Ejes de Contenidos

Definición de Relación

- Según la Real Academia Española, en su sentido matemático, el término significa:

  "*Resultado de comparar dos cantidades expresadas en números*"

- Por ejemplo:
  - Es correcto afirmar que 2 es menor que 5.
  - Es incorrecto afirmar que 2 es divisor de 5.

Definición de Relación

- O sea:
  - La comparación de 2 con 5 arroja resultado positivo, si el criterio de comparación es "*ser menor que*"
  - La comparación de 2 con 5 arroja resultado negativo, si el criterio de comparación es "*ser divisor de*"

- Podemos afirmar entonces que una relación queda determinada por el **conjunto de pares** que arrojan resultado positivo cuando son sometidos al "*criterio de comparación*" que determina la relación.

Definición Formal

Sean A y B dos conjuntos, una relación R entre A y B será un subconjunto del producto cartesiano $A \times B$

O sea: $R \subseteq A \times B$

Ejemplo

$A = \{2, 4, 8, 10\}$

$B = \{1, 3, 9\}$

La relación R $=$ "*es menor que*" se representa matemáticamente mediante el siguiente subconjunto de $A \times B$:

$R = \{(2, 3), (2, 9), (4, 9), (8, 9)\}$

Entonces la afirmación:

- "2 es menor que 9" se formaliza expresando $(2, 9) \in R$
- "4 no es menor que 1" se formaliza expresando $(4, 1) \notin R$

Notación

- Si R es una relación entre A y A, decimos que R es una relación **sobre** A
- Si R es una relación sobre A, y $(a, b) \in R$, entonces escribimos

  $$a \sim_R b$$

  o simplemente

  $$a \sim b$$

Tipos fundamentales de relaciones

- **Funciones**
  No serán abordadas en este curso
- **Relaciones de equivalencia**
  Esta clase:
  su vinculación con las particiones de un conjunto
- **Relaciones de orden**
  Casi la totalidad de la primera parte de la materia

Propiedades de las relaciones

Sea R una relación sobre un conjunto A. Decimos que R es:

- **reflexiva** si y sólo si para todo $a \in A$: $a \sim a$
- **simétrica** si y sólo si para todo $a, b \in A$,

  $a \sim b$ implica que $b \sim a$
- **antisimétrica** si y sólo si para todo $a, b \in A$

  $a \sim b$ y $b \sim a$ implican que $a = b$
- **transitiva** si y sólo si para todo $a, b, c \in A$,

  $a \sim b$ y $b \sim c$ implican que $a \sim c$

Ejemplo 1: Relación "divide"

Es la relación sobre los naturales positivos definida mediante:

$a \sim b$ si y sólo si a es divisor de b

En cursos anteriores se utilizó la notación $a|b$

¿Cuáles de las 4 propiedades son satisfechas por la relación divide?

Ejemplo 2: Relación "congruente módulo k"

Dado un k fijo, es la relación sobre **Z** definida mediante:

$a \sim_k b$ si y sólo si k es divisor de $b - a$

En cursos anteriores se utilizó la notación $a \equiv b \; mod(k)$

¿Cuáles de las 4 propiedades son satisfechas por la relación "congruente módulo k"?

Relaciones de equivalencia

Son las relaciones que satisfacen las propiedades **reflexividad, simetría y transitividad**

Por ejemplo, la relación "congruente módulo k" es una relación de equivalencia, cualquiera sea k

Clases de equivalencia

Sea $\sim$ una relación de equivalencia sobre un conjunto A y sea x un elemento de A.

La *clase de equivalencia de x* se denota por $[x]$ y es el conjunto

$$[x] = \{y \in A \mid y \sim x\}$$

Por ejemplo, en la relación "congruente módulo 3",

$$[0] = \{0, 3, -3, 6, -6, 9, -9, ...\}$$
$$[1] = \{1, 4, -2, 7, -5, 10, -8, ...\}$$
$$[2] = \{2, 5, -1, 8, -4, 11, -7, ...\}$$
$$[3] = [0]$$
$$[4] = [1]$$
$$[5] = [2] \; ....$$

Partición de un conjunto

Una **partición** de un conjunto A es una familia de subconjuntos no vacíos de A, que son disjuntos entre sí, y cuya unión es todo A.

Por ejemplo, las siguientes son distintas particiones de $A = \{a, \ b, \ c\}$:

P_1 : $\{a\}, \{b\}, \{c\}$;
P_2 : $\{a\}, \{b, c\}$;
P_3 : $\{a, \ b, \ c\}$.

Teorema

Sea $\sim$ una relación de equivalencia en un conjunto A y sean x, y elementos de A. Entonces

1. $[x] = [y]$ si y sólo si $x \sim y$.
2. si $x \not\sim y$, entonces $[x]$ e $[y]$ son disjuntas.

