Möbius Function, Inversion, and Beyond

Beifang Chen

Department of Mathematics
Hong Kong University of Science and Technology
Clear Water Bay, Kowloon, Hong Kong

mabfchen@ust.hk,

Combinatorics Senimar

August 26, 2020

Outline

Möbius Function of Number Theory

- The Möbius function μ of number theory is defined as

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ (-1)^r & \text{if } n \text{ is a protuct of } r \text{ distinct primes,} \\ 0 & \text{otherwise.} \end{cases}$$

- Möbius inversion: Given two functions $f(n), g(n)$, where $n \in \mathbb{Z}_+$. The identity

$$g(n) = \sum_{d|n} f(d) = \sum_{ab=n} f(a), \quad \forall n \in \mathbb{Z}_+$$

holds if and only if

$$\begin{aligned} f(n) &= \sum_{d|n} \mu(d) g(n/d) \\ &= \sum_{ab=n} \mu(a) g(b), \quad \forall n \in \mathbb{Z}_+. \end{aligned}$$

Möbius function of number theory

- The Möbius function satisfies

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n > 1. \end{cases}$$

In other words, μ can be inductively defined by $\mu(1) = 1$,

$$\mu(n) = \sum_{d|n,\, d\neq n} \mu(d), \quad n \geq 2.$$

- Proof of the Möbius inversion:

$$\begin{aligned} \sum_{ab=n} \mu(a) g(b) &= \sum_{ab=n} \mu(a) \sum_{d|b} f(d) \\ &= \sum_{d|n} f(d) \sum_{a|\frac{n}{d}} \mu(a) \\ &= f(n). \end{aligned}$$

Möbius function of number theory

- Euler totient (phi) function $\phi(n) = |\{k \in [n] : \gcd(a, n) = 1\}|$. E.g., $\phi(10) = 4$, since $1, 3, 7, 9$ are the only numbers in $[10]$ coprime to 10.
- Fix an integer $n \geq 1$; the set $S_n = \{(a, b) : a \leq b, \gcd(a, b) = 1, b|n\}$ of positive integer ordered pairs has the cardinality

$$|S_n| = \sum_{b|n} \phi(b).$$

  The function $f : S_n \to [n], f(a, b) = an/b$, is a bijection. Injectivity is trivial. Surjectivity follows from $f(a, b) = k$ with $a = k/d$, $b = n/d$, $d = \gcd(k, n)$. So

$$n = \sum_{d|n} \phi(d).$$

- By the Möbius inversion,

$$\phi(n) = \sum_{d|n} \mu(d) n/d.$$

Möbius function of number theory

- Let M be an n-multiset of a k-set S of type $(n_1, \ldots, n_k)$, i.e., the first element of S appears n_1 times in M, the second element appears n_2 times in M, and so on. What is the number of circular permutations of M? That is, find the number of ways of arranging all members of M on a circle.

- The number of permutations of M is just the multinomial coefficient

$$\binom{n}{n_1, \ldots, n_k}.$$

- If m is the greatest common divisor of $n_1, \ldots, n_k$ above. Then the number of circular permutations of M is

$$\frac{1}{n} \sum_{d|m} \binom{n/d}{n_1/d, \ldots, n_k/d} \phi(d).$$

Möbius function of number theory

- The convolution of two functions f, g on $\mathbb{Z}_+$ is the function
$$f * g(n) = \sum_{ab=n} f(a)g(b), \quad n \in \mathbb{Z}_+.$$
- The sequence $\delta(n) := \delta_{1n}$ $(n \geq 1)$ is the identity of the convolution product:
$$\delta * f = f * \delta.$$
- A sequence $f(n)$ is invertible if and only if $f(1) \neq 0$. The inverse g of f can be inductively constructed as
$$g(1) = \frac{1}{f(1)},$$
$$\begin{aligned} g(n) : &= -\frac{1}{f(1)} \sum_{ab=n,\, b\neq n} f(a)g(b) \\ &= -\frac{1}{f(1)} \sum_{d|n,\, d\neq n} f(n/d)g(d), \quad n > 1. \end{aligned}$$

Möbius function of number theory

- The Möbius function μ is the inverse of the constant sequence
$$(1, 1, \ldots).$$
- Associated with a complex-valued sequence $f(n)$ $(n \geq 1)$ is the Dirichlet series (a complex function)
$$\widehat{f}(s) := \sum_{n=1}^{\infty} \frac{f(n)}{n^s}, \qquad s = \text{complex}.$$
- The Dirichlet series of the sequence $(1, 0, 0, \ldots)$ is the constant function
$$\widehat{\delta} \equiv 1.$$
- The Dirichlet series of the constant sequence $(1, 1, \ldots)$ is the Riemann zeta function
$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Möbius function of number theory

