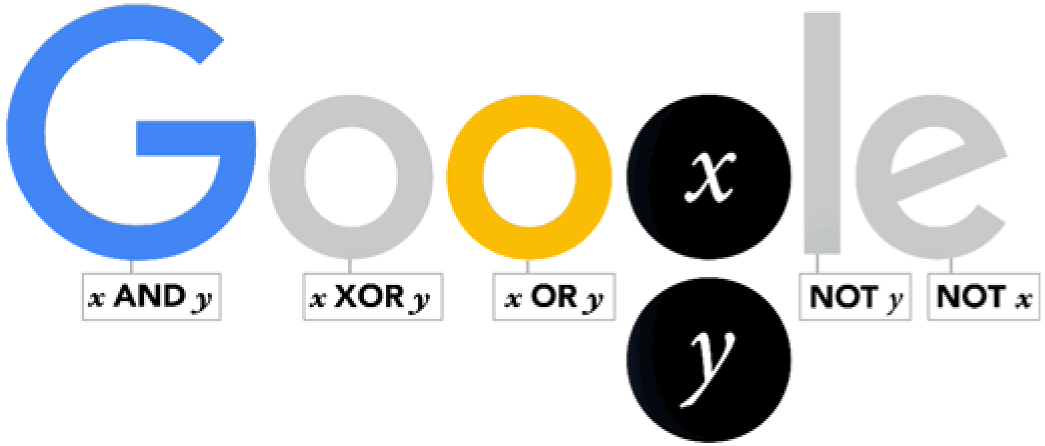
ÁLGEBRAS DE BOOLE

Gregorio Hernández

UPM

Matemática Discreta I


x
y
x AND y
x XOR y
x OR y
NOT y
NOT x

ÁLGEBRAS DE BOOLE

Un álgebra de Boole es un retículo complementario y distributivo

$(P(X), \subset)$ y $(D_{30}, |)$ son álgebras de Boole

$(D_{20}, |)$ no es complementario, luego no es álgebra de Boole

Propiedades:

(1) Involutiva $(a')' = a \quad \forall a \in A$

(2) Leyes de De Morgan

$$(a \vee b)' = a' \wedge b' \quad \text{y} \quad (a \wedge b)' = a' \vee b' \qquad \forall a,b \in A$$

(1) Por ser a' el complementario de a se cumple que $a \vee a' = 1$ y $a \wedge a' = 0$

Si además el complementario es único, $(a')' = a$

ÁLGEBRAS DE BOOLE

Un álgebra de Boole es un retículo complementario y distributivo

$(P(X), \subset)$ y $(D_{30}, |)$ son álgebras de Boole

$(D_{20}, |)$ no es complementario, luego no es álgebra de Boole

Propiedades:

(1) Involutiva $(a')' = a \quad \forall a \in A$

(2) Leyes de De Morgan

$$(a \vee b)' = a' \wedge b' \quad \text{y} \quad (a \wedge b)' = a' \vee b' \quad \forall a,b \in A$$

(2) Hemos de probar que el complementario de $a \vee b$ es $a' \wedge b'$

$$(a \vee b) \vee (a' \wedge b') = a \vee (b \vee (a' \wedge b')) = a \vee ((b \vee a') \wedge (b \vee b')) =$$
$$= a \vee ((b \vee a') \wedge 1) = a \vee (b \vee a') = 1$$

$$(a \vee b) \wedge (a' \wedge b') = ((a \vee b) \wedge a') \wedge b' = ((a \wedge a') \vee (b \wedge a')) \wedge b' =$$
$$= (1 \vee (b \wedge a')) \wedge b') = b \wedge a' \wedge b' = 0$$

Construcción de ÁLGEBRAS DE BOOLE

El producto de álgebras de Boole es un álgebra de Boole

Proposición

Si A es un álgebra de Boole, B un retículo y $f{:}A\to B$ un isomorfismo de conjuntos ordenados entonces B es un álgebra de Boole

Dem.:

(1) B es acotado

f es isomorfismo de retículos luego $f(1_A)$ es el máximo de B y $f(0_A)$ es el mínimo de B

(2) B es complementario

Dado $b\in B$, $\exists! a \in A$, tal que $f(a) = b$, $f(a')$ es el complementario de b

$$b \vee f(a') = f(a) \vee f(a') = f(a \vee a') = f(1_A) = 1_B$$

$$b \wedge f(a') = f(a) \wedge f(a') = f(a \wedge a') = f(0_A) = 0_B$$

Construcción de ÁLGEBRAS DE BOOLE

El producto de álgebras de Boole es un álgebra de Boole

Proposición

Si A es un álgebra de Boole, B un retículo y $f:A \to B$ un isomorfismo de conjuntos ordenados entonces B es un álgebra de Boole

Dem.:

