Introducción a la Lógica y la Computación

Mariana Badano Héctor Gramaglia
Pedro Sánchez Terraf Mauricio Tellechea
Guido Ivetta César Vallero

FaMAF, 1 de septiembre de 2020

Contenidos estimados para hoy

1. Reticulados distributivos
   - Reticulados de partes
   - (Contra)ejemplos
   - Teorema M_3-N_5
   - Intermezzo: Posets y Partes
   - Precalentamiento: Representación de posets
2. Reticulados complementados y álgebras de Boole
   - Leyes de De Morgan
   - Isomorfismo de álgebras de Boole
   - Ejemplos

Avisos

- Por favor, respeten la distribución alfabética de cada comisión.

Reticulados distributivos

Partes de un conjunto $(\mathscr{P}(A), \subseteq) \longleftrightarrow (\mathscr{P}(A), \cup, \cap)$

- Todo $X \in \mathscr{P}(A)$ tiene un **complemento**: un $Y \in \mathscr{P}(A)$ tal que

$$X \cup Y = 1^{\mathscr{P}(A)} = A \qquad X \cap Y = 0^{\mathscr{P}(A)} = \varnothing.$$

Reticulados distributivos

Partes de un conjunto $(\mathscr{P}(A), \subseteq) \longleftrightarrow (\mathscr{P}(A), \cup, \cap)$

- Todo $X \in \mathscr{P}(A)$ tiene un **complemento**: un $Y \in \mathscr{P}(A)$ tal que

$$X \cup Y = 1^{\mathscr{P}(A)} = A \qquad X \cap Y = 0^{\mathscr{P}(A)} = \varnothing.$$

- Las operaciones distribuyen:

$$X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$$
$$X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z).$$

Reticulados distributivos

Partes de un conjunto $(\mathscr{P}(A), \subseteq) \longleftrightarrow (\mathscr{P}(A), \cup, \cap)$

- Todo $X \in \mathscr{P}(A)$ tiene un **complemento**: un $Y \in \mathscr{P}(A)$ tal que

$$X \cup Y = 1^{\mathscr{P}(A)} = A \qquad X \cap Y = 0^{\mathscr{P}(A)} = \varnothing.$$

- Las operaciones distribuyen:

$$X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$$
$$X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z).$$

Definición

L es **distributivo** si para todos los $a, b, c \in L$,

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$$
$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c).$$

Ejemplos

L es **distributivo** si para todos los $a, b, c \in L$,

- $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$.
- $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$.

Ejemplos

L es **distributivo** si para todos los $a, b, c \in L$,

- $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$.
- $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$.

Ejemplo

1. Todos los órdenes totales.
2. $(\mathbb{N}, |)$.
3. $(\mathscr{P}(A), \subseteq)$ para cada conjunto A.

Ejemplos

L es **distributivo** si para todos los $a, b, c \in L$,

- $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$.
- $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$.

Ejemplo

1. Todos los órdenes totales. Por análisis por casos
2. $(\mathbb{N}, |)$.
3. $(\mathscr{P}(A), \subseteq)$ para cada conjunto A.

UNC Universidad Nacional de Córdoba 1613 - 2013 400 AÑOS

Ejemplos

L es **distributivo** si para todos los $a, b, c \in L$,

- $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$.
- $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$.

Ejemplo

1. Todos los órdenes totales. Por análisis por casos
2. $(\mathbb{N}, |)$. Subreticulados también! D_n
3. $(\mathscr{P}(A), \subseteq)$ para cada conjunto A.

Un criterio de distributividad

Sea L un reticulado. $S \subseteq L$ es un **subuniverso** de $(L, \vee, \wedge)$ si es cerrado por las operaciones $\vee$ y $\wedge$. En tal caso, $(S, \vee, \wedge)$ es un **subreticulado** de $(L, \vee, \wedge)$.

Un criterio de distributividad

Sea L un reticulado. $S \subseteq L$ es un **subuniverso** de $(L, \vee, \wedge)$ si es cerrado por las operaciones $\vee$ y $\wedge$. En tal caso, $(S, \vee, \wedge)$ es un **subreticulado** de $(L, \vee, \wedge)$.