- The Dirichlet series of the convolution sequence $f * g$ is

$$
\begin{aligned}
\widehat{f * g}(s) &= \sum_{n=1}^{\infty} \frac{1}{n^s} \sum_{ab=n} f(a)g(b) \\
&= \sum_{n=1}^{\infty} \sum_{ab=n} \frac{f(a)}{a^s} \cdot \frac{g(b)}{b^s} \\
&= \left(\sum_{a=1}^{\infty} \frac{f(a)}{a^s} \right) \left(\sum_{b=1}^{\infty} \frac{f(b)}{b^s} \right) \\
&= \widehat{f}(s)\widehat{g}(s).
\end{aligned}
$$

- Dirichlet generating function of the Möbius function μ is related to the Riemann zeta function ζ as follow:

$$
\widehat{\mu}(s) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \frac{1}{\zeta(s)}.
$$

Möbius Function of Poset

Möbius function of poset

- The divisibility order of positive integers is crucial in the Möbius function and Möbius inversion of number theory.
- Let P be a partially ordered set (poset) with partial order $\leq$, i.e., (i) $x \leq x$ for all $x \in P$, (ii) if $x \leq y$ and $y \leq x$ then $x = y$, (iii) if $x \leq y$ and $y \leq z$ then $x \leq z$. We assume that P is locally finite, i.e., each interval $[x, y] := \{z \in P \mid x \leq z \leq y\}$ is finite.
- Let R be a commutative ring with the identity $1 \neq 0$ (the zero). The set $\mathcal{I}(P, R)$ of all functions from the set of all pairs (x, y) of P such that $x \leq y$ is an R-module by its usual addition and scalar multiplication, and is an algebra (call the incidence algebra) under the convolution

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

Möbius function of poset

- The identity of the incidence algebra $\mathcal{I}(P, R)$ is

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

- Given an incidence function $f \in \mathcal{I}(P, R)$. The following statements are equivalent: (1) f has a left inverse; (2) f has a right inverse; (3) $f(x, x)$ is invertible in R for all $x \in P$.
- The inverse g of an invertible $f \in \mathcal{I}(P, R)$ can be constructed as

$$g(x, x) = \frac{1}{f(x, x)},$$

$$\begin{aligned} g(x, y) :&= \frac{1}{f(y, y)} \sum_{x < z \leq y} f(x, z) g(z, y) \\ &= \frac{1}{f(x, x)} \sum_{x \leq z < y} g(x, z) f(z, y). \end{aligned}$$

Möbius function of poset

- Zeta function $\zeta \in \mathcal{I}(P, R)$ is the contant function $\zeta(x, y) = 1$ for all $x \leq y$. Its inverse μ is called the Möbius function of the poset P. So

$$\zeta * \mu = \mu * \zeta = \delta.$$

- The Möbius function of a poset P can be inductively given by

$$\mu(x, x) = 1,$$

$$\begin{aligned} \mu(x, y) : &= \sum_{x < z \leq y} \mu(z, y) \\ &= \sum_{x \leq z < y} \mu(x, z), \quad x < y. \end{aligned}$$

Möbius function of poset

- Inversion formulas:

$$g(x) = \sum_{a \le x,\, a \in P} f(a)\alpha(a,x) \;\Leftrightarrow\; f(x) = \sum_{a \le x,\, a \in P} g(a)\alpha^{-1}(a,x)$$

$$g(x) = \sum_{x \le a \in P} \alpha(x,a)f(a) \;\Leftrightarrow\; f(x) = \sum_{x \le a \in P} \alpha^{-1}(x,a)g(a)$$

- The Möbius inversion of poset:

$$g(x) = \sum_{a \le x} f(a) \;\Leftrightarrow\; f(x) = \sum_{a \le x} g(a)\mu(a,x)$$

$$g(x) = \sum_{x \le a} f(a) \;\Leftrightarrow\; f(x) = \sum_{x \le a} \mu(x,a)g(a)$$

- For the totally ordered set $\mathbb{Z}$ under its natural order of integers, its Möbius function is

$$\mu(a,b) = \begin{cases} 1 & \text{if } a = b, \\ -1 & \text{if } b = a+1, \\ 0 & \text{otherwise.} \end{cases}$$

