Tema 1. Relaciones de Orden. Algebras de Boole

1.1. Conjuntos

→ <u>Definiciones</u>:

Un conjunto es una colección de objetos distintos. Un conjunto se puede describir de forma extensiva, enumerando todos sus elementos, o de forma comprensiva, describiendo una propiedad que cumplen exclusivamente sus elementos. Por ejemplo, $A = \{a, e, i, o, u\}$ y $A = \{x, tales\ \ que\ es\ x\ una\ vocal\ \}$, son la forma extensiva y comprensiva, respectivamente, de describir el mismo conjunto.

El cardinal de un conjunto es el número de elementos del mismo.

El conjunto vacío, $\emptyset$, es el conjunto que no tiene ningún elemento. Por tanto, su cardinal es 0.

El conjunto A es un subconjunto del conjunto B, si todo elemento de A es también un elemento de B. Se denota por $A \subseteq B$.

Dos conjuntos A y B son iguales, si tienen los mismos elementos. Por tanto, si se verifica que $A \subseteq B$ y $B \subseteq A$.

Si A es un conjunto, el conjuntos partes de A , es el conjunto formado por todos los subconjuntos de A, y se denota por $\wp(A)$.

→ <u>Operaciones con conjuntos</u>:

Dados dos conjuntos A y B , se definen las siguientes operaciones:

1. Unión de conjuntos: $A \cup B = \{x \ ; \ \ x \in A \quad o \ \ x \in B \ \}$
2. Intersección de conjuntos: $A \cap B = \{x \ ; \ \ x \in A \quad y \ \ x \in B \ \}$
3. Si $A \subseteq X$, el complementario de A en X : $A' = \{x \ ; \ \ x \in X \quad y \ \ x \notin A \ \}$
4. Producto cartesiano: $A \times B = \{\ (a, b) \ ; \ \ a \in A \quad y \ \ b \in B\}$

Algunas propiedades:

Asociativas: $(A \cup B) \cup C = A \cup (B \cup C)$; $(A \cap B) \cap C = A \cap (B \cap C)$

Conmutativas: $A \cup B = B \cup A$; $A \cap B = B \cap A$

Elemento neutro: $A \cup \emptyset = A$; $A \cap X = X$ (donde X es el conjunto referencia)

Distributivas: $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$

$(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$

$(A \cup B) \times C = (A \times C) \cup (B \times C)$

$(A \cap B) \times C = (A \times C) \cap (B \times C)$

Cardinal del producto: $|A \times B| = |A| \cdot |B|$

1.2. Relaciones Binarias

→ Definiciones:

Una relación binaria R entre dos conjuntos A y B, es un subconjunto del producto cartesiano $A \times B$.

Si $R \subseteq A \times B$ y $(a, b) \in R$, diremos que a está relacionado con b mediante R, y lo expresaremos de la forma $a\, R\, b$.

Si A y B son iguales, es decir, si $R \subseteq A \times A$, se dirá que R es una relación en A.

El dominio de R es el conjunto $Dom\,(R) = \{\, a \in A \;;\; \exists\, b \in B \;\; verificando \;\; a\, R\, b\}$

El rango de R es el conjunto $Rang\,(R) = \{b \in B \;;\; \exists\, a \in A \;\; verificando \;\; x\, R\, b\}$

Claramente $Dom\,(R) \subseteq A$ y $Rang\,(R) \subseteq B$

Al ser una relación un subconjunto, admite las representaciones extensiva y comprensiva. Además se puede representar mediante diagramas de Venn, y mediante una matriz, donde las filas corresponden al conjunto inicial A, y las columnas al conjunto final B.

