X are finite. The number of orbits equals $\frac{1}{|G|} \sum_{g \in G} \psi(g)$, where $\psi(g) = \#\{x \in X | gx = x\}$.*

Proof.

$$\begin{aligned}\sum_{g\in G}\psi(g) &= \#\{(g,x)\in G\times X|gx=x\}\\ &= \sum_{x\in X}\#\{g\in G|gx=x\}\\ &= \sum_{x\in X}|stab(x)|\\ &= \sum_{x\in X}\frac{|G|}{|Orb(x)|}\\ &= |G|(\#\text{ of orbits })\end{aligned}$$

□

Now let's apply to our case: $G = C_k = \{1, r^1, r^2, \ldots, r^{k-1}\}, X = \{$ all necklaces $(a_1, \ldots, a_k)|a_i \in [n]\}$, and $\psi(r^i) = n^d$ where $d = GCD(i, k)$.

*note: $d = GCD(i,k)$, then $r^i(\underline{a}) = (\underline{a})$ if and only if $r^d(\underline{a}) = (\underline{a})$ and $\#\{i \in [k]|GCD(i,k) = d\} = \phi(k/d)$

Then Burnside's Lemma gives us

$$M(k) = \frac{1}{k}\sum_{i=1}^{k}\psi(r^i) = \frac{1}{k}\sum_{d|k}\phi(k/d)n^d$$

Multiplicative Functions, Dirichlet Series

Let $f, g : \mathbb{N} \to \mathbb{C}$. We will denote convolution by $*$. Then $(f * g)(n) = \sum_{d|n} f(d)g(\frac{n}{d})$. It is useful to consider dirichlet series which are functions of the form $F(s) = \sum_{n\geq 1}\frac{f(n)}{n^s}$. The product of two dirichlet functions is

$$\begin{aligned}F(S)G(S) &= (\sum_{n\geq 1}\frac{f(n)}{n^s})(\sum_{n\geq 1}\frac{g(n)}{n^s})\\ &= \sum_{k\geq 1}\sum_{l\geq 1}\frac{f(k)g(l)}{(kl)^s}\\ &= \sum_{n\geq 1}\frac{\sum_{kd=n} f(k)g(l)}{n^s}\\ &= \sum_{n\geq 1}\frac{(f*g)(n)}{n^s}\end{aligned}$$

which is also a dirichlet series/function.

Definition: A function f is *multiplicative* if f(mn) = f(m)f(n) whenever GCD(m,n) =1.

For example $\phi, \mu, n^\alpha, \tau(n) = \#\{\text{divisors of n}\}, \sigma_\alpha(n) = \sum_{d|n} d^\alpha$ are all multiplicative functions.

If f is multiplicative, then $\sum_{n\geq 1} \frac{f(n)}{n^s} = \prod_{\text{p prime}}(f(1)+\frac{f(p)}{p^s}+\frac{f(p^2)}{p^{2s}}+\dots)$, which is called the Euler Product.

For example, let $f(n) = 1$ forall n, and let

$$\begin{aligned}\zeta(s) &= \sum_{n\geq 1} \frac{1}{n^s} \\ &= \prod_{\text{p prime}} (1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \dots) \\ &= \prod_{\text{p prime}} \frac{1}{1-p^{-s}}\end{aligned}$$

Then

$$\begin{aligned}\frac{1}{\zeta(s)} &= \prod_{\text{p prime}} (1-p^{-s}) \\ &= \sum_{n\geq 1} \frac{f(n)}{n^s}\end{aligned}$$

where $f(p_1 \dots p_k) = (-1)^k$ if p_i distinct primes and $f(n) = 0$ if n is not square-free

Hence

$$\sum_{n\geq 1} \frac{f(n)}{n^s} = \sum_{n\geq 1} \frac{\mu(n)}{n^s}$$

This gives us more ways to express Möbius Inversion:

$$f(n) = \sum_{d|n} g(d) \leftrightarrow g(n) = \sum_{d|n} \mu(\frac{n}{d}) f(d)$$

or equivalently

$$f = g * 1 \leftrightarrow g = \mu * f$$

or equivalently

$$F(s) = G(s)\zeta(s) \leftrightarrow G(s) = \frac{1}{\zeta(s)} F(s)$$

To end this section we will explore two more properties of convolution.