- Let P_1, P_2 be posets with Möbius functions μ_1, μ_2 respectively. Then the product set $P := P_1 \times P_2$ is a poset whose partial order is

$$(x_1, x_2) \leq (y_1, y_2) \quad \text{if} \quad x_1 \leq y_1,\ x_2 \leq y_2,$$

and the Möbius function of P is given by

$$\mu\big((x_1, x_2), (y_1, y_2)\big) = \mu_1(x_1, y_1)\mu_2(x_2, y_2).$$

Möbius function of poset

- Let $\mathbb{P} = \{p_1, p_2, \ldots\}$ be the set of all primes. Each rational number q, when uniquely factorized into $q = p_{i_1}^{a_{i_1}} \cdots p_{i_k}^{a_{i_k}}$, can be considered as a function $a : \mathbb{Q} \to \mathbb{Z}$ with finite support. Then $\mathbb{Q}$ can be identified as the set $\mathbb{Z}^\infty$, whose members are integer-valued sequences $(a_1, a_2, \ldots)$ having the zero tail.
- The natural linear order on $\mathbb{Z}$ induces a product partial order on $\mathbb{Z}^\infty$, which imposes the divisibility partial order on $\mathbb{Q}$. The divisibility in $\mathbb{Q}$ is

$$q \mid r \;\Leftrightarrow\; r/q \in \mathbb{Z}_+.$$

There is an isomorphism $[q, r] \simeq [1, r/q]$ of divisibility intervals.

- Functions $f(n), n \in \mathbb{Z}_+$ can be identified to the incidence function

$$f(q, r) = f(r/q), \quad r/q \in \mathbb{Z}_+.$$

The convolution of sequences is isomorphic to the convolution of incidence functions.

Möbius function of poset

- For $q = p_1^{d_1} \cdots p_k^{d_k}, r = p_1^{e_1} \cdots p_k^{e_k} \in \mathbb{Q}$ such that $n := r/q \in \mathbb{Z}_+$,

$$\begin{aligned} \mu(n) &= \mu_{\mathbb{Q}}(q,r) = \mu_{\mathbb{Z}}(d_1,e_1)\cdots\mu_{\mathbb{Z}}(d_k,e_k) \\ &= \begin{cases} \prod_{i=1}^k (-1)^{e_i-d_i} & \text{if } e_i \le d_i+1, \\ 0 & \text{otherwise.} \end{cases} \\ &= \begin{cases} 1 & \text{if } n = 1, \\ (-1)^j & \text{if } n \text{ is a product of } j \text{ distinct primes,} \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$

- For $k \in \mathbb{Z}_+$, $(\zeta-\delta)^k(x,y) = \sum_{x=x_0<x_1<\cdots<x_k=y} 1$ is the number of chains of length k from x to y.

- The function $2\delta - \zeta$ is invertible, and $(2\delta-\zeta)^{-1}(x,y)$ is the total number of chains from x to y, since $(\delta-(\zeta-\delta))^{-1} = \sum_{k=1}^{\infty}(\zeta-\delta)^k$.

Möbius function on poset

- Theorem (Rota): Let P be a finite poset with the minimum element 0 and the maximum element 1. Let c_k be the number of chains $0 = x_0 < x_1 < \cdots < x_k = 1$ of length k from 0 and 1. Then

$$\mu_P(0,1) = c_0 - c_1 + c_2 - \cdots .$$

Proof: $\mu = \zeta^{-1} = (\delta + (\zeta - \delta))^{-1} = \sum_{k=0}^{|P|-1}(-1)^k(\zeta - \delta)^k$.

- A poset is lower graded if for each $x \in P$ all maximal chains of $[\cdot, x]$ have the same length.
- Each lower graded poset P has a rank function $r : P \to \mathbb{N}$ such that $r(x) = 0$ for each minimal element x, and $r(y) = r(x) + 1$ if y covers x (i.e., $\#[x, y] = 2$).
- Associate with a lower graded finite poset P with a minimum element $\hat{0}$ is Rota's characteristic polynomial

$$\chi(P,t) := \sum_{x \in P} \mu(\hat{0}, x)t^{n-r(x)}. \quad (1)$$

- The Möbius algebra $M(L,R)$ of a finite lattice L over a commutative ring R is the algebra generated by members of L, whose multiplication is induced by the meet operation $\wedge$, i.e.,

$$\left(\sum_{x\in L} a_x x\right)\left(\sum_{y\in L} a_y y\right) := \sum_{x,y\in L} a_x b_y (x\wedge y).$$

- For each $x \in L$, define

$$\sigma_x := \sum_{y\leq x} \mu(y,x) y$$

in $M(L,R)$. By the Möbius inversion,

$$x = \sum_{y\leq x} \sigma_y.$$

- This means that the collection $\{\sigma_x : x \in L\}$ forms a basis of the Möbius algebra $M(L,R)$.