Lema

- *Si L es distributivo y L' es isomorfo a L, entonces L' es distributivo*

Un criterio de distributividad

Sea L un reticulado. $S \subseteq L$ es un **subuniverso** de $(L, \vee, \wedge)$ si es cerrado por las operaciones $\vee$ y $\wedge$. En tal caso, $(S, \vee, \wedge)$ es un **subreticulado** de $(L, \vee, \wedge)$.

Lema

- *Si L es distributivo y L' es isomorfo a L, entonces L' es distributivo*
- *Si L es distributivo, entonces todos sus subreticulados lo son.*

Un criterio de distributividad

Sea L un reticulado. $S \subseteq L$ es un **subuniverso** de $(L, \vee, \wedge)$ si es cerrado por las operaciones $\vee$ y $\wedge$. En tal caso, $(S, \vee, \wedge)$ es un **subreticulado** de $(L, \vee, \wedge)$.

Lema

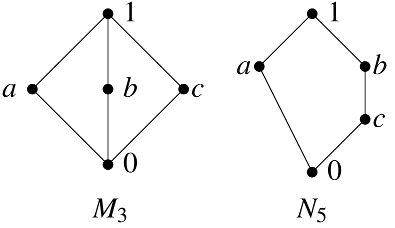
- *Si L es distributivo y L' es isomorfo a L, entonces L' es distributivo*
- *Si L es distributivo, entonces todos sus subreticulados lo son.*

Corolario

*Si L es distributivo y L' es isomorfo a un subreticulado L ("L' se **incrusta** en L"), entonces L' es distributivo.*

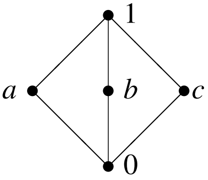
No todos lo son

¡Contraejemplos!

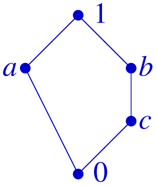


No todos lo son

¡Contraejemplos!

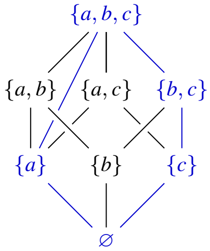


M_3



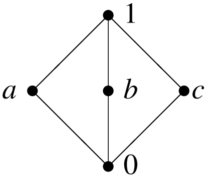
N_5

Subposets pero no subreticulados

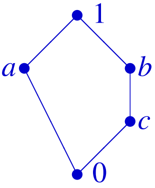


No todos lo son

¡Contraejemplos!

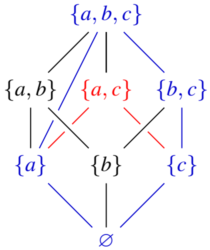


M_3



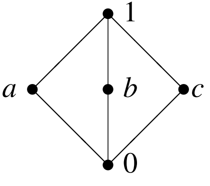
N_5

Subposets pero no subreticulados

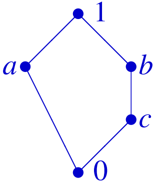


No todos lo son

¡Contraejemplos!

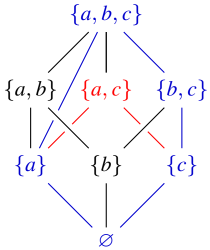


M_3



N_5

Subposets pero no subreticulados



Lema (Propiedad "cancelativa")

Sea L distributivo. Para todos $a, b, c \in L$,

$$\left.\begin{aligned} a \vee b &= a \vee c \\ a \wedge b &= a \wedge c \end{aligned}\right\} \implies b = c.$$

Teorema M_3-N_5

Teorema

Un reticulado L es distributivo si y sólo si ninguno de sus subreticulados es isomorfo a M_3 ni a N_5 (i.e., no se incrustan).

Teorema M_3-N_5

Teorema

Un reticulado L es distributivo si y sólo si ninguno de sus subreticulados es isomorfo a M_3 ni a N_5 (i.e., no se incrustan).

Teóricamente es muy limpio, pero como algoritmo apesta.

Teorema M_3-N_5

Teorema

Un reticulado L es distributivo si y sólo si ninguno de sus subreticulados es isomorfo a M_3 ni a N_5 (i.e., no se incrustan).

Teóricamente es muy limpio, pero como algoritmo apesta.
Para obtener mejores resultados es necesario poder presentar a los reticulados distributivos y sus operaciones de manera más concreta.