(3) B es distributivo

$\forall x,y,z \in B$ sean $x=f(a)$, $y=f(b)$, $z=f(c)$

$$(x \vee y) \wedge z = (f(a) \vee f(b)) \wedge f(c) = f(a \vee b) \wedge f(c) = f((a \vee b) \wedge c) =$$
$$f((a \wedge c) \vee (b \wedge c)) = f(a \wedge c) \vee f(b \wedge c)) = (f(a) \wedge f(c)) \vee (f(b) \wedge f(c)) =$$
$$= (x \wedge z) \vee (y \wedge z)$$

Y análogamente la otra propiedad distributiva

Construcción de ÁLGEBRAS DE BOOLE

Proposición

Si $(A, \leq)$ es un álgebra de Boole, $x \in A$, $A_x = \{z \in A \,/\, z \leq x\}$ es un álgebra de Boole

Dem.:

(1) A_x es subretículo

Si $a,b \in A_x$ entonces $a \leq x$, $b \leq x$, luego $\sup\{a,b\} \leq x$, $\inf\{a,b\} \leq x$

(2) A_x es acotado   El máximo es **x** y el mínimo es $0 = \min(A)$

(3) A_x es distributivo, pues las operaciones $\wedge$, $\vee$ son cerradas en A_x

(4) A_x es complementario. Dado $z \in A_x$, z' su complementario en A

$z' \wedge x$ es el complementario en A_x porque

$$z \vee (z' \wedge x) = (z \vee z') \wedge (z \vee x) = 1 \wedge x = x$$

$$z \wedge (z' \wedge x) = (z \wedge z') \wedge x) = 0 \wedge x = 0$$

TEOREMA

$\boxed{(D_n,|) \text{ es álgebra de Boole} \quad \Leftrightarrow \quad n = p_1 \cdot p_2 \cdot \ldots \cdot p_k \quad \text{con } p_i \neq p_j \quad i \neq j}$

Dem.:

$\Rightarrow$) $(D_n, |)$ es siempre retículo acotado de mínimo 1 y máximo n
Así si a y a' son complementarios en D_n será mcd(a,a') = 1 y
mcm(a,a´) = n, luego aa' = n, por lo que a' = n/a

Supongamos que $n = p^r q$ con $r>1$
Entonces $a = p$ no tiene complementario en D_n , pues si lo
hubiera sería $a' = p^{r-1}q$ con mcd(a,a') $\neq 1$

Por tanto, todo factor primo de n tiene exponente 1

TEOREMA

$\boxed{(D_n,|) \text{ es álgebra de Boole } \Leftrightarrow \quad n = p_1 \cdot p_2 \cdot \ldots \cdot p_k \quad \text{con } p_i \neq p_j \quad i \neq j}$

Dem.:

$\Leftarrow$) Para demostrar que D_n es álgebra de Boole construimos un isomorfismo de conjuntos ordenados $P(X) \to D_n$ para cierto X

Si $n = p_1 \cdot p_2 \cdot \ldots \cdot p_k$ llamamos $X = \{p_1, p_2, \ldots, p_k\}$ y definimos

$$\begin{aligned} f : P(X) &\to D_n \\ A &\to f(A) \\ \varnothing &\to 1 \end{aligned}$$

f(A) es el producto de los primos que aparecen en A (todos distintos)

f es una biyección por construcción

f es isomorfismo de conjuntos ordenados porque
$A \subset B \Leftrightarrow f(A) \mid f(B)$

Por tanto, $(D_n,|)$ es álgebra de Boole por el teorema anterior

TEOREMA

Toda álgebra de Boole finita es isomorfa al álgebra de Boole de las partes de un conjunto finito

Es decir, dada $(A,\leq)$ álgebra de Boole finita, existe un conjunto C tal que $(A, \leq) \approx (P(C), \subset)$

Lema 1

Sea A álgebra de Boole finita y $M = \{a_1, a_2, \ldots, a_k\}$ el conjunto de los elementos minimales de $A - \{0\}$. Entonces $\forall\ a \in A - \{0\}$ se verifica que

$$a = a_i \vee \ldots \vee a_j \qquad \text{con } a_i \ldots a_j \in M$$

Lema 2

La descomposición del lema anterior es única salvo el orden de los elementos minimales (no hay repetidos)

Lema 1

Sea A álgebra de Boole finita y $C = \{a_1, a_2, \ldots, a_k\}$ el conjunto de los elementos minimales de $A - \{0\}$. Entonces $\forall\, a \in A - \{0\}$ se verifica que

$$a = a_i \vee \ldots \vee a_j \qquad \text{con } a_i \ldots a_j \in C$$

Dem.: Si a es minimal en $A - \{0\}$ ya está, si no lo es existe $a_i \in C$ con $a_i \leq a$ pues A es finita.

Así $a = a_i \vee a'$ con $a' = a \wedge a'_i$

Si a' minimal ya está. Si no es así se repite el razonamiento
Como A es finita en un número finito de pasos llegaremos a expresar a como disyunción de minimales.

Corolario

En las condiciones del lema, $a_1 \vee \ldots \vee a_k = 1$

Lema 2

La descomposición del lema anterior es única salvo el orden de los elementos minimales y elementos repetidos.