Möbius function of poset

- The multiplication of the generators σ_x in the Möbius algebra $M(L,R)$ is given by

$$\sigma_x\sigma_y = \begin{cases} \sigma_x & \text{if } x = y, \\ 0 & \text{if } x \neq y. \end{cases}$$

- Proof: In the R-module $M(L,R)$ we define a new multiplication

$$\sigma_x \cdot \sigma_y := \delta_{xy}\sigma_x$$

through linear extension. Then

$$\begin{aligned} x \cdot y &= \left(\sum_{z \le x} \sigma_z\right) \cdot \left(\sum_{w \le y} \sigma_w\right) \\ &= \sum_{z \le x,\, w \le y} \sigma_z \cdot \sigma_w = \sum_{z \le x,\, z \le y} \sigma_z \\ &= \sum_{z \le x \wedge y} \sigma_z = x \wedge y = xy. \end{aligned}$$

- This means that the multiplications $\cdot$ and $\wedge$ are the same.

Möbius function of poset

- Weisner's Thm: Let L be a finite lattice with $\hat{0}, \hat{1}$. Let $a \in L$ with $a \neq \hat{1}$. Then
$$\sum_{x \wedge a = \hat{0}} \mu(x, \hat{1}) = 0.$$
- *Proof.* Consider the element $a \cdot \sigma_{\hat{1}} \in M(L, R)$. Since $a \neq \hat{1}$, we have
$$a \cdot \sigma_{\hat{1}} = \left(\sum_{x \leq a} \sigma_x \right) \cdot \sigma_{\hat{1}} = \sum_{x \leq a} \sigma_x \cdot \sigma_{\hat{1}} = 0$$
on the one hand. On the other hand,
$$\begin{aligned} a \cdot \sigma_{\hat{1}} &= a \cdot \left(\sum_{x \leq \hat{1}} \mu(x, \hat{1}) x \right) = \sum_{x \in L} \mu(x, \hat{1})(x \wedge a) \\ &= \sum_{y \in L} \sum_{x \wedge a = y} \mu(x, \hat{1}) y \end{aligned}$$
- It follows that $\sum_{x \wedge a = y} \mu(x, \hat{1}) = 0$ for $y \in L$. In particular, for $y = \hat{0}$.

Möbius function of poset

- Let $\mathbb{F}_q$ be a finite field of q elements and V a vector space over $\mathbb{F}_q$. Let $L(V)$ denote the lattice of all subspaces of V. The Möbius function $\mu_n := \mu(V_1, V_2)$ depends only on $n := \dim(V_2/V_1)$.
- Assume $n = \dim V$. Given a co-dimension 1 subspace H of V. The number of 1-dim subspaces that are not contained in H is

$$\frac{q^n - 1}{q - 1} - \frac{q^{n-1} - 1}{q - 1} = q^{n-1}.$$

Note that $\hat{0} = \{0\}$, $\hat{1} = V$. Let $a = H$. Then by Weisner's Thm

$$\sum_{x \wedge a = \hat{0}} \mu(x, \hat{1}) = \mu(\hat{0}, \hat{1}) + \sum_{\dim X = 1, X \cap H = \{0\}} \mu(X, \hat{1}) = 0.$$

Hence $\mu_n = \mu(\{0\}, V) = -q^{n-1}\mu_{n-1} \Rightarrow \mu_n = (-1)^n q^{n(n-1)/2}$.

Subspace Arrangment

- A hyperplane arrangement is a collection $\mathcal{A} := \{H_1, \ldots, H_m\}$ of some hyperplanes H_i of a vector space V.
- If $V = \mathbb{R}^n$ and m hyperplanes are in general position, then the number of regions divided by the m hyperplanes has the nice formula

$$\binom{m}{0} + \binom{m}{1} + \cdots + \binom{m}{n}.$$

- How about the situation when the hyperplanes are not in general position? If $V = \mathbb{C}^n$, what is the topological information of the complement

$$M(\mathcal{A}) := V \setminus \bigcup_{H \in \mathcal{A}} H,$$

which is a connected topological space?
- Many combinatorial problems can be formulated as counting or measuring the size of the complement of a hyperplane arrangement.

Subspace arrangement

- Graph coloring problem: How many ways to color vertices of a graph by t colors such that no two adjacent vertices receive the same color?
- Given a graph G having vertex set $\{1, 2, \ldots, n\}$. If the colors are indexed by real numbers, i.e., the color set is $\mathbb{R}$, then the set of all proper colorings is the complement of the hyperplanes

$$x_i - x_j = 0, \quad ij = \text{edge}.$$

The collection of such hyperplanes is known as graphical hyperplane arrangement $\mathcal{A}(G)$ of G.

- The number of proper colorings of a graph G with t colors, $\chi(G, t)$, is a polynomial function of t. In fact, choose an edge $e = ij$, then

$$\chi(G, t) = G(G \backslash e, t) - \chi(G/e, t),$$

where $G \backslash e$ and G/e are graphs obtained from G by deleting e and contracting e respectively.