Relación de equivalencia y Partición

Son conceptos duales

Sea $\sim$ una relación de equivalencia en un conjunto A, entonces las clases de equivalecia determinan una partición de A

Sea $P_1, P_2, ...$ una partición de A, entonces la relación definida mediante $a \sim b$ si y sólo si existe k tal que $a, b \in P_k$ es una relación de equivalecia sobre A

Relación de Orden Parcial

Una **relación de orden parcial** R sobre un conjunto A es una relación que satisface las propiedades de **reflexividad**, **antisimetría** y **transitividad**

Notación: $a \leq b$ en lugar de $(a, b) \in R$

Ejemplos:

1. Si a y b son números, entonces $a \leq b$ denota la relación de orden usual sobre $\mathbb{R}$ (o $\mathbb{Z}$), salvo que se diga explícitamente otra cosa.
2. $a \leq b$ si y sólo si a divide a b sobre $\mathbb{N}$, (se puede usar $a|b$)
3. $X \leq Y$ si y sólo si $X \subseteq Y$ sobre $\mathcal{P}(A)$

Relación de Orden Parcial

Una **relación de orden parcial** R sobre un conjunto A es una relación que satisface las propiedades de **reflexividad**, **antisimetría** y **transitividad**

Notación: $a \leq b$ en lugar de $(a, b) \in R$

Relación de Orden Parcial

Ejemplos:

1. **Relación de orden usual** sobre $\mathbb{R}$ (o $\mathbb{Z}$): Si a y b son números, entonces $a \leq b$ refleja la relación de orden dada por la representación geométrica de la recta, salvo que se diga explícitamente otra cosa.
2. La relación definida por $a \leq b$ si y sólo si a divide a b (sobre $\mathbb{N} = \{1, 2, 3, ...\}$) es una relación de orden. También utilizamos $a|b$.
3. $X \leq Y$ si y sólo si $X \subseteq Y$ (sobre $\mathcal{P}(A)$) es una relación de orden

Diagramas de Hasse

Definición de la relación cubrimiento
Sea A un conjunto y $\leq$ un orden parcial sobre A. Sean $a, b \in A$ elementos distintos. Decimos que b *cubre* a a si $a \leq b$ y no existe c distinto de a y b tal que $a \leq c$ y $c \leq b$.

Definición de Diagrama de Hasse
Consiste de puntos llamados **vértices** que representan los elementos del conjunto y de **arcos** o **segmentos ascendentes** que unen pares de vértices de la siguiente manera:

a está conectado con b mediante un arco ascendente si y sólo si b cubre a a.

Conjunto Parcialmente Ordenado (CPO o POSET)

Es un par $(P, \leq)$ donde P es un conjunto y $\leq$ es un orden parcial sobre P

Ejemplos:

1. $(\mathbb{R}, \leq)$ es un POSET
2. $(\mathbb{N}, |)$ es un POSET
3. $(\{1, 2, 3, 5, 6, 8\}, |)$ es un POSET
4. $(\mathcal{P}(\mathbb{N}), \subseteq)$ es un POSET

Máximos y Mínimos

$(P, \leq)$ un POSET

- a es mínimo de P si para todo x en P se tiene $a \leq x$
- a es máximo de P si para todo x en P se tiene $x \leq a$

¿Cuáles de los siguientes tienen máximo y/o mínimo?

1. $(\mathbb{N}, \leq)$
2. $([0, 1), \leq)$
3. $(\{2, 4, 6, 12, 16\}, |)$
4. $(\{2, 4, 6, 12\}, |)$
5. $(\{\{c\}, \{a, b\}, \{a, b, c\}\}, \subseteq)$

Maximales y Minimales

$(P, \leq)$ un POSET

- a es **minimal** de P si para todo x en P, $x \leq a$ implica que $x = a$
- a es **maximal** de P si para todo x en P, $a \leq x$ implica que $a = x$

¿Cuáles de los siguientes tienen maximales y/o minimales?

1. $(\mathbb{N}, \leq)$
2. $([0, 1), \leq)$
3. $(\{2, 4, 6, 12, 16\}, |)$
4. $(\{2, 4, 6, 12\}, |)$
5. $(\{\{c\}, \{a, b\}, \{a, b, c\}\}, \subseteq)$

Orden Total o Cadena

Un *orden total* sobre un conjunto P es un orden parcial $\leq$ sobre P que satisface la **ley de dicotomía**:

$$\text{para todo } a, b \in P, \quad a \leq b \ \text{ o } \ b \leq a.$$

Algunos ejemplos de órdenes totales:

1. El orden $\leq$ en $\mathbb{R}$
2. El orden lexicográfico en un diccionario.

Supremos e Ínfimos

Sea $(P, \leq)$ un poset y sea $S \subseteq P$.

1. $a \in P$ se dice *cota superior* de S si para todo $b \in S$ ocurre que $b \leq a$.
2. $a \in P$ se dice *cota inferior* de S si para todo $b \in S$ ocurre que $a \leq b$.
3. $a \in P$ se dice *supremo* de S si a es una cota superior de S y para toda cota superior b de S se cumple que $a \leq b$.
4. $a \in P$ se dice *ínfimo* de S si a es una cota inferior de S y para toda cota inferior b de S se cumple que $b \leq a$.

Isomorfismo de POSETS

Sean $(P, \leq)$, $(Q, \leq')$ dos posets, y sea $f : P \to Q$ una función.