Teorema M_3-N_5

Teorema

Un reticulado L es distributivo si y sólo si ninguno de sus subreticulados es isomorfo a M_3 ni a N_5 (i.e., no se incrustan).

Teóricamente es muy limpio, pero como algoritmo apesta.
Para obtener mejores resultados es necesario poder presentar a los reticulados distributivos y sus operaciones de manera más concreta.

Un **teorema de representación** nos permite entender a una familia estructuras "abstractas" en términos de ejemplos concretos (más manejables)

Teorema M_3-N_5

Teorema

Un reticulado L es distributivo si y sólo si ninguno de sus subreticulados es isomorfo a M_3 ni a N_5 (i.e., no se incrustan).

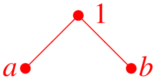
Teóricamente es muy limpio, pero como algoritmo apesta.
Para obtener mejores resultados es necesario poder presentar a los reticulados distributivos y sus operaciones de manera más concreta.

Un **teorema de representación** nos permite entender a una familia estructuras “abstractas” en términos de ejemplos concretos (más manejables)

A continuación, representaremos posets usando partes de conjuntos.

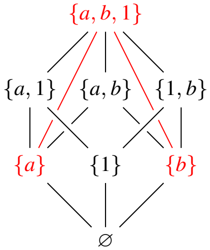
Posets y subconjuntos

Poset P



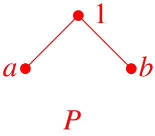
P

Partes $\mathscr{P}(P)$

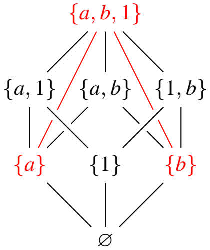


Posets y subconjuntos

Poset P



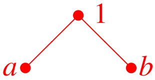
Partes $\mathscr{P}(P)$



Notemos que cada $d \in P$ se corresponde con el **ideal principal** $d{\downarrow} := \{x \in P : x \leq d\}$.

Posets y subconjuntos

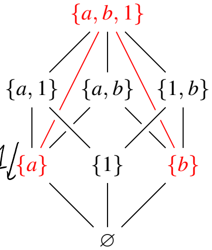
Poset P



$1 \xmapsto{P} \{x \in P : x \leq 1\} =: 1\downarrow$

$\{a, b, 1\}$

Partes $\mathscr{P}(P)$



$y \leq x \leq d$

$\Downarrow$ Transit

$y \leq d.$

$y \in d\downarrow$

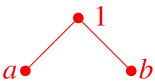
Notemos que cada $d \in P$ se corresponde con el **ideal principal** $d\downarrow := \{x \in P : x \leq d\}$.

$x \in d\downarrow$ & $y \leq x \Rightarrow y \in d\downarrow$

$d \mapsto d\downarrow$ es 1-1

Posets y subconjuntos

Poset P

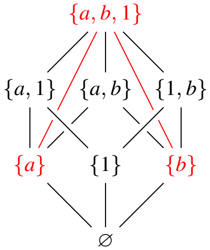


P

$\sup\{a\} = a$

$\sup\{a, b, 1\} = 1$

Partes $\mathscr{P}(P)$



Notemos que cada $d \in P$ se corresponde con el **ideal principal** $d{\downarrow} := \{x \in P : x \leq d\}$.

$d \mapsto d{\downarrow}$ es 1-1

Basta ver que $d = \sup d{\downarrow} = \sup c{\downarrow} = c$.

UNC Universidad Nacional de Córdoba 1613 - 2013 400 AÑOS

Precalentamiento: Representación de posets

De hecho, hay más:

Lema

Para todos $d, c \in P,\ d \leq c \iff d{\downarrow} \subseteq c{\downarrow}$.

Precalentamiento: Representación de posets

De hecho, hay más:

Lema

Para todos $d, c \in P,\ d \leq c \iff d{\downarrow} \subseteq c{\downarrow}.$

$x \in$

$x \in d{\downarrow} \iff x \leq d \leq c$

$\Downarrow$

$x \leq c$

$\Downarrow$

$x \in c{\downarrow}$

Demostración.

- $(\Rightarrow)$ Por la transitividad de $\leq$.