→ Operaciones con relaciones:

Sean R y S relaciones entre los conjuntos A y B, y T una relación entre los conjuntos B y C. Se pueden definir las siguientes relaciones:

R unión S: $a\,(R \cup S)\, b$ si y sólo si $a\, R\, b \;\; o \;\; a\, S\, b$

R intersección S: $a\,(R \cap S)\, b$ si y sólo si $a\, R\, b \;\; y \;\; a\, S\, b$

Complementario de R: $a\, \bar{R}\, b$ si y sólo si no es $a\, R\, b$

Relación inversa de R : $R^{-1} \subseteq B \times A$, $b\, R^{-1}\, a$ si y sólo si $a\, R\, b$

Composición de R y T : $(T \circ R) \subseteq A \times C$,

$$a\,(T \circ R)\,c \quad \text{si y sólo si} \ \exists\, b \in B \ ; \ a\,R\,b \quad y \quad b\,T\,c$$

1.3. Aplicaciones

→ Definiciones:

Una aplicación f de A en B, es una relación entre A y B, en la que cada elemento de A está relacionado con un único elemento de B. Se denota por $f{:}\,A \longrightarrow B$.
Si $(a,b) \in f$, se suele escribir $f(a) = b$.

Al ser una relación, su dominio es $Dom\,(f) = \{\, a \in A \ ; \ \exists\, b \in B \ \ con\, f(a) = b\} = A$

Y su imagen o rango $Im\,(f) = Rang\,(f) = \{b \in B \ ; \ \exists\, a \in A \ \ con\, f(a) = b\}$

La imagen recíproca de un elemento b de B es $f^{-1}(b) = \{a \in A\,;\ f(a) = b\}$

→ Tipos de aplicaciones: Sea $f{:}\,A \longrightarrow B$ una aplicación.

f es inyectiva si y sólo si $\forall\, a, a' \in$ A, si $a \neq a'$, entonces $f(a) \neq f(a')$

f es suprayectiva o sobreyectiva si y sólo si $\forall\, b \in B \ \ \exists\, a \in A$ tal que $f(a) = b$. Esta condición es equivalente a que $Im\,(f) = B$.

f es biyectiva si es a la vez inyectiva y suprayectiva. Esta condición es equivalente a que $\forall\, a \in A$ existe un único $b \in B$ tal que $f(a) = b$.

1.4. Relaciones en un conjunto

→ Definiciones. Sea R una relación en A; es decir $R \subseteq A \times A$. Se dice que:
R es reflexiva si $\forall\, a \in A$ se cumple que $a\,R\,a$
R es irreflexiva si $\forall\, a \in A$ no se cumple $a\,R\,a$
R es simétrica si $\forall\, a, b \in A$ se cumple que si $a\,R\,b$, entonces $b\,R\,a$
R es antisimétrica si $\forall\, a, b \in A$ se cumple que si $a\,R\,b$, y $b\,R\,a$ entonces $a = b$
R es transitiva si $\forall\, a, b, c \in A$ se cumple que si $a\,R\,b$, y $b\,R\,c$ entonces $a\,R\,c$
R es circular si $\forall\, a, b, c \in A$ se cumple que si $a\,R\,b$, y $b\,R\,c$ entonces $c\,R\,a$

1.5. Relaciones de equivalencia

→ Definiciónes.

Una relación R en un conjunto A es una relación de equivalencia si verifica las siguientes propiedades:

1. Reflexiva: $\forall\, a \in A$ se verifica que $a\, R\, a$.
2. Simétrica: : $\forall\, a, b\ \in A$ se cumple que si $a\, R\, b$, entonces $b\, R\, a$.
3. Transitiva: $\forall\, a, b, c \in A$, se tiene que si $a\, R\, b$ y $b\, R\, c$, entonces $a\, R\, c$.

Si R es una relación de equivalencia en un conjunto A, para todo $a \in A$, la clase de equivalencia del elemento a, se define como

$$[a] = \{x \in A\ ;\ \ x\, R\, a\}$$

Y el conjunto cociente, es el conjunto de todas las clases de equivalencia:

$$A/_R = \{[a]\ ;\ \ a \in A\}$$

→ <u>Teorema</u> : Si R es una relación de equivalencia en A, entonces $A/_R = \{[a]\ ;\ \ a \in A\}$ es una partición de A

→ <u>Teorema</u>: Sea $\{A_1,\ A_2, \dots, A_i, \dots\ \}$ una partición de A, entonces la relación R definida en A por $a\, R\, b \quad \Leftrightarrow \quad \exists\, i\ \in I$ tal que $a, b \in A_i$, es una relación de equivalencia en A

