Combinatorics 2018 Fall

Teaching by: Professor Xiande Zhang

2018.10.08

Key words: *Möbius Inversion*, Poset

Recall: $f = \{f(n)\}$, $g = \{g(n)\}$

(1) $(f \odot g)(n) = \sum_{d \mid n} f(d)g(\frac{n}{d})$

(2) Identity: $I = \{I(n)\} = \{1, 0, 0, \dots\}$, $f \odot I = I \odot f = f$
if $f \odot g = I$, say f is D-invertible $\Longleftrightarrow f(1) \neq 0$

(3) $e = \{e(n)\} = \{1, 1, 1, \dots\}$, $(f \odot e)(n) = \sum_{d \mid n} f(d)$

$\mu = \{\mu(n)\}$, where $\mu(n) = \begin{cases} 1 & n = 1 \\ (-1)^r & n = p_1 p_2 \cdots p_r \\ 0 & n \text{ is not square-free} \end{cases}$

(4) *Möbius Inversion*: $f(n) = \sum_{d|n} g(d) \Longleftrightarrow g(n) = \sum_{d|n} \mu(\frac{n}{d}) f(d)$

(5) Euler Function: $\varphi = \{\varphi(n)\}$
$N = \{N(n)\} = \{1, 2, 3, \dots\}$
$N = \varphi \odot e$, i.e. $n = \sum_{d|n} \varphi(d)$
$\varphi = N \odot \mu$, i.e. $\varphi(n) = \sum_{d|n} \frac{n}{d}\mu(d)$

(6) $C_m(n) = \sharp$ cycles of length n over $[m]$
$L(p) = \sharp$ lines of length n with period p
$M(p) = \sharp$ cycles of length n with period p
$f(n) = \sharp$ lines of length n over $[m] = m^n$
Let's compute $C_m(n)$:

(1) $M(p)\cdot p = L(p),\ C_m(n) = \sum\limits_{d\ |\ n} M(p),\ f(n) = \sum\limits_{d\ |\ n} L(p),$ i.e. $f = L\odot e \Longrightarrow L = f\odot\mu \Longrightarrow C_m(n) = \sum\limits_{p|n}\frac{1}{p}\sum\limits_{d|p}\mu(\frac{p}{d})m^d$

(2) $C = M\odot e,\ f = L\odot e,\ L = NM,$

$\Longrightarrow NC = N(M\odot e) = (NM)\odot(Ne) = L\odot N = f\odot\mu N = f\odot\varphi$

$\Longrightarrow C_m(n) = \frac{1}{n}\sum\limits_{d\ |\ n}\varphi(\frac{n}{d})m^d$

Ex: prove $N(M\odot e) = (NM)\odot(Ne)$

E.g. $C_{10}(9) = \frac{1}{9}(\varphi(9)\cdot 10^1 + \varphi(3)\cdot 10^3 + \varphi(1)\cdot 10^9) = 111111340$

n-th cyclotomic polynomial:

$z^n = 1$, roots $z = \theta^0, \theta^1, \cdots, \theta^{n-1}$, θ^k is the primitive root if $(k,n) = 1$, then $\Phi_n(z) = \prod\limits_{\substack{1\ \le\ i\ \le\ n \\ (i,\ n)\ =\ 1}} (z-\theta^i)$ is the n-th cyclotomic polynomial.

Theorem 5. $z^n - 1 = \prod\limits_{d|n}\Phi_d(z)$

proof: $z^n - 1 = \prod\limits_{t=0}^{n-1}(z-\theta^t)$

if $(t,n) = d$, then $(\frac{t}{d}, \frac{n}{d}) = 1$

Let $t' = \frac{t}{d}, n' = \frac{n}{d}$, then $\theta^t = e^{\frac{2\pi i}{n}t} = e^{\frac{2\pi i}{n'}t'}$

$\Longrightarrow \theta^t$ is n'-th primitive root.

$\Longrightarrow z^n - 1 = \prod\limits_{d|n}\prod\limits_{\substack{t\ =\ 0 \\ (t,\ n)\ =\ d}}^{n-1}(z-\theta^t) = \prod\limits_{d|n}\Phi_{\frac{n}{d}}(z) = \prod\limits_{d|n}\Phi_d(z)$

□

Theorem 6. $\Phi_n(z) = \prod\limits_{d|n}(z^d-1)^{\mu(\frac{n}{d})}$

proof: $ln(z^n-1) = \sum\limits_{d|n} ln(\Phi_d(z))$

$\Longrightarrow ln(\Phi_n(z)) = \sum\limits_{d|n}\mu(\frac{n}{d})ln(z^d-1))$

$\Longrightarrow \Phi_n(z) = \prod\limits_{d|n}(z^d-1)^{\mu(\frac{n}{d})}$

□

Inversion Formula on Poset

Def: A partially ordered set(**poset**) $P = (X, \leq)$ is a set X with a relation "$\leq$" on X, s.t.