UNC Universidad Nacional de Córdoba 1613 - 2013 400 AÑOS

De hecho, hay más: $d\downarrow = \{x \in P : x \leq d\}$

Lema

Para todos $d, c \in P$, $d \leq c \iff d\downarrow \subseteq c\downarrow$.

Demostración.

- $(\Rightarrow)$ Por la transitividad de $\leq$.
- $(\Leftarrow)$ $d \in c\downarrow$ implica $d \leq c$.

$\underset{\text{reflex}}{d \in} d\downarrow \subseteq c\downarrow$ $\therefore d \leq c$

Precalentamiento: Representación de posets

De hecho, hay más:

Lema

Para todos $d, c \in P,\ d \leq c \iff d{\downarrow} \subseteq c{\downarrow}$.

Demostración.

- $(\Rightarrow)$ Por la transitividad de $\leq$.
- $(\Leftarrow)$ $d \in c{\downarrow}$ implica $d \leq c$.

Teorema

$(P, \leq)$ *es isomorfo a un subposet de* $(\mathscr{P}(P), \subseteq)$.

Precalentamiento: Representación de posets

De hecho, hay más:

Lema

Para todos $d, c \in P, \ d \leq c \iff d{\downarrow} \subseteq c{\downarrow}$.

Demostración.

- $(\Rightarrow)$ Por la transitividad de $\leq$.
- $(\Leftarrow)$ $d \in c{\downarrow}$ implica $d \leq c$.

Teorema

$(P, \leq)$ *es isomorfo a un subposet de* $(\mathscr{P}(P), \subseteq)$.

Un teorema de representación más ajustado nos diría a qué subposets de partes es isomorfo.

Precalentamiento: Representación de posets

De hecho, hay más:

Lema

Para todos $d, c \in P,\ d \leq c \iff d{\downarrow} \subseteq c{\downarrow}$.

Demostración.

- $(\Rightarrow)$ Por la transitividad de $\leq$.
- $(\Leftarrow)$ $d \in c{\downarrow}$ implica $d \leq c$.

Teorema

$(P, \leq)$ *es isomorfo a un subposet de* $(\mathscr{P}(P), \subseteq)$.

Un teorema de representación más ajustado nos diría a qué subposets de partes es isomorfo.

Además "subposet" no es compatible con las operaciones.

Reticulados complementados y álgebras de Boole

Recordemos:

- L es **acotado** si tiene primer elemento 0^L y último elemento 1^L.
- Sea L acotado y sean $a, b \in L$. b es un **complemento** de a si

$$a \vee b = 1^L \qquad a \wedge b = 0^L.$$

  L es **complementado** si todo elemento tiene complemento.

Reticulados complementados y álgebras de Boole

Recordemos:

- L es **acotado** si tiene primer elemento 0^L y último elemento 1^L.
- Sea L acotado y sean $a, b \in L$. b es un **complemento** de a si

$$a \vee b = 1^L \qquad a \wedge b = 0^L.$$

L es **complementado** si todo elemento tiene complemento.

Definición (Álgebra de Boole)

Un **álgebra de Boole** $(B, \vee, \wedge, \neg, 0, 1)$ es una estructura donde $(B, \vee, \wedge, 0, 1)$ es un retículo distributivo acotado y $\neg : B \to B$ da un complemento:

$$a \vee \neg a = 1 \qquad a \wedge \neg a = 0.$$

Leyes de De Morgan

Proposición

En toda álgebra de Boole, se dan

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

Leyes de De Morgan

$$\left.\begin{array}{l} 1 = a \vee b = a \vee c = 1 \\ 0 = a \wedge b = a \wedge c = 0 \end{array}\right\} \Rightarrow b = c.$$

Proposición

En toda álgebra de Boole, se dan

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

$\neg a$ es el único complemento de a

Demostración.

Ver que $\neg x \wedge \neg y$ es complemento de $x \vee y$ y aplicar la propiedad cancelativa.
La segunda ley es análoga.