1.6. Relaciones de orden

→ <u>Definiciones</u>: Una relación R en un conjunto A es una relación de orden si verifica las siguientes propiedades:

4. Reflexiva: $\forall\, a \in A$ se verifica que $a\, R\, a$.
5. Antisimétrica: : $\forall\, a, b \in A$, tales que $a\, R\, b$ y $b\, R\, a$ se verifica que $a = b$.
6. Transitiva: $\forall\, a, b, c \in A$, se tiene que si $a\, R\, b$ y $b\, R\, c$, entonces $a\, R\, c$.

Un conjunto ordenado (A, R) es un par formado por un conjunto A y una relación de orden R definida en él.

→ <u>Ejemplos</u>:

$(\mathbb{N}\ ,\ \leq)$

$(\mathbb{N}\ ,\ /)$, donde / es la relación de divisibilidad (a/b si existe $n\ \in \mathbb{N}$ tal que $b = a \cdot n$)

$(D_n\ ,\ /)$, donde D_n es el conjunto de los números naturales que dividen a $n \in \mathbb{N}$

$(\wp(S)\ ,\ \subseteq)$, para cualquier conjunto S

$(\mathbb{Z},\ /)$ <u>NO</u> es un conjunto ordenado, ya que no cumple la propiedad antisimétrica.

→ <u>Definiciones</u>: Los elementos a y b del conjunto ordenado (A, R) se dicen comparables si $a\, R\, b$ o $b\, R\, a$.

(A, R) es un conjunto totalmente ordenado si dos elementos cualesquiera de A son comparables. Se dice entonces que R es un orden total. En caso contrario, R es un orden parcial.
$(\mathbb{N}, \leq)$ es totalmente ordenado
$(\mathbb{N}, /)$, $(D_n, /)$ y $(\wp(S), \subseteq)$ son conjuntos parcialmente ordenados.

→ Diagramas de Hasse.
El diagrama de Hasse de un conjunto ordenado finito es una representación del mismo en la que cada elemento se representa por un punto del plano.
Si $a\,R\,b$ se dibuja a por debajo de b , y se unen por medio de un segmento.
Finalmente, se suprimen los segmentos que corresponden a la propiedad transitiva, es decir, si $a\,R\,b$ y $b\,R\,c$, se suprime el segmento correspondiente a $a\,R\,c$.

→ Órdenes en el conjunto producto.

Si (A, R) y (B, S) son dos conjuntos ordenados, en el conjunto producto $A \times B$ se pueden definir dos relaciones de orden:

Orden Producto: $(a, b)\; Prod\; (c, d) \;\Leftrightarrow\; a\,Rc \;\; y \;\; b\,Sd$

Orden lexicográfico : $(a, b)\; Lex\; (c, d) \;\Leftrightarrow\; \begin{cases} a \neq c \;\; y \;\; a\,R\,c \\ a = c \;\; y \;\; b\,S\,d \end{cases}$

Si (A, R) y (B, S) son dos conjuntos totalmente ordenados, entonces el conjunto $(A \times B, Lex)$ es también totalmente ordenado. Sin embargo, el conjunto producto $(A \times B, Prod)$ no es necesariamente totalmente ordenado.

1.7. Elementos característicos en un conjunto ordenado

→ Definiciones: Sea $(A, \leq)$ un conjunto ordenado, y S un subconjunto no vacío de A.

$M \in A$ es un maximal de A si no existe $x \neq M$, $x \in A$, tal que $M \leq x$.
$m \in A$ es un minimal de A si no existe $x \neq m$, $x \in A$, tal que $x \leq m$.
$M \in A$ es un máximo de A si $\forall\, x \in A$, es $x \leq M$.
$m \in A$ es un mínimo de A si $\forall\, x \in A$, es $m \leq x$.