Subspace arrangement

- Associated with a hyperplane arrangement $\mathcal{A} = \{H_1, \ldots, H_m\}$ is the characteristic polynomial

$$\chi(\mathcal{A}, t) := \sum_{X \in L(\mathcal{A})} \mu(X, V) t^{\dim X},$$

where $L(\mathcal{A})$ is the collection of all possible intersections $\cap_{i \in I} H_i \neq \emptyset$, including the whole space $V := \cap_{i \in \emptyset} H_i$, and μ is the Möbius function of the poset $L(\mathcal{A})$ whose partial order is the set inclusion.

- The polynomial $\chi(\mathcal{A}, t)$ is just the characteristic polynomial of the graded poset $L(\mathcal{A})$ whose partial order is the reverse of the set inclusion so that V is the minimum and $\mathrm{rank}(X) = \dim V - \dim X$.
- It turns out that for a graph G,

$$\chi(G, t) = \chi(\mathcal{A}(G), t).$$

Subspace arrangement

- Why the characteristic polynomial of a subspace arrangement is interesting and important? What is the meaning of such a polynomial?
- Fix a finite dimensional vector space V over a field $\mathbb{K}$. Consider the lattice $\mathcal{L}(V)$ of its all flats (affine subspaces) and the Boolean algebra $\mathcal{B}(V)$ generated by $\mathcal{L}(V)$. We want count (measure) the size of each member of $\mathcal{B}(V)$, satisfying certain obvious rules (common sense).
- Given a nonempty set S. A relative Boolean algebra is a class of some subsets of S, closed under set intersection, union, and relative complement, i.e., if $S_1, S_2 \in \mathscr{B}$, then $S_1 \cap S_2, S_1 \cup S_2, S_2 - S_1 \in \mathscr{B}$.
- The relative Boolean algebra $\mathscr{B}(\mathcal{C})$, generated by a class $\mathcal{C}$ of subsets of a set S, is the smallest relative Boolean algebra that contains $\mathcal{C}$.
- A class $\mathcal{I}$ of subsets of a set S is said to be intersectional if it is closed under set intersection.

Subspace arrangement

- A valuation (=finitely additive measure) on a relative Boolean algebra $\mathscr{B}$ of a set S is a function $\nu : \mathscr{B} \to A$, where A is an abelian group, such that for $S_1, S_2 \in \mathscr{B}$,

$$\nu(\emptyset) = 0,$$
$$\nu(S_1) + \nu(S_2) = \nu(S_1 \cap S_2) + \nu(S_1 \cup S_2).$$

- Groemer's Theorem: A set function $\nu : \mathcal{I} \to A$, where $\mathcal{I}$ is an intersectional class and A an abelian group, can be extended to a valuation on $\mathscr{B}(\mathcal{I})$ if and only if the Inclusion-Exclusion Formula

$$\nu(S_1 \cup \cdots \cup S_n) = \sum_{k=1}^{n} (-1)^{k-1} \sum_{i_1 < \cdots < i_k} \nu(S_{i_1} \cap \cdots \cap S_{i_k}),$$

is satisfied, where $S_1, \ldots, S_n \in \mathcal{I}$ and $S_1 \cup \cdots, S_n \in \mathcal{I}$.

- Given a relative Boolean algebra $\mathscr{B}$ on a set S. A function $f : S \to R$ is said to be $\mathscr{B}$-measurable if f has finitely many values and $f^{-1}(a) \in \mathscr{B}$ for each nonzero $a \in R$.

Subspace arrangement

- The integral of a $\mathscr{B}$-measurable function $f : S \to R$, with respect to a valuation $\nu : \mathscr{B} \to M$, is the sum

$$\int f \,\mathrm{d}\nu := \sum_{a \in R} a\, \nu(f^{-1}(a)),$$

  where $\mathscr{B}$ is a relative Boolean algebra and M is an R-module M.
- The class $\mathscr{L}(V)$ of all flats (=affine subspaces) of a vector space V over $\mathbb{K}$ is an intersectional class. The relative Boolean algebra $\mathscr{B}(V)$ generated by $\mathscr{L}(V)$ is just the Boolean algebra generated by $\mathscr{L}(V)$.
- Theorem (Ehrenborg and Readdy 1998). If $\mathbb{K}$ is an infinite field, then there exists a unique affine linear group invariant valuation $\nu : \mathscr{B}(V) \to \mathbb{Z}[t]$ such that for each flat W,

$$\nu(W) = t^{\dim W}.$$

- If $\mathcal{A}$ is an arrangement of affine subspaces of a vector space V over an infinite field $\mathbb{K}$, then the indicator function $1_{M(\mathcal{A})}$ of the complement $M(\mathcal{A})$ is $\mathscr{B}(V)$-measurable, and

$$\chi(\mathcal{A}, t) = \int 1_{M(\mathcal{A})} \mathrm{d}\nu.$$

- If $\mathbb{K} = \mathbb{R}$ and $\mathcal{A}$ is a hyperplane arrangement, then $M(\mathcal{A})$ is a disjoint union of some convex regions. However, the indicator function of each of these convex regions is *not* $\mathscr{B}(V)$-integrable.