Isomorfismo de álgebras de Boole

Definición

Un **isomorfismo de álgebras de Boole**
$f : (B, \vee, \wedge, \neg, 0, 1) \to (B, \vee', \wedge', \neg', 0', 1')$ es un iso de retículos
$f : (B, \vee, \wedge) \to (B, \vee', \wedge')$ tal que para todo $x \in B$,

$$f(\neg x) = \neg' f(x) \qquad \text{y} \qquad f(0) = 0' \qquad \text{y} \qquad f(1) = 1'$$

Isomorfismo de álgebras de Boole

Definición

Un **isomorfismo de álgebras de Boole**
$f : (B, \vee, \wedge, \neg, 0, 1) \to (B, \vee', \wedge', \neg', 0', 1')$ es un iso de retículos
$f : (B, \vee, \wedge) \to (B, \vee', \wedge')$ tal que para todo $x \in B$,

$$f(\neg x) = \neg' f(x) \qquad \text{y} \qquad f(0) = 0' \qquad \text{y} \qquad f(1) = 1'$$

Son lo mismo que los isos de posets (inducidos por la estructura de retículo).

Isomorfismo de álgebras de Boole

Definición

Un **isomorfismo de álgebras de Boole**
$f : (B, \vee, \wedge, \neg, 0, 1) \to (B, \vee', \wedge', \neg', 0', 1')$ es un iso de retículos
$f : (B, \vee, \wedge) \to (B, \vee', \wedge')$ tal que para todo $x \in B$,

$$f(\neg x) = \neg' f(x) \qquad \text{y} \qquad f(0) = 0' \qquad \text{y} \qquad f(1) = 1'$$

Son lo mismo que los isos de posets (inducidos por la estructura de retículo).

Teorema

$f : (B, \vee, \wedge, \neg, 0, 1) \to (B, \vee', \wedge', \neg', 0', 1')$ *es iso* $\iff$
$f : (B, \leq) \to (B', \leq')$ *es iso.*

Isomorfismo de álgebras de Boole

Definición

Un **isomorfismo de álgebras de Boole**
$f : (B, \vee, \wedge, \neg, 0, 1) \to (B, \vee', \wedge', \neg', 0', 1')$ es un iso de retículos
$f : (B, \vee, \wedge) \to (B, \vee', \wedge')$ tal que para todo $x \in B$,

$$f(\neg x) = \neg' f(x) \qquad \text{y} \qquad f(0) = 0' \qquad \text{y} \qquad f(1) = 1'$$

Son lo mismo que los isos de posets (inducidos por la estructura de retículo).

Teorema

$f : (B, \vee, \wedge, \neg, 0, 1) \to (B, \vee', \wedge', \neg', 0', 1')$ *es iso* $\iff$
$f : (B, \leq) \to (B', \leq')$ *es iso.*

Demostración.

Si y es complemento de x, $f(x)$ es complemento de $f(y)$ (por estar definido usando el orden), y aplico propiedad cancelativa.

Ejemplos

Bien, ahora a los ejemplos de álgebras de Boole.

Ejemplos

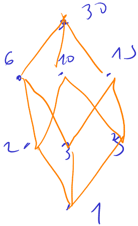
Bien, ahora a los ejemplos de álgebras de Boole.

Ejemplo

- $\mathscr{P}(A)$ para todo A.

Bien, ahora a los ejemplos de álgebras de Boole.

$(\mathcal{P}(\{2,3,5\}), \subseteq) \cong$



Ejemplo

- $\mathscr{P}(A)$ para todo A.
- D_n con $n = p_1 \cdots p_m$ producto de primos distintos.

Ejemplos

Bien, ahora a los ejemplos de álgebras de Boole.

Ejemplo

- $\mathscr{P}(A)$ para todo A.
- D_n con $n = p_1 \cdots p_m$ producto de primos distintos. Es isomorfa a $\mathscr{P}(\{p_1, \ldots, p_m\})$.

Bien, ahora a los ejemplos de álgebras de Boole.

Ejemplo

- $\mathscr{P}(A)$ para todo A.
- D_n con $n = p_1 \cdots p_m$ producto de primos distintos. Es isomorfa a $\mathscr{P}(\{p_1, \ldots, p_m\})$. Es decir, esencialmente parte del ejemplo anterior.

Ejemplos

Bien, ahora a los ejemplos de álgebras de Boole.

Ejemplo

- $\mathscr{P}(A)$ para todo A.
- D_n con $n = p_1 \cdots p_m$ producto de primos distintos. Es isomorfa a $\mathscr{P}(\{p_1, \ldots, p_m\})$. Es decir, esencialmente parte del ejemplo anterior.
- $\ldots$

Ejemplos

Bien, ahora a los ejemplos de álgebras de Boole.

