Conjuntos parcialmente ordenados y retículos
Notas de Clase
Días de Combinatoria 2017

Rafael S. González D'León

18 de julio de 2017

Resumen

Notas de clase del minicurso de introducción a los conjuntos parcialmente ordenados y retículos. La mayor parte de estas notas está basada en la obra y notas de clase de Richard Stanley [2, Capítulo 3] y en el en el artículo de Federico Ardila [1, Sección 4] para la parte de conjuntos parcialmente ordenados; y en las notas de clase de Michelle Wachs [3] para la parte de topología de conjuntos parcialmente ordenados.

Índice

1. Conjuntos Parcialmente Ordenados

1.1. Definiciones básicas

Definición 1.1. Un conjunto parcialmente ordenado, también llamado *po-conjunto* o *poset* (por su nombre en inglés), es un par $(P, \leq)$ en donde P es un conjunto y $\leq$ es una *relación de orden*, o sea una relación binaria que es:

(I). (Reflexiva) Para todo $x \in P$ se tiene $x \leq x$.

(II). (Antisimétrica) Para $x, y \in P$ se tiene que $x \leq y$ y $y \leq x$ implica $x = y$.

(iii). (Transitiva) Para $x, y, z \in P$ se tiene que $x \leq y$ y $y \leq z$ implica $x \leq z$.

Uno de los ejemplos más simples que se puede dar de un conjunto parcialmente ordenado es el de una colección $\mathcal{C}$ de conjuntos relacionados por la relación de inclusión no estricta "$\subseteq$". En donde $A \subseteq B$ quiere decir que todo elemento de A es también un elemento de B. En esta relación tenemos que para todo conjunto A es cierto que $A \subseteq A$, verificando la relación reflexiva. Adicionalmente se verifican fácilmente la antisimetría ya que $A \subseteq B$ y $B \subseteq A$ implican que A y B tienen los mismos elementos (o sea $A = B$) y la transitividad ya que $A \subseteq B$ y $B \subseteq C$ claramente implican $A \subseteq C$. Nótese que en una clase de conjuntos $\mathcal{C}$ pueden existir dos conjuntos A y B para los cuales $A \nsubseteq B$ y $B \nsubseteq A$ y entonces A y B no están relacionados o son *incomparables*, de ahí el nombre de orden **parcial**. Un conjunto parcialmente ordenado P se se llama *orden total* o *cadena* si para cualquier par de elementos $x, y \in P$ tenemos que x y y son comparables, o sea $x \leq y$ o $y \leq x$.

Se usa frecuentemente la notación $x \leq_P y$ para aclarar que la relación de orden es la asociada a $(P, \leq)$. Cuando la relación de orden es clara en el contexto normalmente abusaremos de la notación y diremos que P es un poset sin hacer referencia a la relación de orden. También decimos que $x < y$ cuando $x \leq y$ pero $x \neq y$. Si $x \leq y$ en P y no existe un $z \in P$ tal que $x < z < y$ entonces diremos que y *cubre* a x y lo denotamos $x \lessdot y$.

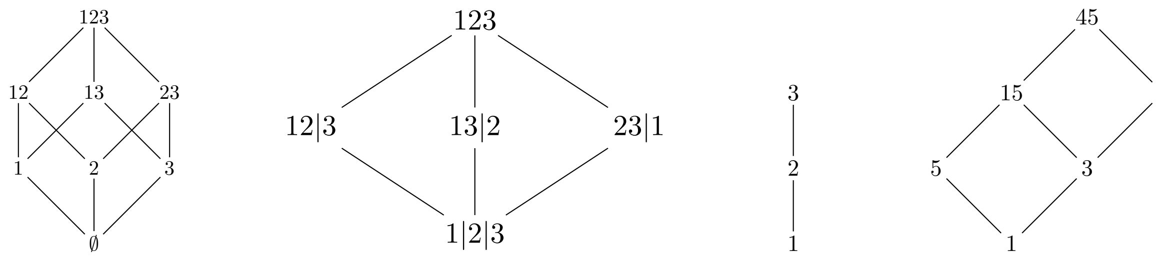
Ejemplo 1.2. Denotemos $\mathbb{B}_S$ al conjunto potencia (algunas veces se usa $\mathcal{P}([n])$ o $2^{[n]}$) de un conjunto S, es decir el conjunto de subconjuntos de S. En particular cuando $S = [n] := \{1, 2, \ldots, n\}$ denotamos $B_n := B_S$. Usando el mismo orden dado por inclusión descrito anteriormente podemos considerar $\mathbb{B}_n$ como un poset y llamaremos este poset *el álgebra de Boole sobre* $[n]$ o *el poset de subconjuntos de* $[n]$. El *diagrama de Hasse* de un poset P es un grafo dirigido cuyos vértices son los elementos de P y cuyas aristas dirigidas son las relaciones de cobertura en P. En la Figura 1a se ilustra el diagrama de Hasse de $\mathbb{B}_3$.

Ejemplo 1.3. Una *cadena* es un poset en donde sus elementos están totalmente ordenados. En particular los reales $\mathbb{R}$, los enteros $\mathbb{Z}$ y los naturales $\mathbb{N}$ forman una cadena de acuerdo a su orden usual. Estas cadenas son cadenas infinitas. Vamos a denotar $\mathbf{n}$ ó C_n a la cadena que sus elementos son $[n]$ y en donde $x \leq y$ en $\mathbf{n}$ de acuerdo al orden usual de los enteros. Llamamos $\mathbf{n}$ la *cadena de orden* n (o la *cadena de longitud* $n-1$, razón que es aparente en el diagrama de Hasse de la Figura 1c).

Ejemplo 1.4. El conjunto D_n de divisores enteros positivos del entero n puede considerarse como un poset con la relación de orden parcial dada por $x \leq y$ siempre que $x|y$ (x divida a y). D_n se es conocido como el *poset de divisibilidad de* n o el *poset de divisores de* n, ver la Figura 1d.