Note: * is associative!

$$(f * g) * h = f * (g * h)$$

$$(FG)H = F(GH)$$

Example: Compute $\sum_{d|n} \phi(d)\tau(\frac{n}{d})$, where $\tau(n) = \#\{d|\text{d divides n}\}$.

$$\begin{aligned}\sum_{d|n} \phi(d)\tau(\frac{n}{d}) &= (\phi * \tau)(n) \\ &= ((\mu * n) * (1 * 1))(n) \\ &= ((\mu * 1) * (n * 1))(n)\end{aligned}$$

Let $\delta = (\mu * 1)$, then $\delta(n) = 1$ when $n = 1$ and 0 for $n \geq 2$. δ is the identity for convolution, $\delta * f = f$. Hence counting with our problem we have

$$\begin{aligned}((\mu * 1) * (n * 1))(n) &= (n * 1)(n) \\ &= \sum_{d|n} d\end{aligned}$$

Note: if f,g are multiplicative, then f*g is also multiplicative.

$$\begin{aligned}\sum_{n\geq 1} \frac{(f * g)(n)}{n^s} &= (\sum_{n\geq 1} \frac{f(n)}{n^s})(\sum_{n\geq 1} \frac{g(n)}{n^s}) \\ &= \prod_{\text{p prime}} (\sum_{k\geq 0} \frac{f(p^k)}{p^{ks}})(\sum_{l\geq 0} \frac{g(p^l)}{p^{ls}}) \\ &= \prod_{\text{p prime}} \sum_{k,l\geq 0} \frac{f(p^k)g(p^l)}{p^{ks}p^{ls}} \\ &= \prod_{\text{p prime}} \sum_{m\geq 0} \frac{1}{p^{ms}} \sum_{k+l=m} f(p^k)g(p^l) \\ &= \prod_{\text{p prime}} \sum_{m\geq 0} \frac{1}{p^{ms}} \sum_{d|p^m} f(d)g(\frac{p^m}{d}) \\ &= f * g(p^m)\end{aligned}$$

Permutations and Stirling Numbers

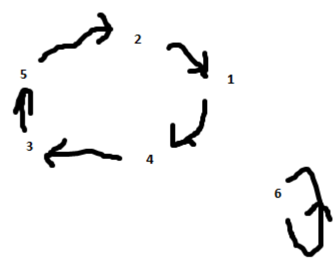
Permutation $\pi \in S_n$ where $S_n = \{\text{bijections from } [n] \to [n]\}$
In two-line notation

```
1 2 3 4 5 6

--------------

4 1 5 3 2 6
```

means $\pi(1) = 4, \pi(2) = 1, \pi(3) = 5, \pi(4) = 3, \pi(5) = 2, \pi(6) = 6$. In cycle notation this permutation π would be represented by (14352)(6) as shown below



Let $c(n, k)$ (signless Stirling number of the first kind) be the number of $\pi \in S_n$ that have exactly k cycles. For example,

$$c(n, n) = 1$$

This is because there is only one way to put each element in [n] into its own cycle.

$$c(n, 1) = (n - 1)!$$

Letting 1 be the first element we list in the cycle notation (ie. (1 . . .)), then there are (n-1)! different ways to order the elements that come next which correspond to the different ways to arrange the cycle.

$$c(n, n - 1) = \binom{n}{2}$$

Let c_i denote the length of the ith cycle and $c_i \leq c_{i+1}$. Then $\sum_{i \in [n-1]} c_i = n$ and $c_i \geq 1$. It follows that $c_i = 1$ for $i \in [n - 2]$ and $c_{n-1} = 2$. Hence there are n-2 cycles of length 1 and one cycle of length 2. There are $\binom{n}{2}$ ways to choose the elements that are in the 2-cycle. Since cycle $(ab) = (ba)$, $\binom{n}{2}$ is not undercounting and the result follows.

Lemma. $c(n,k) = (n-1)c(n-1,k) + c(n-1,k-1)$

Proof. Given a permutation $\pi \in S_{n-1}$, one can either

(1) Insert n in an existing cycle, $(n-1)c(n-1,k)$
(2) Make n into its own cycle, $c(n-1,k-1)$

□

Here are a few values for $c(n,k)$:

	n \ k	1	2	3	4
	0				
n	1	1	0	0	0
	2	1	1	0	0
	3	2	3	1	0
	4	6	11	6	1

Lemma. $\sum_{k=1}^{n} c(n,k)x^k = x(x+1)(x+2)\dots(x+n-1)$

We will prove this next lecture.