- Zaslavsky's Formula: If $\mathcal{A}$ is a hyperplane arrangement in a real vector space V, then the number of regions of the complement $M(\mathcal{A})$ is

$$|\chi(\mathcal{A}, -1)|,$$

and the number of bounded regions (or regions bounded only by parallel hyperplanes) of $M(\mathcal{A})$ is

$$|\chi(\mathcal{A}, 1)|.$$

Subspace arrangement

- Given a subset arrangement $\mathcal{A} = \{S_1, \ldots, S_m\}$ of a nonempty set S. For each $X \in L(\mathcal{A})$, set

$$\mathring{X} := X - \bigcup_{Y \in L(\mathcal{A}),\, Y < X} Y.$$

- For each $X \in L(\mathcal{A})$,

$$X = \bigcup_{Y \in L(\mathcal{A}),\, Y \leq X} \mathring{Y} \quad \text{(disjoint)}.$$

In fact, it is clear that RHS is contained in LHS. For each $x \in X$, let $Y_1, \ldots, Y_k$ be all members of $L(\mathcal{A})$ that contains x. Then $Y := \bigcap_{i=1}^{k} Y_i$ is the smallest unique member of $L(\mathcal{A})$ such that $x \in Y$, i.e., $x \notin Z$ for $Z < Y$. By definition, $x \in \mathring{Y}$. Hence

$$1_X = \sum_{Y \leq X} \mathring{Y}.$$

Subspace arrangement

- By the Möbius inversion,

$$1_{\mathring{X}} = \sum_{Y \le X} \mu(Y, X) 1_Y. \tag{2}$$

In particular, if $X = V$, then $\mathring{V} = M(\mathcal{A})$. We thus have

$$1_{M(\mathcal{A})} = \sum_{Y \le V} \mu(Y, V) 1_Y. \tag{3}$$

- Apply the valuation ν to both sides of (3), we have

$$\nu(M(\mathcal{A})) = \sum_{Y \le V} \mu(Y, V) t^{\dim Y} = \chi(\mathcal{A}, t).$$

- Applying the Euler characteristic χ to (3),

$$\begin{aligned} \chi(\mathcal{A}, -1) &= \sum_{Y \le V} \mu(Y, V)(-1)^{\dim Y} = \chi(M(\mathcal{A})) \\ &= (-1)^{\dim V} \#\{\text{regions of } M(\mathcal{A})\}. \end{aligned}$$

Subspace arrangement

- There is another Euler characteristic $\bar{\chi}$, defined for each polyhedral set X of $\mathbb{R}^d$ as

$$\bar{\chi}(X) = \lim_{r\to\infty} \chi(X \cap B(o,r)),$$

where $B(o,r)$ is the closed ball in $\mathbb{R}^d$ of center o and radius r.

- For each relatively open convex set U,

$$\bar{\chi}(U) = \begin{cases} (-1)^{\dim P} & \text{if } U = K^\circ \oplus V, \\ 0 & \text{if } U = M \oplus L, \end{cases}$$

where K° is a bounded relatively open convex set, V is vector subspace, M is a manifold without boundary, and L is a half-line.

- If U is a bounded relatively open convex set, then

$$\bar{\chi}(U) = \chi(U) = (-1)^{\dim U}.$$

Subspace arrangement

- Apply the Euler characteristic $\bar{\chi}$ to both sides of (3), we have

$$\begin{aligned} \bar{\chi}(M(\mathcal{A})) &= \sum_{Y \le V} \mu(Y, V)\bar{\chi}(Y) \\ &= \sum_{Y \le V} \mu(Y, V) \cdot 1 \\ &= \chi(\mathcal{A}, 1). \end{aligned}$$

- Thus

$$\chi(\mathcal{A}, 1) = (-1)^d \#\{\text{bounded regions of } M(\mathcal{A})\}.$$