Diremos que f es un **isomorfismo** si f es biyectiva y para todo $x, y \in P$, se cumple que

$x \leq y$ si y sólo si $f(x) \leq' f(y)$

Propiedad Fundamental de los Isomorfismos

Lema

Sean $(P, \leq)$ y $(Q, \leq')$ posets. Sea $f : P \to Q$ un isomorfismo.

1. Para cada $S \subseteq P$, se tiene que existe $\sup(S)$ si y sólo si existe $\sup(f(S))$ y en el caso de que existan tales elementos se tiene que $f(\sup(S)) = \sup(f(S))$.
2. Para cada $S \subseteq P$, se tiene que existe $\inf(S)$ si y sólo si existe $\inf(f(S))$ y en el caso de que existan tales elementos se tiene que $f(\inf(S)) = \inf(f(S))$.

Supremos e Ínfimos

Sea $(P, \leq)$ un poset y sea $S \subseteq P$.

1. $a \in P$ se dice *cota superior* de S si para todo $b \in S$ ocurre que $b \leq a$.
2. $a \in P$ se dice *cota inferior* de S si para todo $b \in S$ ocurre que $a \leq b$.
3. $a \in P$ se dice *supremo* de S si a es una cota superior de S y para toda cota superior b de S se cumple que $a \leq b$.
4. $a \in P$ se dice *ínfimo* de S si a es una cota inferior de S y para toda cota inferior b de S se cumple que $b \leq a$.

Isomorfismo de POSETS

Sean $(P, \leq)$, $(Q, \leq')$ dos posets, y sea $f : P \to Q$ una función.

Diremos que f es un **isomorfismo** si f es biyectiva y para todo $x, y \in P$, se cumple que

$$x \leq y \text{ si y sólo si } f(x) \leq' f(y)$$

Propiedad Fundamental de los Isomorfismos

Lema

Sean $(P, \leq)$ y $(Q, \leq')$ posets. Sea $f : P \to Q$ un isomorfismo.

1. Para cada $S \subseteq P$, se tiene que existe $\sup(S)$ si y sólo si existe $\sup(f(S))$ y en el caso de que existan tales elementos se tiene que $f(\sup(S)) = \sup(f(S))$.
2. Para cada $S \subseteq P$, se tiene que existe $\inf(S)$ si y sólo si existe $\inf(f(S))$ y en el caso de que existan tales elementos se tiene que $f(\inf(S)) = \inf(f(S))$.

Posets Rerticulados

Diremos que un poset $(L, \leq)$ es un poset **reticulado** si para todo $a, b \in L$, existen $\sup(\{a, b\})$ e $\inf(\{a, b\})$.

Notación: $a \vee b = \sup\{a, b\}$ $\quad a \wedge b = \inf\{a, b\}$

¿Cuáles de los siguientes posets son reticulados?

- $(\mathbb{N}, \leq)$
- $([0, 1), \leq)$
- $(\{2, 4, 6, 12, 24\}, |)$
- $(\{2, 4, 5, 6, 12\}, |)$
- $(\mathcal{P}(\{a, b, c\}, \subseteq)$

Reticulado de divisores de *n*

$D_n = \{k \in \mathbb{N} : k|n\}$

$(D_n, |)$ es un reticulado

$x \vee y = mcm(x, y)$

$x \wedge y = mcd(x, y)$

1 es mínimo de D_n

n es el máximo de D_n

Reticulado de partes de X

$(\mathcal{P}(X), \subseteq)$ es un reticulado

$A \vee B = A \cup B$

$A \wedge B = A \cap B$

$\emptyset$ es mínimo de $\mathcal{P}(X)$

X es el máximo de $\mathcal{P}(X)$

Propiedades básicas del supremo e ínfimo

Dado un reticulado $(L, \leq)$, y elementos $x, y, z, w \in L$, se cumplen las siguientes propiedades:

1. $x \leq x \vee y$
2. $x \wedge y \leq x$
3. $x \leq y \quad \Leftrightarrow \quad x \vee y = y \quad \Leftrightarrow \quad x \wedge y = x$,
4. ley de compatibilidad

$$x \leq z \text{ e } y \leq w \quad \text{implican} \quad x \vee y \leq z \vee w, \quad x \wedge y \leq z \wedge w$$

Propiedades fundamentales del supremo e ínfimo

1. leyes de idempotencia:

$$x \vee x = x \wedge x = x$$

2. leyes conmutativas:

$$x \vee y = y \vee x, \qquad x \wedge y = y \wedge x$$

3. leyes de absorción:

$$x \vee (x \wedge y) = x, \qquad x \wedge (x \vee y) = x$$

4. leyes asociativas:

$$(x \vee y) \vee z = x \vee (y \vee z), \qquad (x \wedge y) \wedge z = x \wedge (y \wedge z)$$

Desigualdades distributivas

$$x \vee (y \wedge z) \leq (x \vee y) \wedge (x \vee z)$$

$$(x \wedge y) \vee (x \wedge z) \leq x \wedge (y \vee z)$$

Noción de Estructura Algebraica

Estructura Algebraica = conjunto con operaciones

Por ejemplo, los números enteros dotados de las operaciones suma, producto y las constantes 0 y 1 tienen estructura de **Anillo**.