Ejemplo 1.5. Una partición de un conjunto S es una colección $\{B_1, B_2, \ldots, B_k\}$ de subconjuntos disjuntos (también llamados *bloques*) de S tal que su unión $\cup_{i=1}^k B_i = S$. Sea Π_n el conjunto de particiones de $[n]$ y para $\pi, \pi' \in \Pi_n$ decimos que π es un *refinamiento* de π' si para cada bloque $B \in \pi$ hay un bloque $B' \in \pi'$ tal que $B \subseteq B'$. Podemos verificar que Π_n tiene la estructura de poset con la relación dada por refinamiento, o sea, $\pi \leq \pi'$ siempre que π sea un refinamiento de π'. Llamamos a Π_n el *poset de particiones*. La Figura 1b ilustra el diagrama de Hasse de Π_3.

Observación 1.6. Si en la definición 1.1 la relación $\leq$ solamente satisface las propiedades (i) y (ii), el par $(P, \leq)$ es llamado un preorden o *preposet*. Si en un preposet consideramos la relación de equivalencia $x \sim y$ siempre que $x \leq y$ y $y \leq x$ en P, entonces $\leq$ induce un orden parcial en el conjunto de clases de equivalencia. En la Figure 2 se ilustra un ejemplo del diagrama de Hasse de las clases de equivalencia de un preposet sobre el conjunto $\{a, b, c, d, e, f, g, h\}$. En este caso tenemos por ejemplo que $b \leq c$ y $c \leq b$ pero $b \neq c$.



(a) $\mathbb{B}_3$ (b) Π_3 (c) C_3 (d) D_{45}

Figura 1: Ejemplos de posets

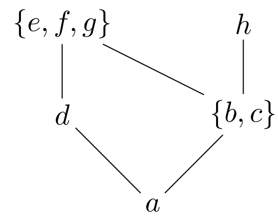


Figura 2: Diagrama de Hasse de un preposet

Observación 1.7. Decimos que un poset P es *finito* si $|P| < \infty$. En un poset finito es suficiente con describir las relaciones de cobertura para describir todo el poset (véase la Figura 1). Esto no es cierto para un poset infinito, por ejemplo en $\mathbb{R}$ con su relación de orden total clásica no existen relaciones de cobertura. En este minicurso trabajaremos con posets finitos a no ser de que se especifique lo contrario.

1.2. Mapas entre posets

Definición 1.8. Una *función monótona, preservante de orden, mapa de posets o morfismo de posets* es una función $f : P \to Q$ en donde P y Q son posets y siempre que $x \leq_P y$ tenemos que $f(x) \leq_Q f(y)$. Un *isomorfismo* entre los posets P y Q es una biyección monótona $f : P \to Q$ tal que su inversa $f^{-1} : Q \to P$ también es monótona. En el lenguaje de la teoría de categorías diríamos que un isomorfismo de posets es un isomorfismo en la categoría $\mathcal{P}oset$ formada por posets y funciones monótonas.

Definición 1.9. Para un poset P definimos su *poset dual* P^* como el poset formado por el mismo conjunto de elementos que P pero tal que $x \leq_{P^*} y$ si y solo si $y \leq_P x$. En el ejemplo de la Figura 3 están los diagramas de Hasse de un poset y su dual.

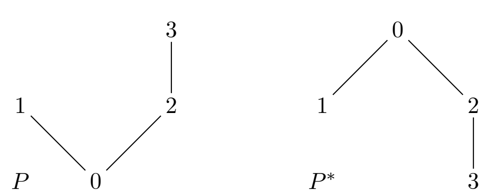


Figura 3: Un par de posets duales

Proposición 1.10. *El algebra de Boole $\mathbb{B}_n$ es auto-dual, es decir, $\mathbb{B}_n \cong \mathbb{B}_n^*$.*

Demostración. El mapa definido por $A \mapsto [n] \backslash A$ para cada $A \subseteq [n]$ es una biyección que claramente es monótona y su inversa es monótona, osea es un isomorfismo de posets. □

Ejemplo 1.11. Una *composición de n* es una sucesión finita de enteros positivos cuya suma es igual a n. Por ejemplo $(2, 1, 1, 3, 1)$ es una composición de 8. Denotemos $\mathbb{COMP}_n$ al conjunto de composiciones de n. Para $\nu, \mu \in \mathbb{COMP}_n$ definimos la relación de cobertura $\nu \lessdot \mu$ si μ puede ser obtenido de ν sumando entradas adyacentes, por ejemplo $(2, 1, 1, 3, 1) \lessdot (2, 1, 4, 1)$.

Proposición 1.12. *Tenemos que $\mathbb{COMP}_n \cong \mathbb{B}_{n-1}$.*

Demostración. Sea $f : \mathbb{COMP}_n \to \mathbb{B}_{n-1}^*$ la función definida por $f(\mu) = \{\mu_1, \mu_1 + \mu_2, \mu_1 + \mu_2 + \mu_3, \ldots, \mu_1 + \mu_2 + \cdots + \mu_{|\mu|-1}\}$ en donde $|\mu|$ es el número de elementos en μ.

- f **es una biyección:** f tiene una inversa $f^{-1} : \mathbb{B}_{n-1}^* \to \mathbb{COMP}_n$ definida $f^{-1}(A) = (a_1, a_2 - a_1, a_3 - a_2, \ldots, a_{|A|} - a_{|A|-1}, n - a_{|A|})$ para $A = \{a_1 < a_2 < \cdots < a_{|A|}\}$.
- f **es monótona:** Sea $\mu \lessdot \nu$, para algún $r \in [|\mu| - 1]$ tenemos que $\nu_i = \mu_i$ siempre que $i < r$, $\nu_r = \mu_r + \mu_{r+1}$ y $\nu_i = \mu_{i+1}$ siempre que $i > r$. Entonces $\sum_{j=1}^{i} \nu_j = \sum_{j=1}^{i} \mu_j$ cuando $i < r$, y $\sum_{j=1}^{i} \nu_j = \sum_{j=1}^{i+1} \mu_j$ cuando $i \geq r$ y entonces $f(\mu) \supseteq f(\nu)$. Como estamos trabajando con posets finitos solo tenemos que chequear que f es monótona en relaciones de cobertura ya que a la conclusión se llega por inducción.
- f^{-1} **es monótona:** Sea $A = \{a_1 < a_2 < \cdots < a_{|A|}\} \supseteq B = \{a_1 < a_2 < \cdots < \widehat{a_r} < \cdots < a_{|A|}\}$ una relación de cobertura en $\mathbb{B}_{n-1}^*$, en donde $\widehat{a_r}$ indica que el elemento a_r lo hemos removido de A. Entonces por definición tenemos que $f^{-1}(B)_i = f^{-1}(A)_i$ para $i < r$, $f^{-1}(B)_r = a_{r+1} - a_{r-1} = a_{r+1} - a_r + a_r - a_{r-1} = f^{-1}(A)_r + f^{-1}(A)_{r+1}$ y $f^{-1}(B)_i = f^{-1}(A)_{i+1}$ para $i > r$. □