Dem.:

Supongamos que hay dos descomposiciones de a en minimales

$$a = a_{i_1} \vee \cdots \vee a_{i_r} = b_{j_1} \vee \cdots \vee b_{j_s}$$

Así $a_{i_1} = a \wedge a_{i_1} = a_{i_1} \wedge (a_{i_1} \vee \cdots \vee a_{i_r}) = a_{i_1} \wedge (b_{j_1} \vee \cdots \vee b_{j_s})$

$$a_{i_1} = (a_{i_1} \wedge a_{i_1}) \vee \cdots \vee (a_{i_1} \wedge a_{i_r}) = (a_{i_1} \wedge b_{j_1}) \vee \cdots \vee (a_{i_1} \wedge b_{j_s})$$

Como todas las a’s y b’s son minimales en A – {0}

$a_{i_1} \wedge b_{j_1} = \cdots = a_{i_1} \wedge b_{j_s} = 0$ Luego $a_{i_1} = 0$

Contradicción!!

TEOREMA

Toda álgebra de Boole finita es isomorfa al álgebra de Boole de las partes de un conjunto finito

Es decir, dada (A,≤) álgebra de Boole finita, existe un conjunto C tal que (A, ≤) ≈ (P(C), ⊂)

Dem.:

Siguiendo la notación del lema 1, el conjunto C será el de los elementos minimales de A – {0}

Se construye la aplicación f: A → P(C)

$$a \to \{a_{i_1}, \cdots, a_{i_r}\}$$
$$0 \to \varnothing$$

siendo $a = a_{i_1} \vee \cdots \vee a_{i_r}$ la descomposición del lema 1

Debemos probar que f es una biyección que conserva el orden con lo que f será un isomorfismo de conjuntos ordenados

TEOREMA

Toda álgebra de Boole finita es isomorfa al álgebra de Boole de las partes de un conjunto finito

Dem. (sigue): f: A $\to$ P(C)

$$a \to \{a_{i_1}, \cdots, a_{i_r}\} \qquad a = a_{i_1} \vee \cdots \vee a_{i_r}$$

$$0 \to \varnothing$$

f es inyectiva, si f(a) = f(b) entonces $\{a_{i_1}, \cdots, a_{i_r}\} = \{b_{j_1}, \cdots, b_{j_s}\}$

luego, $a = a_{i_1} \vee \cdots \vee a_{i_r} = b_{j_1} \vee \cdots \vee b_{j_s} = b$

f es suprayectiva, dado un subconjunto H de C, $\{c_{i_1}, \cdots, c_{i_r}\}$
el elemento *c* de A $c = c_{i_1} \vee \cdots \vee c_{i_r}$ es tal que f(c) = H

TEOREMA

Toda álgebra de Boole finita es isomorfa al álgebra de Boole de las partes de un conjunto finito

Dem. (sigue): f: A $\to$ P(C)

$$a \to \{a_{i_1}, \cdots, a_{i_r}\} \qquad\qquad a = a_{i_1} \vee \cdots \vee a_{i_r}$$

$$0 \to \varnothing$$

f conserva el orden, es decir, a$\leq$b $\Leftrightarrow$ f(a) $\subset$ f(b)

Si f(a) $\subset$ f(b) es claro que a$\leq$b

Si a$\leq$b entonces a$\wedge$b = a luego

$(a_i \vee \ldots \vee a_s) \wedge (b_i \vee \ldots \vee b_t) = a_i \vee \ldots \vee a_s$ aplicando distributiva

$$\bigcup_{\substack{i=1,\ldots,s \\ j=1,\ldots,t}} (a_i \wedge b_j) = a_i \vee \ldots \vee a_s$$

Por la unicidad, para cada i=1,…,s existe j tal que $a_i \wedge b_j = a_i \Rightarrow a_i = b_j$

Por tanto, $\{a_i, \ldots, a_s\} \subset \{b_i, \ldots, b_t\}$ es decir, f(a) $\subset$ f(b)

TEOREMA

Toda álgebra de Boole finita es isomorfa al álgebra de Boole de las partes de un conjunto finito

Corolario

Para toda álgebra de Boole finita existe n tal que $|A| = 2^n$

ÁLGEBRAS DE BOOLE $\{0, 1\}^n$

El conjunto B = {0,1} con las operaciones $\vee$ y $\wedge$ definidas por:

$\vee$	0	1
0	0	1
1	1	1

$\wedge$	0	1
0	0	0
1	0	1

es un álgebra de Boole y, por tanto, también lo es $B^n = B\times \cdots \times B$

Teorema

Si C es un conjunto de n elementos, entonces las álgebras de Boole P(C) y B^n son isomorfas

Dem.: Si $C = \{c_1, \ldots, c_n\}$ se define $f: P(C) \to B^n$ así:

Para $S \subset C$, $f(S) = (a_1, \ldots, a_n)$ con $a_j = 1$ si $c_j \in S$, $a_j = 0$ si $c_j \notin S$

Se comprueba fácilmente que f es una biyección que conserva el orden, por lo que es un isomorfismo de álgebras de Boole