Math 108 - Geometric Combinatorics Nadia Lafrenière

Möbius function & inversion 1/13/2022

Given a poset P, a (closed) interval $[s,t]$ is the induced subposet

$$\{u \mid u \geq s \text{ and } u \leq t\}.$$

A poset is said to be locally finite if all its intervals are finite.

E.g. $(\mathbb{N}, \leq)$ is an infinite, but locally finite poset.

All finite posets are locally finite.

Definition

Let P be a locally finite poset, and $\mathrm{Int}(P)$ the set of its intervals.

The incidence algebra of P $I(P)$ is the set of all functions $f: \mathrm{Int}(P) \to \mathbb{R}$ under the operations of

- addition

$$(f+g)\underbrace{(x,z)}_{\text{interval } [x,z]} = f(x,z) + g(x,z)$$

- scalar multiplication, with $c \in \mathbb{R}$

$$(c \cdot f)(x,z) = c(f(x,z)).$$

- convolution product

$$(f * g)(x,z) = \sum_{x \leq y \leq z} f(x,y)\, g(y,z).$$

Theorem

If P is a locally finite poset, $I(P)$ is an associative algebra.

The proof is straightforward and not very enlightning. However we should point out what the identity element is for the convolution:

$$\delta(x,z) = \begin{cases} 1 & \text{if } x = z \\ 0 & \text{otherwise.} \end{cases}$$

Proposition

Let $f \in I(P)$. The following conditions are equivalent:

(i) f has a left inverse

(ii) f has a right inverse

(iii) f has a two-sided inverse

(iv) $f(t,t) \neq 0 \quad \forall t \in P$.

Moreover, if f^{-1} exists, then $f^{-1}(s,t)$ depends only on $[s,t]$

Some elements of the incidence algebra

- The zeta function ζ, defined by

$$\zeta(t,u) = 1 \quad \text{for all } t \leq u \text{ in } P.$$

- ζ^2:

$$\zeta^2(s,u) = \sum_{s \leq t \leq u} 1 = \#[s,u]$$

- or more generally:

$$\zeta^k(s,u) = \sum_{s = s_0 \leq s_1 \leq \dots \leq s_{k-1} \leq s_k = u} 1$$

is the number of multichains (i.e. chains with repeated elements) from s to u.

- Similarly,

$$(\zeta - 1)(s,u) = \begin{cases} 1 & \text{if } u > s \\ 0 & \text{otherwise.} \end{cases}$$

- and

$$(\zeta - 1)^k(s,u)$$

is the number of (regular) chains of length k from s to u.

- Consider $2 - \zeta = 2\delta - \zeta$:

$$(2 - \zeta) = \begin{cases} 1 & \text{if } s = t \\ -1 & \text{if } s < t \end{cases}$$

By the proposition from last page, $2 - \zeta$ is invertible

Claim: $(2-\zeta)^{-1}$ is the total number of chains.

Sketch of proof: Let ℓ be the length of the longest chain in the interval $[s,u]$. Then, $(\zeta-1)^{\ell+1}(t,v)=0$ for all $s\le t\le v\le u$. Thus, we have

$$(2-\zeta)[1+(\zeta-1)+(\zeta-1)^2+\dots+(\zeta-1)^{\ell}](t,v)$$
$$=[1-(\zeta-1)][1+(\zeta-1)+(\zeta-1)^2+\dots+(\zeta-1)^{\ell}](t,v)$$
$$=[1-(\zeta-1)^{\ell+1}](t,v)=\delta(t,v).$$

Hence, $(2-\zeta)^{-1}=1+(\zeta-1)+\dots+(\zeta-1)^{\ell}$ is the total number of chains in the interval.

- eta function.

$$\eta(s,t)=\begin{cases}1 & \text{if } t \text{ covers } s\\ 0 & \text{otherwise.}\end{cases}$$

- and

$$(1-\eta)^{-1}(s,t)$$

is the number of maximal chains in the interval $[s,t]$.

Proof: exercise.

- Möbius function

The inverse of the zeta function is the Möbius function, defined as

$$\mu(s,t)=\begin{cases}1 & \text{if } s\le t\\ -\sum\limits_{s\le u<t}\mu(s,u), & \text{otherwise.}\end{cases}$$

If a poset has a $\hat{0}$, we also write $\mu(x)=\mu(\hat{0},x)$.

To be able to prove it, consider the following lemma.

Lemma

$$\sum_{x\le y\le z}\mu(x,y)=\delta_{x,z}.$$

Proof

By definition of μ, if $x=z$, then $\sum \mu(x,y) = \mu(x,x) = 1$.

Otherwise, $\sum_{x \le y \le z} \mu(x,y) = \sum_{x \le y < z} \mu(x,y) + \mu(x,z)$

$$= \sum_{x \le y < z} \mu(x,y) - \sum_{x \le y < z} \mu(x,y)$$

$$= 0.$$

Proof of the inverse

$$(\mu * \zeta)(x,z) = \sum_{x \le y \le z} \mu(x,y)\,\zeta(y,z) \overset{\text{by definition of } \zeta.}{=} \sum_{x \le y \le z} \mu(x,y) = \delta_{x,z}$$

Example

- Compute $\mu(x)$ for $x \in [n] = \{1,2,\dots,n\}$.

$$\mu(x) = \begin{cases} 1 & \text{if } x=1 \\ -1 & \text{if } x=2 \\ 0 & \text{otherwise} \end{cases}$$

Proposition

The Möbius function of any join irreducible element x in a lattice is $\mu(x)=0$ if x is not covering $\hat{0}$.