(1) Reflectivity: $x \leq x$;

(2) Antisymmetry: If $x \leq y$ and $y \leq x$, then $x = y$;

(3) Transitivity: If $x \leq y$ and $y \leq z$, then $x \leq z$.

E.g.

(1) $(\mathbb{Z}_{\geq 0}, <)$, with usual order.

(2) $(\mathbb{Z}_{>0}, \leq)$, divisibility relation, $a \leq b \Leftrightarrow a \mid b$.

(3) $(2^X, \leq)$, inclusion relation, $A \leq B \Leftrightarrow A \subseteq B$.

Def: A locally finite poset $[a, b] = \{z : a \leq z \leq b\}$

Def: $P = (X, \geq)$, locally finite, the incidence algebra of P is

$$\mathbb{A}(P) = \{f : P^2 \to \mathbb{R} | f(x, y) = 0, whenever\ x \nleq y\}$$

E.g.

(1) $0(x, y) = 0$.

(2) delta function: $\delta(x, y) = \left\{ \begin{array}{ll} 1, & x = y \\ 0, & x \neq y \end{array} \right.$.

(3) Zeta function: $\zeta(x, y) = \left\{ \begin{array}{ll} 1, & x \leq y \\ 0, & else \end{array} \right.$.

Facts:

(1) $f, g \in \mathbb{A}(P) \Rightarrow f + g \in \mathbb{A}(P)$.

(2) $f \in \mathbb{A}(P) \Rightarrow cf \in \mathbb{A}(P), \forall c \in \mathbb{R}$.

Def: Let $f, g \in \mathbb{A}(P)$, the Dedekind convolution of f and g is $f * g \in \mathbb{A}(P)$, where $(f * g)(x, y) = \sum_{z \,:\, x \leq z \leq y} f(x, z) g(z, y)$.

Fact:

(1) $*$ is non-commutative, associative, distributive.

(2) $\mathbb{A}(P), *, +, \cdot$ form an incidence algebra.

(3) $(f * 0)(x, y) = 0$.
$(f * \delta)(x, y) = f(x, y)\delta(y, y) = f(x, y) = (\delta * f)(x, y)$, so δ is the identity.
$(f * \zeta)(x, y) = \sum_{z \,:\, x \leq z \leq y} f(x, z)$

Def: If $f * g = \delta$, we say f is left-inverse of g
if $f * g_1 = \delta = g_2 * f$, then $g_1 = g_2$

Theorem 1. *$f \in \mathbb{A}(P)$, then f has a (left)right inverse $\Longleftrightarrow f(x, x) \neq 0$, $\forall x \in P$.*

proof:
"$\Rightarrow$": $\exists g \in \mathbb{A}(P)$, s.t. $f * g = \delta \Longrightarrow \delta(x, x) = f(x, x) g(x, x) = 1 \Longrightarrow f(x, x) \neq 0$
"$\Leftarrow$": Find $g \in \mathbb{A}(P)$, s.t. $f * g = \delta$.

$$\begin{cases} f(x, x) g(x, x) = \delta(x, x) = 1 & \Longrightarrow \quad g(x, x) = \frac{1}{f(x,x)}, \forall x \\ \sum\limits_{\substack{z \\ x \leq z \leq y}} f(x, z) g(z, y) = \delta(x, y) = 0 & \qquad x \neq y \end{cases}.$$

Then

$$f(x, x) g(x, y) + \sum_{\substack{z \\ x < z \leq y}} f(x, z) g(z, y) = 0,$$

i.e. $g(x, y) = -\frac{1}{f(x,x)} \left(\sum\limits_{\substack{z \\ x < z \leq y}} f(x, z) g(z, y) \right) = 0$, by recursion.

$\square$

Note: to compute left-inversr, $g(x,y) = -\frac{1}{f(y,y)} \left(\sum_{\substack{z \\ x \le z < y}} g(x,z) f(z,y) \right)$.

Def: *Möbius Function* over P is $\mu_P = \zeta^{-1}$, where

$$\mu_P(x,y) = \begin{cases} 1, & x = y \\ -\sum\limits_{x < z \le y} \mu_P(z,y) = -\sum\limits_{x \le z < y} \mu_P(x,z), & x < y \\ 0, & else \end{cases}.$$

<u>**Theorem**</u> **2.** ***(Inverse Formula I)*** *If P has a minimum element m(i.e. $m \le x$, $\forall x \in P$). Let f, g be functions $P \to \mathbb{R}$,then*

$$f(y) = \sum_{z \le y} g(z), \ \forall y \in P \iff g(y) = \sum_{z \le y} f(z) \mu_P(z,y), \ \forall y \in P$$

Note: m' is a minimal element of P if $\nexists x \in P$ s.t. $x \le m'$