Ejemplo

- $\mathscr{P}(A)$ para todo A.
- D_n con $n = p_1 \cdots p_m$ producto de primos distintos. Es isomorfa a $\mathscr{P}(\{p_1, \ldots, p_m\})$. Es decir, esencialmente parte del ejemplo anterior.
- ...
- ...

UNC Universidad Nacional de Córdoba 1613 - 2013 400 AÑOS

Ejemplos

Bien, ahora a los ejemplos de álgebras de Boole.

Ejemplo

- $\mathscr{P}(A)$ para todo A.
- D_n con $n = p_1 \cdots p_m$ producto de primos distintos. Es isomorfa a $\mathscr{P}(\{p_1, \ldots, p_m\})$. Es decir, esencialmente parte del ejemplo anterior.
- $\ldots$
- $\ldots$

Sí, hay más ejemplos. Pero parece que el conjunto de partes es uno muy importante.

Ejemplos

Bien, ahora a los ejemplos de álgebras de Boole.

Ejemplo

- $\mathscr{P}(A)$ para todo A.
- D_n con $n = p_1 \cdots p_m$ producto de primos distintos. Es isomorfa a $\mathscr{P}(\{p_1, \ldots, p_m\})$. Es decir, esencialmente parte del ejemplo anterior.
- …
- …

Sí, hay más ejemplos. Pero parece que el conjunto de partes es uno muy importante.
Para continuar, podemos imaginarnos formas de asociar una familia de conjuntos a $(B, \vee, \wedge, \neg, 0, 1)$.

Ejemplos

Bien, ahora a los ejemplos de álgebras de Boole.

Ejemplo

- $\mathscr{P}(A)$ para todo A.
- D_n con $n = p_1 \cdots p_m$ producto de primos distintos. Es isomorfa a $\mathscr{P}(\{p_1, \ldots, p_m\})$. Es decir, esencialmente parte del ejemplo anterior.
- ...
- ...

Sí, hay más ejemplos. Pero parece que el conjunto de partes es uno muy importante.

Para continuar, podemos imaginarnos formas de asociar una familia de conjuntos a $(B, \vee, \wedge, \neg, 0, 1)$.

Fuerza bruta

Una estrategia a lo bestia (exponencial)

Si todo falla, considerá todas las combinaciones.

Fuerza bruta

Una estrategia a lo bestia (exponencial)

Si todo falla, considerá todas las combinaciones.

En este caso, es arrancar con $\mathscr{P}(B)$.
Esta estrategia de fuerza bruta también se usará en la tercera parte de la materia.

Fuerza bruta

Una estrategia a lo bestia (exponencial)

Si todo falla, considerá todas las combinaciones.

En este caso, es arrancar con $|\mathscr{P}(B)| = 2^{|B|} > |B|$.
Esta estrategia de fuerza bruta también se usará en la tercera parte de la materia.

¿Cómo asociamos a cada $b \in B$ un $F(b) \subseteq B$?

Ayuda: usemos el orden (y b) para definir $F(b)$.

Teorema de Representación de álgebras de Boole finitas

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

Teorema

Para toda álgebra de Boole finita B existe A tal que B es isomorfa a $\mathscr{P}(A)$.

¿Quién es A?

¿Qué objetos juegan el rol de elementos de A?

Átomos

Sea B un poset finito acotado con al menos dos elementos.

Definición

$a \in B$ es un **átomo** si a cubre a 0. $At(B)$ es el conjunto de los átomos de B.

Átomos

a átomo $\iff$ $a > 0$ y $\nexists x : 0 < x < a$.

Sea B un poset finito acotado con al menos dos elementos.

Definición

$a \in B$ es un **átomo** si a cubre a 0. $At(B)$ es el conjunto de los átomos de B.

arbitrario.

Ejercicios

- Supongamos $a \in At(B)$. ¿Cuántos valores posibles puede dar $b \wedge a$?

  Actividad en Aula virtual!
- Encontrar el conjunto de átomos de D_n.
- Sea $a \leq b$. Entonces a es átomo de $B \iff a$ es átomo del subposet $b\downarrow$.