Characteristic Polynomial of Matroid

Characteristic polynomial of matroid

- A matroid is a system $M(E, \mathcal{I})$, where E is a finite set and $\mathcal{I}$ is a class of independent subsets of E satisfying the three properties:
  - $\varnothing \in \mathcal{I}$.
  - If $I \in \mathcal{I}$ and $I' \subseteq I$ then $I' \in \mathcal{I}$.
  - If $I_1, I_2 \in \mathcal{I}$ and $|I_1| < |I_2|$, then $\exists\ e \in I_2 - I_1$ such that $I_1 \cup e \in \mathcal{I}$.
- Dependant sets of E are subsets of E that are *not* independent.
- A circuit of M is a (set-inclusion) minimal dependent subset. A single element circuit is called a matroid loop.
- There exists a rank function $r : \mathcal{P}(E) \to \mathbb{Z}_{\geq 0}$ defined by

$$r(X) = \max\{|I| : I \subseteq X \text{ independent}\}.$$

- The characteristic polynomial of M is

$$\chi(M, t) = \sum_{X \subseteq E} (-1)^{|X|} t^{r(E) - r(X)}. \tag{4}$$

Characteristic polynomial of matroid

- There is a closure operator $\mathcal{P}(E) \to \mathcal{P}(E)$, $X \mapsto \bar{X}$, where

$$\bar{X} = X \cup \{e \in E : \exists \text{ circuit } C \text{ s.t. } e \in C \subseteq X \cup e\}.$$

- A flat of a matroid M is a subset $X \subseteq E$ such that $\bar{X} = X$. The class of flats of M forms a graded poset under set-inclusion:

$$\mathscr{L}(M) = \{\text{flats of } M\}.$$

- Rota's characteristic polynomial of the lattice $\mathscr{L}(M)$ of flats is

$$\chi(\mathscr{L}(M), t) = \sum_{F \in \mathscr{L}(M)} \mu(\bar{\varnothing}, F) t^{r(E)-r(F)}.$$

- The two characteristic polynomials of M are related by

$$\chi(\mathscr{L}(M), t) = \chi(M \setminus \bar{\varnothing}, t).$$

Characteristic polynomial of matroid

- Given a total order on the ground set E of a matroid M. A broken circuit M is a set of the form $C \setminus e$, where C is a circuit and e is the minimal element of C under the total order.
- Rota's Cross-cut Thm: For each flat F of M,

$$\mu(\bar{\varnothing}, F) = \sum_{\substack{S \subseteq F \setminus \bar{\varnothing} \\ r(S) = r(F)}} (-1)^{|S|} = (-1)^{r(F)} \#\{\text{NBC bases of } F\}.$$

- NBC Thm of Characteristic polynomial:

$$\chi(M \setminus \bar{\varnothing}, t) = \chi(\mathscr{L}(M), t) = \sum_{i=0}^{r(E)} (-1)^i c_i t^{r(E)-i},$$

where c_i is the number of i-subsets of E containing no broken circuit.
- The NBC thm does not need the total order.

Satisfiability of Boolean Functions

Satisfiability of Boolean function

- One can consider subspace arrangement over a finite field of q elements. For $q = 2$, we have $\mathbb{Z}/2\mathbb{Z} = \{0, 1\}$ with $1 + 1 = 0$. We adopt Boolean operations on $B = \{0, 1\}$.
- A literal is a bijection $x' : B \to B$, either the identity function x or its negation $\bar{x}$. Every Boolean function $f : B^n \to B$ has a disjunctive normal form

$$F(x_1, \ldots, x_n) = \bigvee_{i=1}^{m} G_i(x_1, \ldots, x_n),$$

  where $G_i = \wedge_{j \in J_i} x'_j$ are clauses with either $x'_j = x_j$ or $x'_j = \bar{x}_j$.
- A Boolean function F of n variables is said to be satisfied at $(a_1, \ldots, a_n) \in B^n$ if $F(a_1, \ldots, a_n) = 1$.
- The satisfiability problem is to verify (by certain algorithm) whether a Boolean function F is identically the constant function 1.

- The disjunctive normal form can be changed to the conjunctive normal form

$$f(x_1,\dots,x_n)=\bigwedge_{i=1}^{m} g_i(x_1,\dots,x_n)$$

with $f=\overline{F}$, $g_i=\overline{G}_i=\vee_{j\in J_i}x'_j$, $x'_j=x_j$ or $x'_j=\bar{x}_j$. Write $\vee$ as addition $+$ and *wedge* as multiplication. Then each $g_i(x_1,\dots,x_n)$ becomes

$$\sum_{j\in J_i} x'_j = a_{i1}x'_1+\cdots+a_{in}x'_n, \quad a_{ij}\in B.$$

- Consider the subspace (hyperplane) arrangement $\mathcal{A}=\{H_i : i=1,\dots,m\}$, where

$$H_i=\{x\in B^n : g_i(x)=0\}.$$

- The subspace arrangement $\mathcal{A}(F)$ has the characteristic polynomial

$$\chi(\mathcal{A}(F),t)=\sum_{X\in L(\mathcal{A})}\mu(X,B^n)t^{\dim X}.$$

Satisfiability of Boolean function

- (F is satisfied if there exists an instance of values such that F has value 1.) The Boolean formula F is satisfiable if and only if

$$\chi(\mathcal{A}(F), 2) = 0. \tag{5}$$

  The big problem is whether there exists a polynomial (of m and n) algorithm to check (5). This is equivalent to whether $P = NP$?