Proposición 1.13. *Si $f : P \to P$ es una biyección monótona y P es un poset finito entonces f es un automorfismo de posets.*

Demostración. Si f es el mapa identidad entonces la conclusión es trivial, en cualquier otro caso como f es una biyección sobre el mismo conjunto entonces es una permutación de P. Como P es finito entonces f tiene orden finito en el grupo permutaciones de P, osea para algún $k > 1$ tenemos que $f^k = Id$. Tenemos entonces que $f^{-1} = f^{k-1}$ es un mapa monótono ya que la composición de mapas monótonos es un mapa monótono. □

Ejemplo 1.14. La conclusión de la Proposición 1.13 no se cumple cuando P no es finito. Consideremos por ejemplo el poset infinito P de la Figura 4 y el mapa $f : P \to P$ dado por $f(i) = i$ y $f(i') = (i + 1)'$ para todo $i \in \mathbb{Z}$. Este mapa es una biyección monótona pero su inversa no es monótona.

Definición 1.15. A un poset Q lo llamamos *subposet en el sentido débil* de un poset P si $Q \subseteq P$ como conjuntos y para cada $x, y \in Q$ tenemos que $x \leq_Q y$ implica que $x \leq_P y$, en otras palabras, el mapa de inclusión $Q \hookrightarrow P$ es un mapa de posets. Si $Q = P$ como conjuntos entonces decimos que P es un *refinamiento* de Q. Decimos que Q es un *subposet (inducido)* de P si $Q \subseteq P$ como conjuntos y para $x, y \in Q$ tenemos que $x \leq_Q y$ si y solo si $x \leq_P y$. En otras palabras, un subposet de P se obtiene al tomar un subconjunto Q de P junto con todas las relaciones que tienen los elementos de Q en P.

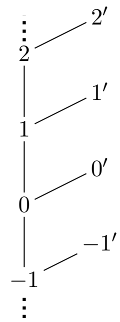


Figura 4

Dos ejemplos particulares de subposets son los invervalos cerrados $[x, y] := \{z \in P \mid x \leq z \leq y\}$ y los intervalos abiertos $(x, y) := \{z \in P \mid x < z < y\}$. De un poset en el cual todo intervalo es finito se dice que es *localmente finito*. Por ejemplo la cadena infinita $\mathbb{Z}$ de enteros con su orden natural es localmente finita. Las cadenas de subposet P son todos los subposets de P cuyo orden inducido sea total. Una cadena $C \subseteq P$ es *saturada* si no hay un $z \in P \setminus C$ tal que $x < z < y$ para todo par de elementos $x, y \in C$ tal que $C \cup \{z\}$ es también una cadena. Una cadena es *máxima* si no hay un $z \in P \setminus C$ tal que $C \cup \{z\}$ sea también una cadena. La *longitud* de un poset se define como $\ell(P) := \{|C| \mid C \subseteq P \text{ es una cadena}\}$. A un poset se le llama *puro, graduado o ranqueado* si todas las cadenas maximas tienen la misma longitud. A un elemento $x \in P$ se le llama *minimal* (*maximal*) si no hay un elemento $z \in P$ tal que $z < x$ ($z > x$). Denotaremos $\mathcal{M}in(P)$ ($\mathcal{M}ax(P)$) al conjunto de elementos minimales (maximales) de P.

Proposición 1.16. *Si P es un poset finito graduado entonces existe una función bien definida $\rho : P \to \mathbb{N}_0$ (llamada* función de grado*) tal que $\rho(x) = 0$ siempre que $x \in \mathcal{M}in(P)$ y si $x \lessdot y$ entonces $\rho(y) = \rho(x) + 1$.*

Cuando P es graduado con función de grados ρ decimos que el *grado* de un elemento x es $\rho(x)$. La *función generadora por grados* de P es el polinomio

$$F(P, t) := \sum_{x \in P} t^{\rho(x)} = \sum_{k=0}^{\ell(P)} W(P, k) t^k,$$

en donde

$$W(P, k) := \sum_{\substack{x \in P \\ \rho(x) = k}} 1$$

se llaman los *números de Whitney del segundo tipo.*

Ejemplo 1.17. (a) $F(C_n, t) = 1 + t + \cdots + t^n = \dfrac{1 - t^{n+1}}{1 - t} = [n + 1]_t$.

(b) $F(\mathbb{B}_n, t) = (1 + t)^n$.

(c) $F(\Pi_n, t) = \sum_{k=0}^{n-1} S(n, n - k) t^k$ en donde $S(n, k)$ es el número de particiones de $[n]$ en exactamente k bloques, también conocidos como *números de Stirling del segundo tipo.*

1.3. Construcciones y operaciones entre posets

Definición 1.18. Entre posets P y Q también tenemos las siguientes operaciones

(I) (Union disjunta) La *union disjunta o suma directa* $P+Q$ se define como el poset cuyo conjunto de elementos es $P \sqcup Q$ y cuya relación de orden está dada por $x \leq_{P+Q} y$ si y solo si $x \leq_P y$ o $x \leq_Q y$.

(II) (Producto directo) El *producto directo o producto cartesiano* $P \times Q$ es el poset cuyo conjunto de elementos es $P \times Q$ y cuya relación de orden esta dada por $(x, x') \leq_{P \times Q} (y, y')$ si y solo si $x \leq_P y$ y $x' \leq_Q y'$.

(III) (Sum ordinal) La *suma ordinal* $P \oplus Q$ es el poset en $P \sqcup Q$ cuya relación de orden esta dada por $x \leq_{P \oplus Q} y$ si y solo si $x \leq_P y$, $x \leq_Q y$ ó $x \in P$ y $y \in Q$.