Se denota: $(\mathbb{Z}, +.\cdot, 0, 1)$

Lo importante de la operación no es el nombre, sino el **tipo**. Por ejemplo el tipo de $+$ es $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$

La estructura está dada no sólo por las operaciones, sino también por las propiedades que las mismas satisfacen, en este caso, la asociatividad, la distributividad del producto respecto de la suma, etc.

Reticulado como Estructura Algebraica

Es una tupla $(L, \vee, \wedge)$ que satisface las propiedades:

1. Idempotencia: $x \vee x = x \wedge x = x$
2. Conmutatividad: $x \vee y = y \vee x \qquad x \wedge y = y \wedge x$
3. Absorción: $x \vee (x \wedge y) = x \qquad x \wedge (x \vee y) = x$
4. Asociatividad:

$$(x \vee y) \vee z = x \vee (y \vee z) \qquad (x \wedge y) \wedge z = x \wedge (y \wedge z)$$

Ejemplos

1. No toda estructura del tipo $(L, \vee, \wedge)$ es un reticulado. Por ejemplo la estructura $(\mathbb{R}, +, \cdot)$ donde $+$ y $\cdot$ son las operaciones de suma y producto usuales de $\mathbb{R}$ no es un reticulado.
2. Por las propiedades fundamentales de supremo e ínfimo, un poset reticulado $(L, \leq)$ puede "mutar" para convertirse en un reticulado (como estructura algebraica): tomamos la estructura $(L, \vee, \wedge)$ donde $\vee$ y $\wedge$ representan al supremo y al ínfimo resp.

Existencia dual de un Reticulado

Sea $(L, \vee, \wedge)$ un reticulado (como estructura algebraica). La relación binaria definida por:

$$x \leq y \iff x \vee y = y$$

es un orden parcial sobre L para el cual se cumple:

$$x \vee y = sup\{x, y\}, \qquad x \wedge y = inf\{x, y\}$$

Ejemplos

1. Si X es un conjunto arbitrario, entonces $(\mathcal{P}(X), \cup, \cap)$ es un reticulado. La relación binaria inducida por $\cup$ y $\cap$ es precisamente la inclusión, pues

$$A = A \cup B \iff B \subseteq A$$

2. Si $n \in \mathbb{N}$ entonces (D_n, mcm, mcd) es un reticulado. La relación binaria inducida es la de divisibilidad, pues

$$mcm(x, y) = y \iff x|y$$

Existencia dual de un Reticulado

- Dado un CPO reticulado $(L, \leq)$, entonces la estructura algebraica $(L, \vee, \wedge)$ satisface las propiedades de idempotencia, conmutatividad, absorción y asociatividad.
- Sea $(L, \vee, \wedge)$ una estructura algebraica que satisface las propiedades de idempotencia, conmutatividad, absorción y asociatividad, entonces la relación binaria definida por:

$$x \leq y \Longleftrightarrow x \vee y = y$$

es un orden parcial sobre L.

Las construcciones son recíprocas

Lema

Sea $(L, \vee, \wedge)$ un reticulado (como estructura algebraica). La relación binaria definida por:

$$x \leq y \Longleftrightarrow x \vee y = y$$

es un orden parcial sobre L para el cual se cumple:

$$x \vee y = sup\{x, y\}, \qquad x \wedge y = inf\{x, y\}$$

Las construcciones son recíprocas

o sea,

El CPO $(L, \leq)$ que se obtiene de $(L, \vee, \wedge)$ definiendo:

$$x \leq y \Longleftrightarrow x \vee y = y$$

es un reticulado en el cual las operaciones supremo e ínfimo coinciden con $\vee$ y $\wedge$ resp.

Ejemplos

1. Si X es un conjunto arbitrario, entonces $(\mathcal{P}(X), \vee, \wedge)$ es un reticulado. La relación binaria inducida por $\cup$ y $\cap$ es precisamente la inclusión, y

$$A \vee B = A \cup B \qquad\qquad A \wedge B = A \cap B$$

2. Si $n \in \mathbb{N}$ entonces $(D_n, \vee, \wedge)$ es un reticulado. La relación binaria inducida es la de divisibilidad,

$$x \vee y = mcm(x, y) \qquad\qquad x \wedge y = mcd(x, y)$$

Notación

Cuando escibimos

"sea L un reticulado"

consideramos L simultaneamente dotado de su estructura de poset $(L, \leq)$ y de estructura algebraica $\langle L, \vee, \wedge \rangle$.

Reticulados acotados

Definición: L será **acotado** si tiene máximo y mínimo.

Notación: Usamos

1^L para denotar al máximo

0^L para denotar al mínimo

Reticulados complementados

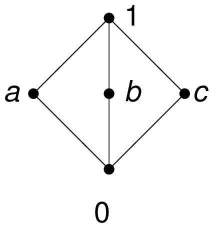
Sea L un reticulado acotado y sea $x \in L$. Decimos que x es **complementado** si existe $y \in L$ tal que

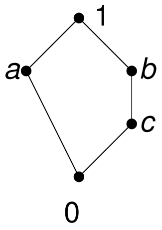
$$x \vee y = 1^L \qquad x \wedge y = 0^L$$

L será un **reticulado complementado** si todos sus elementos tienen al menos 1 complemento.