Proof

x is join irreducible iff it covers exactly one element y.

Then,

$$\mu(x) = \sum_{z<x} -\mu(z) = \left(\sum_{z<y} -\mu(z)\right) - \mu(y) = \left(\sum_{z<y} -\mu(z)\right) - \left(\sum_{z<y} -\mu(z)\right) = 0$$

- Compute $\mu(x)$ for $x \in 2^{[n]}$ (the boolean lattice).

$$\mu(x) = (-1)^{\#x} \quad (\text{here, } x \text{ is a subset of } 2^{[n]})$$

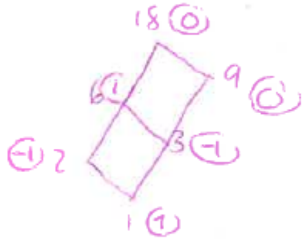
Proof

Recall that $\sum_{y \le x} \mu(y) = \delta_{\hat{0},x}$. This uniquely defines μ, so we only need to check that $\sum_{y \le x} (-1)^{\#y} = 0$ if $x \ne \hat{0}$:

$$\sum_{y \le x} (-1)^{\#y} = \sum_{k \le \#x} (-1)^k \binom{\#x}{k} = 0.$$

- Compute $\mu(x)$ for the divisors lattice.

(example: D_{18}, can we see a pattern?)



$$\mu(n) = \begin{cases} (-1)^m & \text{if } n \text{ is the product of } m \text{ distinct primes} \\ 0 & \text{otherwise.} \end{cases}$$

We prove only a part of it.

If n is the product of m distinct primes, we prove it by recurrence.

- If $n=1$, then $\mu(n)=1$.
- Otherwise, $\mu(n) = \sum_{d|n} \mu(d) \overset{(*)}{=} -\sum_{k<m} \binom{m}{k}(-1)^k = -\sum_{k\leq m} \binom{m}{k}(-1)^k + \binom{m}{m}(-1)^m = (-1)^m$;

where (*) is because every number is a product of k different primes, and by induction hypothesis.

Also, if n is a power of a prime number, let's say $n=p^k$, $k\geq 2$, then, p^k covers exactly one element and $\mu(p^k)$ thus vanishes.

The Möbius function appears a lot in number theory, where it has exactly the definition above. The Prime Number's Theorem can be restated as $\sum_{n=1}^{\infty} \frac{\mu(n)}{n} = 0$ (This is not obvious!)

Theorem (Möbius Inversion Theorem)

Let P be a finite poset, and $f, g: P \to \mathbb{R}$ be two functions.

Then,

(a) $f(x) = \sum_{y\geq x} g(y)$ for all $x\in P$ $\iff$ $g(x) = \sum_{y\geq x} \mu(x,y) f(y)$ for all $x\in P$.

(b) $f(x) = \sum_{y\leq x} g(y)$ for all $x\in P$ $\iff$ $g(x) = \sum_{y\leq x} \mu(y,x) f(y)$ for all $x\in P$.

Proof of (a) ($\Rightarrow$) (everything else is similar).

Assume $f(x) = \sum_{y \geq x} g(y)$ for all $x \in P$. Then,

$$\sum_{y \geq x} \mu(x,y) f(y) = \sum_{y \geq x} \mu(x,y) \sum_{z \geq y} g(z)$$
$$= \sum_{z \geq x} g(z) \sum_{x \leq y \leq z} \mu(x,y)$$
$$= \sum_{z \geq x} g(z)\, \delta_{x,z}$$
$$= g(x).$$

Application

Principle of Inclusion and Exclusion. (PIE)

Recall that, for the boolean lattice,

$$\mu(S) = \begin{cases} 1 & \text{if } \#S \text{ is even} \\ -1 & \text{if } \#S \text{ is odd.} \end{cases}$$

Theorem (PIE)

$$\Big|S - \bigcup_{i=1}^{n} S_i\Big| = |S| - \sum_{1 \leq i \leq n} |S_i| + \sum_{1 \leq i < j \leq n} |S_i \cap S_j| + \dots + (-1)^n |S_1 \cap S_2 \cap \dots \cap S_n|.$$

subsets of S

The proof is a little bit involved, but it works with

$$f(I) = \Big|\bigcap_{i \in I} S_i\Big| \text{ and } g(I) = \Big|\bigcap_{i \in I} S_i - \bigcup_{j \notin I} S_j\Big|$$ = elements in all S_i, $i \in I$, but in no other sets

$g(I) = \sum_{J \supseteq I} \mu(I,J) f(J)$, and $I = \emptyset$. It is also Theorem 5.5.7 in [AOC].

References: [AOC] Bruce E. SAGAN. Combinatorics, the art of counting. §5.4, 5.5, 5.8.

[EC1] Richard P. STANLEY. Enumerative Combinatorics, volume 1. §3.5 to 3.8