(IV) (Producto ordinal) El *producto ordinal o producto diccionario* $P \otimes Q$ es el poset con elementos $P \times Q$ y cuya relación de orden está dada por $(x, x') \leq_{P \times Q} (y, y')$ si y solo si $x \leq_P y$ ó $x = y$ y $x' \leq_Q y'$.

(V) (Potencia) Denotamos Q^P al poset formado por todos los mapas monótonos $f : P \to Q$ con relación de orden dada por $f \leq g$ para $f, g \in Q^P$ si $f(t) \leq g(t)$ para todo $t \in P$.

2. Retículos

2.1. Definiciones básicas

Sea P un poset. Para un subconjunto $A \subseteq P$ decimos que $u \in P$ es una *cota superior* de A si $u \geq x$ para todo $x \in A$. A u le llamamos *cota superior mínima, supremo o juntura* (en inglés se usa comúnmente la palabra “join”) de los elementos de A si para cualquier otra cota superior z se cumple que $z \geq u$. De la misma manera definimos el concepto de *cota inferior* de A como un elemento $l \in P$ tal que $l \leq x$ para todo $x \in A$ y a l le llamamos *cota inferior máxima, infimo o concurrencia* (en inglés se usa comúnmente la palabra “meet”) si cualquier otra cota inferior z cumple que $z \leq l$. Usaremos la notación $\vee A$ y $\wedge A$ para la juntura y concurrencia de A respectivemente siempre que existan, y cuando $A = \{x, y\}$ tenga solo dos elementos usaremos la notación $x \vee y$ y $x \wedge y$. En el poset de la Figura 5 tenemos que $y \vee w = r$ pero el conjunto $\{y, w\}$ no tiene una concurrencia ya que x y z son ambos cotas inferiores de $\{y, w\}$ pero x y z son incomparables. En un poset P denotamos $\hat{1} = \wedge P$ y $\hat{0} = \vee P$ en caso de que estos elementos existan y los llamamos respectivamente elementos *tope* y *base*. A un poset que tenga ambos, un elemento tope y un elemento base, le llamamos *acotado*.

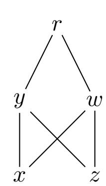


Figura 5

Definición 2.1. Un *retículo* es un poset L en el cuál todo par de elementos $x, y \in P$ tiene una juntura $x \vee y$ y una concurrencia $x \wedge y$.

Ejemplo 2.2. (a) $\mathbb{N}$ es un retículo en el cuál $x \wedge y = \min\{x, y\}$ y $x \vee y = \max\{x, y\}$.

(b) $\mathbb{B}_n$ es un retículo en el cuál $A \wedge B = A \cap B$ y $A \vee B = A \cup B$.

(c) Π_n es un retículo en donde $\pi \wedge \pi' = \{B \cap B' \mid B \in \pi, B' \in \pi'\}$ y $\pi \vee \pi'$ es la partición más fina con la propiedad de que si $B \in \pi$ y $B' \in \pi'$ tienen una intersección no vacía $B \cap B' \neq \emptyset$ entonces ambos $B \subseteq X$ y $B' \subseteq X$ para algún bloque $X \in \pi \vee \pi'$.

(d) D_n es un retículo en el cuál $x \wedge y = \gcd(x, y)$ y $x \vee y = \operatorname{lcm}(x, y)$.

Definición 2.3. A un poset P se le conoce como *semiretículo por concurrencia* (*semiretículo por juntura*) si todo par de elementos en P tiene un ínfimo (supremo).

Proposición 2.4. *Un semiretículo por concurrencia finito con un $\hat{1}$ es un retículo.*

Demostración. Para mostrar que cada par de elementos $x, y \in P$ tienen también una juntura en P consideremos el conjunto

$$A = \{z \in P \mid z \geq x \text{ y } z \geq y\}$$

(nótese que $|A| < \infty$). Entonces $l := \bigwedge_{a \in A} a$ es una cota superior mínima para x y y. □

Observación 2.5. La Proposición 2.4 falla cuando P no es finito, considerese por ejemplo el poset $\{\hat{0}\} \oplus (C_0 + C_0) \oplus \mathbb{N}^*$.

Ejemplo 2.6. El poset $\mathbb{B}_{\leq k}$ formado por los subconjuntos de $[n]$ de cardinalidad a lo sumo k o exactamente n es un retículo.

2.2. Retículos distribuídos

Definición 2.7. Un retículo L se dice que es *distributivo* si satisface las leyes distributivas:

(D1) $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$ para todo $x, y, x \in L$.

(D2) $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ para todo $x, y, x \in L$.

Observación 2.8. Un retículo satisface la propiedad (D1) si y sólo si satisface la propiedad (D2).

Ejemplo 2.9. Las operaciones sobre conjuntos $\wedge = \cap$ y $\vee = \cup$ cumplen con las propiedades (D1) y (D2) entonces $\mathbb{B}_n$ es un retículo distributivo.

Un *ideal de orden (inferior)* I es un subconjunto de P tal que si $x \in I$ y $z \leq x$ entonces $z \in I$. Similarmente un *ideal de orden superior o filtro* U es un subconjunto de P tal que si $x \in I$ y $x \leq z$ entonces $z \in I$. Como estamos trabajando con posets finitos, podemos caracterizar un ideal de orden I por su conjunto de elementos maximales $\max I$. Nótese que todo par de elementos en $\max I$ es incomparable, un conjunto con esta propiedad se conoce como una *anticadena*. Cómo cada anticadena también describe un ideal de orden entonces hay una biyección entre anticadenas de P e ideales de orden de P. Para un subconjunto $A \subseteq P$ denotamos $I(A) := \{z \in P \mid z \leq x \text{ para algún } x \in A\}$ el ideal de orden generado por A y si $|A| = 1$ este ideal se le llama *principal*. El conjunto $J(P)$ de ideales de orden de P tiene la estructura de un poset cuando consideramos la relación de inclusión (ver la Figura 6).