Falla Estructural

El complemento no está determinado por la estructura de orden, como lo están las operaciones supremo e ínfimo.





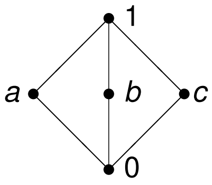
Propiedad de distributividad

$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$$

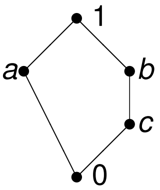
$$(x \wedge y) \vee (x \wedge z) = x \wedge (y \vee z)$$

¿Valen en todo reticulado?

Casos paradigmáticos de no distributividad



M_3



N_5

$$c \vee (b \wedge a) \neq (c \vee b) \wedge (c \vee a)$$

$$b \wedge (c \vee a) \neq (b \wedge c) \vee (b \wedge a)$$

Desigualdades distributivas

$$x \vee (y \wedge z) \leq (x \vee y) \wedge (x \vee z)$$

$$(x \wedge y) \vee (x \wedge z) \leq x \wedge (y \vee z)$$

La propiedad de Distributividad

Lema: Sea L un reticulado; entonces son equivalentes:

1. Para todo x, y, $z \in L$,
$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$$
2. Para todo x, y, $z \in L$,
$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$$

Notar que hay reticulados que no satisfacen ni 1 ni 2.

Distributividad implica compleménto único

Lema:
Si L es un reticulado acotado y distributivo, entonces todo elemento tiene a **lo sumo** un complemento.

Notar que puede **no haber** complementos, por ejemplo

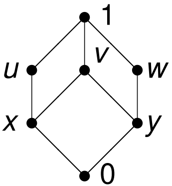
Noción de subreticulado

Sea L un reticulado. Un subconjunto $M \subseteq L$ será llamado *subreticulado* de L si

1. $M \neq \emptyset$,
2. para todo $x, y \in M$, se tiene que $x \vee y, x \wedge y \in M$.

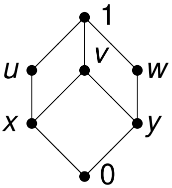
Por ejemplo:

Considere el reticulado



Por ejemplo:

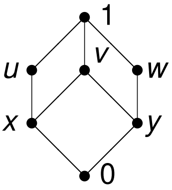
Considere el reticulado



$\{0, x, y, 1\}$ no es subreticulado

Por ejemplo:

Considere el reticulado



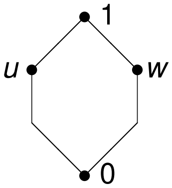
$\{0, x, y, 1\}$ no es subreticulado

$\{0, u, w, 1\}$ es subreticulado

Un subreticulado es un reticulado

Notar que M dotado de las operaciones (y/o el orden) heredadas de L es en sí mismo un reticulado.

$\{0, u, w, 1\}$ es el subreticulado



Noción de subreticulado II

Sean S y L dos reticulados.

Se suele decir que S es subreticulado de L cuando en realidad S es isomorfo a un subreticulado de L

Por ejemplo,

- $\mathcal{P}(\{a, b\})$ es subreticulado de D_{12}
- D_{12} es subreticulado de $\mathcal{P}(\{a, b, c\})$

La propiedad de Distributividad

Lema:
Sea L un reticulado; entonces son equivalentes:

1. Para todo $x, y, z \in L$,
$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$
2. Para todo $x, y, z \in L$,
$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$

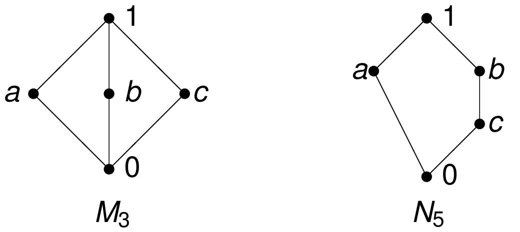
Reticulados Distributivos

Sea L un reticulado, entonces L se dice **distributivo** si satisface alguna de las propiedades del Lema.

Ejemplos:

1. $\mathbb{N}$ con el orden usual es distributivo
2. $[0, 1)$ con el orden usual es distributivo
3. $\mathcal{P}(\{a, b, c\}$ es distributivo
4. D_n es distributivo

Casos paradigmáticos de no distributividad



$$c \vee (b \wedge a) \neq (c \vee b) \wedge (c \vee a)$$

$$b \wedge (c \vee a) \neq (b \wedge c) \vee (b \wedge a)$$

Distributividad implica compleménto único

Lema:
Si L es un reticulado acotado y distributivo, entonces todo elemento tiene a **lo sumo** un complemento.

Notar que puede **no haber** complementos, por ejemplo

Criterio para analizar distributividad

Lema:

Un reticulado es distributivo si y sólo si no contiene subreticulados isomorfos a M_3 ni N_5.