- Critical problem of Rota: Given a subspace arrangement $\mathcal{A}$ of a the vector space V over the finite field $\mathbb{F}_q$ of q elements. The critical exponent over $\mathbb{F}_q$ is

$$c(\mathcal{A}, q) := \min\{k \in \mathbb{Z}_+ : \chi(\mathcal{A}, q^k) \neq 0\}.$$

  The motivation is to find the chromatic number of the chromatic polynomial of a graph.

- This problem can be modified to any field or to lattice arrangements over $\mathbb{Z}$ or to subgroup arrangement.

Regular Cell Complexes

Simplicial Complex

- A simplicial complex K on a finite nonempty set V is a class K of nonempty finite subsets of V, satisfying
  (1) If $\{x\} \in K$ for each $x \in V$.
  (2) If $\sigma \in K$, then $\tau \in K$ for all nonempty $\tau \subseteq \sigma$.

  Set $\dim \sigma := |\sigma| - 1$ for $\sigma \in K$, and $\dim K = \max\{\dim \sigma : \sigma \in K\}$.
- The Euler number of a simplicial complex K is

$$\chi(K) = \sum_{i=0}^{\dim K} (-1)^i b_i = \sum_{i=0}^{\dim K} (-1)^i c_i,$$

  where $b_i = \mathrm{rank} H_i(K, \mathbb{Z})$ and $c_i =$ number of i-cells.
- Order complex of a finite poset P is the simplicial complex $\Delta(P)$, whose i-simplices are chains of P of length $i \geq 0$. Let $\hat{P}$ be the poset with a new minimum element $\hat{0}$ and a new maximum element $\hat{1}$ joined to P. Then

$$\mu_{\hat{P}}(\hat{0}, \hat{1}) = -1 + \chi(\Delta(P)) = \tilde{\chi}(\Delta(P)).$$

- The link of each $\sigma \in \Delta$ (simplicial complex) is the subcomplex

$$\mathrm{lk}(\Delta, \sigma) := \{\tau \in \Delta \mid \tau \cap \sigma = \emptyset, \tau \cup \sigma \in \Delta\}.$$

- If P is a finite poset and $x < y$ in P, then choose saturated chains

$$x_1 < x_2 < \cdots < x_i = x, \quad y = y_1 < y_2 < \cdots < y_j$$

  such that x_1 is a minimal element and y_j is a maximal element of P. Let $\sigma := \{x_1, \ldots, x_i, y_1, \ldots, y_j\}$. Then $\mathrm{lk}(\Delta P, \sigma)$ is the order complex of the open subposet $(x, y) := \{z \in P \mid x < z < y\}$, and

$$\mu(x, y) = \tilde{\chi}\big(\mathrm{lk}(\Delta P, \sigma)\big).$$

- Let X be a topological manifold with or without boundary with a finite triangulation Δ. Then $\Delta(X)$ is a graded poset.

Simplicial Complex

- Let K be a finite simplicial (or regular cell) complex such that $|K|$ is a manifold with or without boundary. Then for the poset $P = P(K)$,

$$\mu_{\widehat{P}}(\sigma,\tau) = \begin{cases} (-1)^{r(\tau)-r(\sigma)} & \text{if} \quad \hat{0} \le \sigma \le \tau \in K, \\ (-1)^{r(\tau)-r(\sigma)} & \text{if} \quad \sigma \in K - \partial K,\ \tau = \hat{1}, \\ (-1)^{r(\hat{1})-r(\sigma)}\beta & \text{if} \quad \sigma \in \partial K,\ \tau = \hat{1}, \end{cases}$$

  where $\widehat{P} = P \cup \{\hat{0}, \hat{1}\}$ with $\hat{0}, \hat{1} \notin P$.

- Manifold with boundary can be extended to stratified space, which is described by the Möbius function between strata. A general (non-pathological) topological space can be viewed as a stratified space by its intrinsic stratification.

- The idea can be developed into a theory on stratified posets, which is not yet explored. Posets of two strata was done.

Other Applications

Other aspects

- Poset of polyhedral cones: For polyhedral cones F, P such that F is a face of P,
$$\mu(F, P) = (-1)^{\dim P - \dim F}.$$
- Bruhat ordering on Weyl group W of a root system: For $x, y \in W$ with $x \leq y$,
$$\mu(x, y) = (-1)^{\ell(y) - \ell(x)}.$$
- Poset of Schubert cells of Grassmannian: Not yet computed myself.
- Poset of non-locally finite such as $\mathscr{L}(V)$, the poset of all subspaces of a vector space V over an infinite field $\mathbb{K}$. I only considered the cases of $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$.

Thank you!