Proposición 2.10. *Sea P un poset finito, entonces $J(P)$ es un retículo distributivo.*

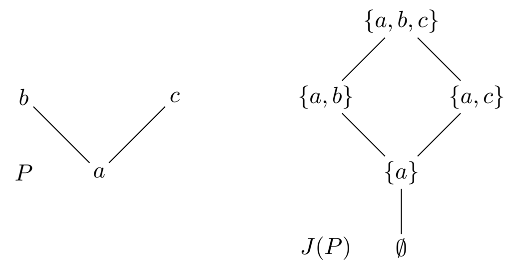


Figura 6

Demostración. Nótese que siempre que I e I' son ideales de orden en $J(P)$ entonces $I \cap I'$ e $I \cup I'$ también lo son. Entonces $J(P)$ es un subposet del álgebra de Boole B_P en los elementos de P cerrado al tomar uniones e intersecciones (también llamado *subretículo*). Y sabemos que uniones e intersecciones en B_P satisfacen (D1) y (D2). $\square$

Observación 2.11. Nótese que si P es un poset con n elementos, entonces $J(P)$ es graduado de grado n.

Definición 2.12. A un elemento $x \neq \hat{0}$ de un retículo L le llamamos *irreducible (con respecto a juntura)* si $x = a \vee b$ implica que $a = x$ o $b = x$, es decir, x no se puede expresar como la juntura de dos elementos estrictamente menores.

Lema 2.13. *Si $x \in L$ es irreducible entonces cubre exactamente un elemento de L.*

Proposición 2.14. *Sea P un poset finito. El subposet de $J(P)$ formado por los elementos irreducibles es isomorfo a P.*

Demostración. Sea $I \in J(P)$ irreducible. Gracias al Lema 2.13 sabemos que I cubre exactamente un elemento, y esto es verdad si y solo si $I = I(x)$ es un ideal de orden principal, en donde $x \in P$. Tenemos entonces una biyección entre los elementos $x \in P$ y los irreducibles (ideales de orden principales) $I(x) \in J(P)$. Adicionalmente $I(x) \subseteq I(y)$ si y solo si $x \leq y$. $\square$

Teorema 2.15 (Teorema Fundamental de los Retículos finitos distribuidos)**.** *Sea L un retículo finito distribuido. Entonces existe un único poset finito (salvo isomorfismo) P tal que $L \cong J(P)$.*

Sketch de la demostración. Sea P el subposet formado por los irreducibles de L, queremos mostrar que $L \cong J(P)$. Para esto consideramos la función $\psi : L \to J(P)$ que para cada $x \in L$ esta dada por

$$\psi(x) = \{z \in P \mid z \leq x\}.$$

Esta función es claramente monótona y cuenta con una inversa dada por

$$\phi(I) = \bigvee_{z \in I} z$$

que es también claramente monótona. $\square$

2.3. Retículos geométricos

Definición 2.16. A un retículo graduado L se le llama *semimodular (superior)* si su función de grados ρ cumple que

$$\rho(x) + \rho(y) \geq \rho(x \wedge y) + \rho(x \vee y) \quad \forall x, y \in L. \tag{2.1}$$

El concepto de *semimodular inferior* se define de manera similar cambiando la dirección de la inigualdad y decimos que$L$ es modular cuando la relación es dada por la igualdad.

Proposición 2.17. *Sea L un retículo finito. Las siguientes condiciones son equivalentes:*

(I) *L es graduado y su función de grados satisface la ecuación 2.1.*

(II) *Para todo $x, y \in L$ si x cubre $x \wedge y$ entonces $x \vee y$ cubre y.*

(III) *Para todo $x, y \in L$ si x y y ambos cubren $x \wedge y$ entonces $x \vee y$ cubre ambos x y y.*

Demostración. Probamos primero $(i) \Rightarrow (ii)$. Podemos reescribir 2.1 de la siguiente manera:

$$\rho(x) - \rho(x \wedge y) \geq +\rho(x \vee y) - \rho(y).$$

Si $x \gtrdot x \wedge y$ entonces $\rho(x) - \rho(x \wedge y) = 1$ y por consiguiente $\rho(x \vee y) - \rho(y)$ puede ser solamente 0 ó 1. Si este valor fuera 0 entonces $\rho(x \vee y) = \rho(y)$ lo que implicaría que $x \leq y$ y $x = x \wedge y$, una contradicción. Entonces $\rho(x \vee y) - \rho(y) = 1$ lo que implica que $x \vee y \gtrdot y$.

Como (iii) se desprende fácilmente de (ii) nos queda únicamente por mostrar que $(iii) \Rightarrow (i)$. Demostraremos primero que L es graduado. Supongamos que no y escojamos un intervalo $[x, y]$ de longitud mínima en L que no sea graduado. Entonces tienen que existir dos elementos $z, w \in [x, y]$ y enteros positivos $\ell_1 \neq \ell_2$ tal que $x \lessdot z$, $x \lessdot w$ y que toda cadena máxima en $[z, y]$ sea de longitud ℓ_1 y toda cadena máxima en $[w, y]$ sea de longitud ℓ_2. Pero (iii) nos dice que $z \vee w$ cubre ambos z y w implicando que toda cadena saturada de la forma $z \vee w = t_0 \lessdot t_1 \lessdot \cdots \lessdot t_k = y$ tiene ambas longitudes $\ell_1 - 1$ y $\ell_2 - 1$, una contradicción. Así que L tiene que ser graduado.

Ahora, asumamos que L falla en satisfacer la ecuación 2.1 y escojamos un par x, y tal que

$$\rho(x) + \rho(y) < \rho(x \wedge y) + \rho(x \vee y)$$

con las propiedades de que el intervalo $[x \wedge y, x \vee y]$ sea de longitud mínima y la cantidad $\rho(x) + \rho(y)$ sea mínima. Nótese que ambos x y y no pueden cubrir $x \wedge y$ al mismo tiempo ya que por (iii) $\rho(x) + \rho(y) = \rho(x \wedge y) + \rho(x \vee y)$, que sería una contradicción. Entonces asumamos sin pérdida de generalidad que hay un elemento x' tal que $x \wedge y < x' < x$.