Resumen de criterios para analizar distributividad

Para comprobar la distributividad de L:

1. Ver que L es subreticulado de algún reticulado de la forma $\mathcal{P}(X)$ o D_n.

Para refutar la distributividad de L:

1. Ver que existe un elemento con más de un complemento.
2. Ver que contiene como subreticulados a M_3 o N_5.

Álgebras de Boole

Es una estructura del tipo $\langle B, \vee, \wedge, ', 0, 1\rangle$, donde B es un conjunto no vacío, y además satisface:

1. $\langle B, \vee, \wedge\rangle$ es un reticulado distributivo
2. Para todo $x \in B$ se tiene

$$0 \leq x \qquad x \leq 1$$

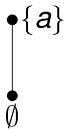
3. para cada $x \in L$, se tiene que

$$x \vee x' = 1, \qquad x \wedge x' = 0$$

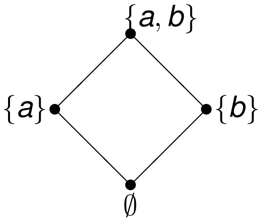
Álgebra de Boole de conjuntos

Sea X un conjunto.

Entonces $\langle \mathcal{P}(X), \cup, \cap, ^c, \emptyset, X \rangle$ es un álgebra de Boole,



$\mathcal{P}(\{a\})$



$\mathcal{P}(\{a, b\})$

Leyes de de Morgan

Sea $\langle B, \vee, \wedge, ', 0, 1 \rangle$ un álgebra de Boole, entonces se cumple:

$$(x \vee y)' = x' \wedge y'$$

$$(x \wedge y)' = x' \vee y'$$

Isomorfismo de Álgebras de Boole

Sean $\langle B, \vee, \wedge, ', 0^B, 1^B \rangle$ y $\langle B_1, \vee_1, \wedge_1, ^*, 0^{B_1}, 1^{B_1} \rangle$ Álgebras de Boole. Una función $F : B \to B_1$ se dice un *isomorfismo* si F es biyectiva y para todo $x, y \in L$ se cumple que

$$F(x \vee y) = F(x) \vee_1 F(y)$$

$$F(x \wedge y) = F(x) \wedge_1 F(y)$$

$$F(x') = (F(x))^*$$

$$F(0^B) = 0^{B_1}$$

$$F(1^B) = 1^{B_1}$$

Comparación de las nociones de Isomorfismo

Isomorfismo como posets:

$$x \leq y \quad \Longleftrightarrow \quad F(x) \leq' F(y)$$

Isomorfismo como estructura algebraica:

$$F(x \vee y) = F(x) \vee_1 F(y)$$
$$F(x \wedge y) = F(x) \wedge_1 F(y)$$
$$F(x') = (F(x))^*$$
$$F(0^B) = 0^{B_1}$$
$$F(1^B) = 1^{B_1}$$

Equivalencia de las nociones de Isomorfismo

Teorema:
Sean $\langle B, \vee, \wedge, ', 0^B, 1^B \rangle$ y $\langle B_1, \vee_1, \wedge_1, ^*, 0^{B_1}, 1^{B_1} \rangle$ Álgebras de Boole y sean $(B \leq)$ y $(B_1, \leq_1)$ los posets asociados.

Para toda $F : B \mapsto B_1$, son equivalentes:

1. F es un isomorfismo entre las estructuras $\langle B, \vee, \wedge, ', ^B, 1^B \rangle$ y $\langle B_1, \vee_1, \wedge_1, ^*, 0^{B_1}, 1^{B_1} \rangle$.
2. F es un isomorfismo entre los posets $(B, \leq)$ y $(B_1, \leq_1)$.

Cuestión a resolver

Todas las Álgebras de Boole vistas (aunque estén camufladas como D_6 o D_{30}) son en definitiva (vía isomorfismo) de la forma $\mathcal{P}(X)$.

O sea, son **álgebras de conjuntos.**

¿Será cierto que todas las Álgebras de Boole son álgebras de conjuntos?

(En tal caso estaríamos en presencia de una abstracción "poco abstracta")

Próximo objetivo: Teorema de Representación

Toda Álgebra de Boole **finita** B es un **álgebra de conjuntos.**
O sea, existe X tal que

$$B \cong \mathcal{P}(X)$$

Pregunta inicial:

¿Qué objetos juegan el rol de elementos de X?

Átomos

Sea B un álgebra de Boole (basta con que sea reticulado).

Un elemento $a \in B$ será llamado **átomo** si a cubre a 0.

Notación: $At(B)$ es el conjunto de todos los átomos de B.

Por ejemplo:

1. En $\mathcal{P}(X)$, los átomos son los conjuntos unitarios.
2. Los átomos de D_{12} son 2 y 3.

Hay suficiente cantidad de átomos

Lema A
Sea B un álgebra de Boole finita. Para todo $x \in B$ distinto de 0 existe $a \in At(B)$ tal que $a \leq x$.

Lema B Sea B un álgebra de Boole finita, y sean $x, y \in B$ tales que $x \not\leq y$. Entonces existe $a \in At(B)$ tal que $a \leq x$ y $a \not\leq y$.