Por la minimalidad de $\ell(x \wedge y, x \vee y)$ y $\rho(x) + \rho(y)$ tenemos que

$$\rho(x') + \rho(y) \geq \rho(x' \wedge y) + \rho(x' \vee y).$$

y como $x \wedge y = x' \wedge y$ concluimos de las dos inigualdades que

$$\rho(x) + \rho(x' \vee y) < \rho(x') + \rho(x \vee y).$$

Como $x \vee (x' \vee y) = x \vee y$ y $x \wedge (x' \vee y) \geq x'$ tenemos que el par $x, x' \vee y$ satisface

$$\rho(x) + \rho(x' \vee y) < \rho(x \wedge (x' \vee y)) + \rho(x \vee (x' \vee y))$$

y $\ell(x \wedge (x' \vee y), x \vee y(x' \vee y)) < \ell(x \wedge y, x \vee y)$, que es una contradicción. $\square$

Proposición 2.18. *Un retículo finito L es modular si y solo si cumple:*

$$\forall x, y, z \in L \text{ tal que } x \leq z, \text{ tenemos } x \vee (y \wedge z) = (x \vee y) \wedge z. \tag{2.2}$$

Observación 2.19. Es un corolario de la Proposición 2.18 que todo retículo finito distribuido es también modular. En la Figura 7 se muestra un ejemplo de un retículo que es semimodular pero no es modular.

Ejemplo 2.20. El álgebra de Boole $\mathbb{B}_n$ es un ejemplo de un retículo modular ya que para todo par de conjuntos A y B se tiene que

$$|A| + |B| = |A \cup B| + |A \cap B|.$$

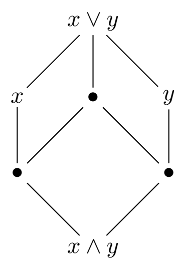


Figura 7

Definición 2.21. En un poset P con $\hat{0}$ llamamos *átomo* a un elemento a que cubre al $\hat{0}$. Decimos que un retículo L es *atómico* si todo elemento $x \in L$ se puede expresar como una juntura $x = \bigvee_{a \in A'} a$ en donde A' es un conjunto de átomos. Un retículo atómico semimodular finito se conoce como un *retículo geométrico*.

Observación 2.22. La razón detrás del nombre retículo geométrico es que estos precisamente son los retículos de conjuntos cerrados de matroides simples (también conocidas como geometrías combinatorias).

Ejemplo 2.23. $\mathbb{B}_n$ es atómico y modular así que también es geométrico.

Proposición 2.24. *Un retículo finito L es geometrico si y solo si satisface la siguiente condición:*

$$x \lessdot y \iff \exists\, a \gtrdot \hat{0} \text{ tal que } y = x \vee a. \tag{2.3}$$

Ejemplo 2.25. En Π_n un átomo es una partición que contiene exactamente un solo bloque que no es singulete con dos elementos. Para cada relación de cobertura $\pi \lessdot \pi'$ en Π_n podemos considerar los dos bloques $B_1, B_2 \in \pi$ que se combinan en un solo bloque en π'. Seleccionemos cualesquier elementos $x \in B_1$ y $y \in B_2$ y llamemos $a_{x,y}$ al átomo cuyo solo bloque que no es singulete es $\{x, y\}$. Es fácil de chequear que $\pi' = \pi \vee a_{x,y}$. Entonces por la Proposición 2.24 concluimos que Π_n is geométrico. Nótese que esto en particular implica que Π_n es a la vez semimodular y atómico.

3. Álgebras de incidencia y la función de Möbius

3.1. Álgebras de incidencia

Sea $\mathbf{k}$ un campo. En esta Sección estaremos trabajando con espacios vectoriales con coeficientes en $\mathbf{k}$. Para un poset finito P denotaremos $\mathrm{Int}(P)$ al conjunto de intervalos cerrados en P.

Definición 3.1. El *álgebra de incidencia de P* es la $\mathbf{k}$-álgebra $I(P)$ generada por todas las funciones

$$f : \mathrm{Int}(P) \to \mathbf{k},$$

con la operación de *convolución* definida para funciones $f, g \in I(P)$ por

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

Proposición 3.2. *$I(P)$ es un álgebra asociativa con unidad dada por la función $\epsilon : \mathrm{Int}(P) \to \mathbf{k}$ definida por*

$$\epsilon([x, y]) = \begin{cases} 1 & \textit{si } x = y \\ 0 & \textit{en cualquier otro caso.} \end{cases}$$

La siguiente proposición nos describe cuales son los elementos invertibles de $I(P)$.

Proposición 3.3. *Las siguientes condiciones son equivalentes para $f \in I(P)$:*

1. *f tiene una inversa por derecha, o sea, existe $g \in I(P)$ tal que $f \star g = \epsilon$.*
2. *f tiene una inversa por izquierda, o sea, existe $h \in I(P)$ tal que $h \star f = \epsilon$.*
3. *f tiene una inversa bilateral única.*
4. *$f([x, x]) \neq 0$ para todo $x \in P$.*

Demostración. La ecuación $f \star g = \epsilon$ se lee como

$$f \star g([x, y]) = \sum_{x \leq z \leq y} f([x, z])g([z, y]) = \begin{cases} 1 & \text{si } x = y \\ 0 & \text{en cualquier otro caso.} \end{cases}$$

Si $x = y$ entonces tenemos que $f([x, x])g([x, x]) = 1$ y esta ecuación se satisface si y solo si $f([x, x]) \neq 0$. En este caso $g([x, x]) = f([x, x])^{-1}$. Si $x < y$ entonces tenemos

$$g([x, y]) = -f([x, x])^{-1} \sum_{x < z \leq y} f([x, z])g([z, y]),$$

y entonces $g([x, y])$ es definida recursivamente y existe si y solo si $f([x, x]) \neq 0$. El mismo argumento aplica con la ecuación $h \star f = \epsilon$. Entonces si se tiene la inversa por un lado se tiene la inversa por el otro y finalmente si tenemos que $f \star g = \epsilon$ y $h \star f = \epsilon$ entonces $h = h \star \epsilon = h \star f \star g = \epsilon \star g = g$. □

3.1.1. Algunas funciones en $I(P)$

Definición 3.4. La *función zeta* ζ es la función en $I(P)$ definida para todo $x \leq y$ en P por $\zeta([x,y]) = 1$.

Ejemplo 3.5. Nótese que las potencias de ζ cuentan ciertos invariantes de P. Por ejemplo,

$$\zeta^{\star 2}([x,y]) := \zeta \star \zeta([x,y]) = \sum_{x \leq z \leq y} \zeta([x,z])\zeta([x,y]) = |\{x \leq z \leq y \mid z \in P\}|.$$

Definición 3.6. Una *multicadena* de (*orden* k) en un poset P es una sucesión de la forma $m_1 \leq m_2 \leq \cdots \leq m_k$ en donde $m_i \in P$ para todo i.