Hay suficiente cantidad de átomos

Lema

Sea B un álgebra de Boole finita. Entonces todo elemento de B se escribe de manera única como supremo de átomos.

O sea: para todo $x \in B$ se tiene:

1. $x = sup\{a \in At(B) : a \leq x\}$,
2. si $A \subseteq At(B)$ y $x = sup\ A$, entonces

$$A = \{a \in At(B) : a \leq x\}$$

Teorema de Representación

Sea $\langle B, \vee, \wedge, ', 0, 1\rangle$ un álgebra de Boole finita, y sea $X = At(B)$. La función

$$\begin{array}{rcl} F : B & \longrightarrow & \mathcal{P}(X) \\ x & \longrightarrow & \{a \in X : a \leq x\} \end{array}$$

es un isomorfismo entre $\langle B, \vee, \wedge, ', 0, 1\rangle$ y $\langle \mathcal{P}(X), \cup, \cap, ^c, \emptyset, X\rangle$.

Esquema de la Prueba del TR

Lema A

$\downarrow$

Lema B

$\downarrow$

Lema

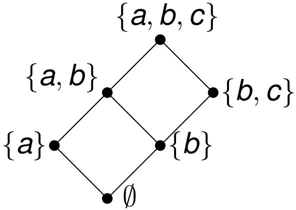
$\downarrow$

Teorema de Representación

Problema de la representación de un reticulado

Las Álgebras de Boole finitas son álgebras de conjuntos.

¿Serán los reticulados finitos reticulados de conjuntos?



Conjuntos decrecientes de un poset

Sea $(P, \leq)$ un poset

Diremos que un subconjunto $D \subseteq P$ es **decreciente** si para todo $x, z \in P$ se tiene que:

$$x \in D \text{ y } z \leq x \implies z \in D.$$

O sea, un conjunto decreciente satisface que si un elemento se encuentra en el conjunto, entonces todos los elementos menores también están.

Reticulado de conjuntos decrecientes de un poset

Denotaremos mediante $\mathcal{D}(P)$ a la familia de todos los subconjuntos decrecientes de P:

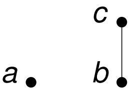
$$\mathcal{D}(P) = \{D \subseteq P : D \text{ es decreciente}\}.$$

Entonces

$$\langle \mathcal{D}(P), \cup, \cap, \emptyset, P \rangle.$$

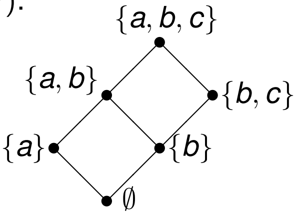
es un **reticulado es distributivo**

Ejemplo: sea P el poset



Los conj. decrecientes son: $\emptyset, \{a\}, \{b\}, \{a,b\}, \{b,c\}, \{a,b,c\}$

Forman el reticulado $\mathcal{D}(P)$:

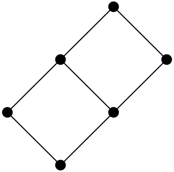


Problema de la representación de un reticulado

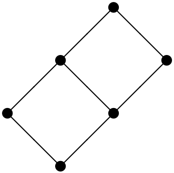
¿Será cierto que para todo reticulado distributivo L existe un poset P tal que

$$L \cong \mathcal{D}(P)$$

Dado L un reticulado, ¿cómo obtengo el P tal que $L \cong \mathcal{D}(P)$?



¿Cómo se obtiene P desde L?



$\downarrow$
$\downarrow$

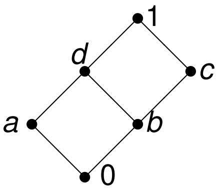
Elementos Irreducibles

Sea L un reticulado acotado. Un elemento $x \in L$ será llamado **irreducible** si

1. $x \neq 0$,
2. si $x = y \vee z$, entonces $x = y$ o $x = z$, para todo $y, z \in L$.

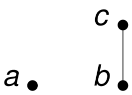
La segunda condición es equivalente a decir que x no se puede obtener como supremo de dos elementos distintos de x.

Ejemplos de Elementos Irreducibles



Elementos irreducibles: a, b, c

Forman el poset:



Poset de Elementos Irreducibles

Definición: $Irr(L) = \{i \in L : i \text{ es irreducible}\}$

Próximo objetivo: Demostrar que todo reticulado distributivo finito L es isomorfo a $\mathcal{D}(P)$, donde el poset $(P, \leq)$ asociado al reticulado L es

$$(Irr(L), \leq)$$

,
donde $\leq$ es el orden heredado de L.

Hay suficiente cantidad de Irreducibles

Lema A

Sea L un reticulado finito, y sean $x, y \in L$ tales que $x \nleq y$. Entonces existe $i \in Irr(L)$ tal que $i \leq x$ e $i \nleq y$.