Proposición 3.7. *Sea P un poset acotado finito, entonces*

$$\zeta^{\star k}(P) = |\{\hat{0} = x_0 \leq x_1 \leq \cdots \leq x_k = \hat{1}\}|,$$

es decir, $\zeta^{\star k}$ cuenta multicadenas de orden $k+1$.

Si lo que queremos contar son cadenas en lugar de multicadenas podemos usar una función un poco modificada.

Proposición 3.8. *Sea P un poset acotado, entonces*

$$(\zeta - \epsilon)^{\star k}(P) = |\{\hat{0} = x_0 < x_1 < \cdots < x_k = \hat{1}\}|.$$

Demostración. Nótese que

$$(\zeta - \epsilon)([x,y]) = \begin{cases} 1 & \text{si } x < y \\ 0 & \text{en cualquier otro caso.} \end{cases}$$ □

Proposición 3.9. *Sea P un poset acotado, entonces*

$$(2\epsilon - \zeta)^{-1}(P) = |\{\hat{0} = x_0 < x_1 < \cdots < x_k = \hat{1} \mid \textit{para algún } k \in \mathbb{N}\}|.$$

Demostración. Nótese que

$$(2\epsilon - \zeta)([x,y]) = \begin{cases} -1 & \text{si } x < y \\ 1 & \text{si } x = y \end{cases}$$

entonces $(2\epsilon - \zeta)$ es invertible y podemos expresar $(2\epsilon - \zeta)^{-1} = (\epsilon - (\zeta - \epsilon))^{-1}$. Ahora consideremos la función $\sum_{k \geq 0} (\zeta - \epsilon)^{\star k}$ en donde $(\zeta - \epsilon)^0 = \epsilon$. Esta es una función válida en $I(P)$ ya que P es finito y entonces $(\zeta - \epsilon)^{\star N} = 0$ para todo $N > \ell(P)$. Además tenemos que

$$(\epsilon - (\zeta - \epsilon)) \star \sum_{k \geq 0} (\zeta - \epsilon)^{\star k} = \epsilon,$$

o sea que

$$(2\epsilon - \zeta)^{-1} = \sum_{k \geq 0} (\zeta - \epsilon)^{\star k}.$$

Finalmente el resultado se concluye usando la Proposición 3.8. □

Definición 3.10. Como $\zeta([x,x]) = 1$ para todo $x \in P$, sabemos por la Proposition 3.3 que ζ es invertible. La *función de Möbius* μ es la inversa de ζ, o sea $\mu := \zeta^{-1}$.

3.2. Calculando la función de Möbius

Proposición 3.11. *La función de Möbius μ puede definirse recursivamente para un intervalo $[x, y]$ como*

$$\mu([x,y]) = \begin{cases} 1 & \textit{si } x = y \\ -\sum_{x \leq z < y} \mu([x,z]) & \textit{en cualquier otro caso.} \end{cases} \tag{3.1}$$

Demostración. Como μ es la inversa de ζ, tenemos que $\mu \star \zeta = \epsilon$, lo que implica que

$$\mu \star \zeta([x,x]) = \mu([x,x])\zeta([x,x]) = \epsilon([x,x]) = 1,$$

o sea que $\mu([x,x]) = 1$. Y si $x < y$ entonces

$$\mu \star \zeta([x,y]) = \sum_{x \leq z \leq y} \mu([x,z])\zeta([z,y]) = \epsilon([x,y]) = 0,$$

lo que implica la fórmula que buscamos. □

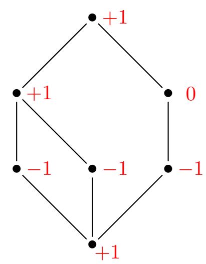


Figura 8: Valores $\mu([\hat{0}, x])$ de la función de Möbius

Ejemplo 3.12. Sea $\mathbf{n}$ la cadena con n elementos. Tenemos entonces queda

$$\mu(\mathbf{n}) = \begin{cases} 1 & \text{si } n = 1 \\ -1 & \text{si } n = 2 \\ 0 & \text{si } n \geq 3. \end{cases}$$

Por inspección podemos calcular $\mu(\mathbf{1}) = 1$, $\mu(\mathbf{2}) = -1$ y $\mu(\mathbf{3}) = 0$. Ahora por inducción y usando la formula recursiva 3.1 tenemos que para $n \geq 3$

$$\mu(\mathbf{n}) = -\sum_{k=1}^{n-1} \mu(\mathbf{k}) = -\mu(\mathbf{1}) - \mu(\mathbf{2}) = 0.$$

Proposición 3.13. *Sean P y Q posets localmente finitos y $(x, y) \leq (x', y')$ en $P \times Q$ entonces*

$$\mu([(x,y),(x',y')]) = \mu([x,x'])\mu([y,y']).$$

Ejemplo 3.14. Cómo $\mathbb{B}_n \cong \mathbf{2}^n$ tenemos que

$$\mu(\mathbb{B}_n) = \mu(\mathbf{2}^n) = \mu(\mathbf{2})^n = (-1)^n.$$

De igual forma si $A \subseteq B$ en $\mathbb{B}_n$, es fácil verificar que $[A, B] \cong \mathbb{B}_{B \setminus A}$, así que

$$\mu([A,B]) = \mu(\mathbb{B}_{B \setminus A}) = (-1)^{|B|-|A|}.$$

La estructura adicional de un retículo facilita la siguiente fórmula recursiva de Weisner para calcular los valores de la función de Möbius.

Teorema 3.15 (Teorema de Weisner). *Para todo $x \leq w < y$ en un retículo L tenemos queda*

$$\sum_{\substack{x \leq z \leq y \\ w \wedge z = x}} \mu([z, y]) = 0. \tag{3.2}$$

Ejemplo 3.16. En Π_n escojamos w como el coátomo $12 \cdots (n-1)|n$. Nótese que los valores de $z \in \Pi_n$ tales que $w \wedge z = \hat{0}$ son $z = \hat{0}$ o elementos de la forma $z = 1|2| \cdots |\hat{i}| \cdots (n-1)|in$, para los cuales se verifica que $[z, \hat{1}] \cong \Pi_{n-1}$. Usando el teorema de Weisner tenemos entonces que

$$\mu(\Pi_n) + (n-1)\mu(\Pi_{n-1}) = 0.$$

Resolviendo ésta ecuación en diferencias tenemos que $\mu(\Pi_n) = (-1)^{n-1}(n-1)!$.