Hay suficiente cantidad de Irreducibles

Lema

Sea L un reticulado distributivo finito. Entonces para todo $x \in L$ se tiene:

1. $x = sup\{i \in Irr(L) : i \leq x\}$,
2. si $D \subseteq Irr(L)$ es decreciente, y $x = sup\, D$, entonces

$$D = \{i \in Irr(L) : i \leq x\}$$

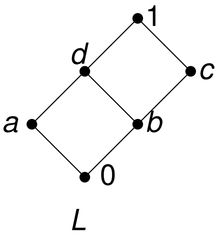
Teorema de Birkhoff

Sea L un reticulado acotado distributivo finito, y sea $P = Irr(L)$. Entonces la función

$$\begin{array}{rcl} F : L & \longrightarrow & \mathcal{D}(P) \\ x & \longrightarrow & \{y \in P : y \leq x\} \end{array}$$

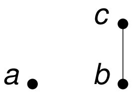
es un isomorfismo entre L y $\mathcal{D}(P)$.

El ejemplo D_{12} completo

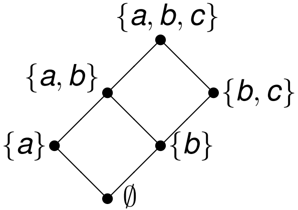


$Irr(L) = \{a, b, c\}$

Forman el poset:



$$\mathcal{D}(P) = \{\emptyset, \{a\}, \{b\}, \{a,b\}, \{b,c\}, \{a,b,c\}\}$$



La correspondencia F dada por el Teorema es:

$$0 \to \emptyset \qquad a \to \{a\}$$
$$b \to \{b\} \qquad d \to \{a,b\}$$
$$c \to \{b,c\} \qquad 1 \to \{a,b,d\}$$

Nuevo criterio de análisis de distributividad

Se puede observar que la única intervención de la distributividad en la prueba del Teorema de Birkhoff es para probar que F es sobre.

Criterio de análisis de distributividad

Un reticulado finito es ditributivo si y sólo si $|L| = |\mathcal{D}(Irr(L))|$

Volviendo a las Álgebras de Boole

Vale:

$At(B) = Irr(B)$

Entonces, si L es un reticulado acotado distributivo finito, se tiene:

L es álgebra de Boole si y sólo si $Irr(L) = At(L)$.

TR no vale para el caso infinito

Existe un álgebra de Boole **infinita** que no es isomorfa $\mathcal{P}(X)$, para ningún X.

Construiremos un Álgebra de Boole $\mathcal{B}$, y usaremos un argumento sobre su cardinalidad para probar que no es isomorfa a ningún álgebra de la forma $\mathcal{P}(X)$.

Cardinal de un conjunto

1. X tiene cardinal **finito** si $X = \emptyset$, o existe $n \in \mathbb{N}$ tal que se puede encontrar una biyección entre X y $\{1, 2, ..., n\}$.
2. Si X no es finito, decimos que X es **infinito.**
3. X tiene cardinal **infinito numerable** si se puede encontrar una biyección entre X y $\mathbb{N}$. En tal caso se dice que X tiene cardinal $\aleph_0$.
4. Si X es infinito y no se puede encontrar tal biyección, decimos que X es **infinito no numerable**.
5. Ejemplos de conjuntos infinitos no numerables: $\mathbb{R}$, $\mathcal{P}(\mathbb{N})$. Ambos tienen cardinal $\aleph_1$.

Cardinal de $\mathcal{P}(X)$

Los cardinales tiene un orden

$0 < 1 < 2 < ... < \aleph_0 < \aleph_1 < ...$

1. Si X es **finito**, entonces $\mathcal{P}(X)$ es finito ¿Cuál es su cardinal?
2. Si X es **infinito**, entonces $\mathcal{P}(X)$ es **infinito no numerable.**

Cardinal de $\mathcal{P}(X)$

Los cardinales tiene un orden

$0 < 1 < 2 < ... < \aleph_0 < \aleph_1 < ...$

1. Si X es **finito**, entonces $\mathcal{P}(X)$ es finito ¿Cuál es su cardinal?
2. Si X es **infinito**, entonces $\mathcal{P}(X)$ es **infinito no numerable.**

Cardinal de $\mathcal{P}(X)$

$$\begin{array}{c|c|c}
0 < 1 < 2 < \quad \ldots & < \aleph_0 & < \aleph_1 < \aleph_2 \; \ldots. \\
\mathcal{P}(X) & & \mathcal{P}(X) \\
(X \text{ finito}) & \downarrow & (X \text{ infinito})
\end{array}$$

No es el cardinal
de ningún $\mathcal{P}(X)$

Conclusión: Si podemos construir un Álgebra de Boole $\mathcal{B}$ que tenga cardinal **infinito numerable** (o sea $\aleph_0$), entonces no podrá existir una biyección (ni un isomorfismo) entre $\mathcal{B}$ y $\mathcal{P}(X)$, para ningún X.

Construcción de $\mathcal{B}$

Un subconjunto de números naturales se dice *cofinito* si su complemento es finito.

Definimos:

$$\mathcal{B} = \{X \subseteq \mathbf{N} : X \text{ es finito o cofinito}\}.$$

Entonces la estructura

$$\langle \mathcal{B}, \cup, \cap, {}^{c}, \emptyset, \mathbf{N} \rangle$$

es un álgebra de Boole.