3.3. La formula de inversión de Möbius

Proposición 3.17 (La fórmula de inversión de Möbius). *Sea P un poset en el cuál para todo $x \in P$ tenemos que $|I(x)| < \infty$ y sean $f, g : P \to \mathbf{k}$ un par de funciones en P. Las siguientes dos aserciones son equivalentes:*

$$g(y) = \sum_{x \leq y} f(x) \quad \forall y \in P \tag{3.3}$$

$$f(y) = \sum_{x \leq y} g(x)\mu([x, y]) \quad \forall x \in P. \tag{3.4}$$

Demostración. El espacio vectoral $\mathbf{k}^P$ formado por las funciones $f : P \to \mathbf{k}$ tiene una acción por derecha del álgebra de incidencia $I(P)$ dada por

$$f\xi(y) = \sum_{x \leq y} f(x)\xi([x, y]) \text{ para todo } f \in \mathbf{k}^P \text{ y para todo } \xi \in I(P).$$

Entonces la ecuación (3.3) se lee en este lenguaje como $g = f\zeta$ y entonces como $\zeta^{-1} = \mu$ tenemos que $f = g\mu$ que es la ecuación (3.4). $\square$

Proposición 3.18 (Forma dual del teorema de inversión de Möbius). *Sea P un poset en el cuál para todo $x \in P$ tenemos que $|I(x)| < \infty$ y sean $f, g : P \to \mathbf{k}$ un par de funciones en P. Las siguientes dos aserciones son equivalentes:*

$$g(y) = \sum_{x \geq y} f(x) \quad \forall y \in P \tag{3.5}$$

$$f(y) = \sum_{x \geq y} \mu([y, x])g(x) \quad \forall x \in P. \tag{3.6}$$

Ejemplo 3.19. (a) En la cadena $\mathbf{n}$ el teorema de inversión de Möbius es una versión discreta del Teorema Fundamental del Cálculo:

$$g(n) = \sum_{k=0}^{n} f(k) \quad \forall n \in \mathbb{N} \tag{3.7}$$

$$f(n) = g(n) - g(n-1) \quad \forall n \in \mathbb{N}. \tag{3.8}$$

(b) En el álgebra de Boole $\mathbb{B}_n$ el teorema de inversión de Möbius es conocido como el Principio de Inclusión-Exclusión:

$$g(A) = \sum_{B \subseteq A} f(B) \quad \forall B \subseteq A \tag{3.9}$$

$$f(A) = \sum_{B \subseteq A} (-1)^{|A|-|B|} g(B) \quad \forall B \subseteq A. \tag{3.10}$$

(c) Si en el álgebra de boole las funciones $g(A)$ y $f(A)$ solamente dependen de la cardinalidad del conjunto A entonces obtenemos un teorema de inversión conocido como Teorema de Inversión Binomial.

$$g(n) = \sum_{k=0}^{n} \binom{n}{k} f(k) \quad \forall n \in \mathbb{P} \tag{3.11}$$

$$f(n) = \sum_{k=0}^{n} \binom{n}{k} (-1)^{n-k} g(k) \quad \forall n \in \mathbb{P}. \tag{3.12}$$

(d) En el retículo de divisibilidad D_n el teorema de inversión de Möbius es un teorema clásico en la teoría de números:

$$g(n) = \sum_{d|n} f(d) \quad \forall n \in \mathbb{P} \tag{3.13}$$

$$f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d) \quad \forall n \in \mathbb{P}, \tag{3.14}$$

en donde $\mu(n)$ es la función de Möbius clásica de teoría de números dada por:

$$\mu(n) = \begin{cases} (-1)^k & \text{si } n = p_1 p_2 \ldots p_k \text{ es libre de cuadrados} \\ 0 & \text{en cualquier otro caso.} \end{cases}$$

Ejemplo 3.20. Dado un alfabeto A de tamaño $|A| = m$, Una *palabra circular* de longitud n es una clase de equivalencia de *palabras lineales* $w = w_1 w_2 \ldots w_n$ bajo la acción de la operación de desplazamiento o shift $\tau w = w_n w_1 w_2 \ldots w_{n-1}$. Una palabra circular es llamada *primitiva* si su clase de equivalencia contiene exactamente n palabras lineales distintas. Denotemos por $a(n)$ al número de palabras circulares primitivas de longitud n y $b(n)$ al número de todas las palabras circulares de longitud n (primitivas y no primitivas). Nuestro objetivo será encontrar una formula para determinar el número de palabras circulares $b(n)$. Nótese que una palabra circular es primitiva si y solo si no es una potencia de otra palabra así que tenemos la relación

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

Nótese también que hay c palabras lineales distintas en la clase de equivalencia de una palabra circular w de longitud $\ell(w) = d$ de la forma $w = u^{\frac{d}{c}}$ en donde u es una palabra circular primitiva de longitud $\ell(u) = c$. Así que contando todas las palabras lineales de longitud d tenemos

$$m^d = \sum_{c|d} c\, a(c).$$

El teorema de inversión de Möbius nos dice que

$$da(d) = \sum_{c|d} \mu\left(\frac{d}{c}\right) m^c.$$

concluimos que

$$b(n) = \sum_{d|n} \frac{1}{d} \sum_{c|d} \mu\left(\frac{d}{c}\right) m^c.$$

Referencias

[1] F. Ardila. Algebraic and geometric methods in enumerative combinatorics. *Handbook of enumerative combinatorics*, pages 3–172, 2015.

[2] R. P. Stanley. *Enumerative combinatorics. Volume 1*, volume 49 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, second edition, 2012.

[3] M. L. Wachs. Poset topology: tools and applications. In *Geometric combinatorics*, volume 13 of *IAS/Park City Math. Ser.*, pages 497–615. Amer. Math. Soc., Providence, RI, 2007.