$C \in A$ es cota superior de S si $\forall\, x \in S$, es $x \leq C$.
$c \in A$ es cota inferior de S si $\forall\, x \in S$, es $c \leq x$.
$s \in A$ es supremo (o mínima cota superior) de S , si es cota superior de S, y para toda C cota superior de S, se tiene que $s \leq C$.
$i \in A$ es ínfimo (o máxima cota inferior) de S , si es cota inferior de S, y para toda c cota inferior de S, se tiene que $c \leq i$.

→ Propiedades

Si $(A, \leq)$ es finito, entonces A tiene al menos un elemento maximal y otro minimal.
Si $(A, \leq)$ es finito, entonces A tiene a lo sumo un elemento máximo y otro mínimo.
Si S es un subconjunto no vacío de A, entonces S tiene a lo sumo un elemento supremo y otro ínfimo.
Máximo, mínimo, supremo e ínfimo de S, si existen, son únicos.
Si un conjunto tiene máximo, se denota por **1** (siempre que no pueda haber confusión), y se llama elemento unidad.
Si un conjunto tiene mínimo, se denota por **0** (siempre que no pueda haber confusión), y se llama elemento cero.

→ Ordenación topológica

Sea $(A, \leq)$ un conjunto finito ordenado. Entonces, existe al menos un orden total $(A, <)$ que lo contiene; es decir, tal que si $a \leq b$ entonces $a < b$.

Para obtener dicho orden, se elige un a_1 elemento minimal de A; después un a_2 elemento minimal de $A - \{a_1\}$; seguidamente un a_3 elemento minimal de $A - \{a_1, a_2\}$; … seguidamente un a_i elemento minimal de $A - \{a_1, a_2, \dots, a_{i-1}\}$, …y así sucesivamente. Como A es finito, este proceso terminará en un número finito de pasos, y se habrá obtenido un orden total para los elementos de A:

$$a_1 < a_2 < \cdots < a_i \dots < a_n$$

Este orden recibe el nombre de orden topológico.

1.8. Retículos

→ Definición.

Un conjunto ordenado $(L, \leq)$ es un retículo si $\forall\, a, b \in L$ existen $sup\,\{a, b\} \in L$ e $inf\,\{a, b\} \in L$

→ Ejemplos

$(\mathbb{N}, \leq)$ es un retículo: $sup_{\leq}\{a, b\} = \max\{a, b\}$ y $inf_{\leq}\{a, b\} = \min\{a, b\}$
$(\mathbb{N}, /)$ y $(D_n, /)$ son retículos : $sup_{/}\{a, b\} = \mathrm{mcm}\{a, b\}$ y $inf_{/}\{a, b\} = \mathrm{mcd}\{a, b\}$
$(\wp(S), \subseteq)$ es un retículo: $sup_{\subseteq}\{A, B\} = A \cup B$ y $inf_{\subseteq}\{A, B\} = A \cap B$

→ Propiedades

Si $(L, \leq)$ es un retículo, entonces $\forall\, a, b, c \in L$, se tiene que:

1. $inf_{\leq}\{a, b\} \leq a, b \leq sup_{\leq}\{a, b\}$
2. Si $a \leq c$ y $b \leq c$, entonces $sup_{\leq}\{a, b\} \leq c$
3. Si $c \leq a$ y $c \leq b$, entonces $c \leq inf_{\leq}\{a, b\}$
4. Si $a \leq b$ y $c \leq d$, entonces $sup_{\leq}\{a, c\} \leq sup_{\leq}\{b, d\}$ e $inf_{\leq}\{a, c\} \leq inf_{\leq}\{b, d\}$

5. $a \leq b \Leftrightarrow sup_{\leq} \{a, b\} = b \quad \Leftrightarrow inf_{\leq} \{a, b\} = a$

→ <u>Definición de retículo a partir de dos operaciones</u>

Un retículo es una terna $(L, \vee, \wedge)$ donde L es un conjunto, y $\vee$, $\wedge$ son dos operaciones binarias definidas en L, verificando las siguientes propiedades:

1. Idempotente: $a \vee a = a$, $a \wedge a = a$, para todo $a \in L$
2. Conmutativa: $a \vee b = b \vee a$, $a \wedge b = b \wedge a$, para todo $a, b \in L$
3. Asociativa: $(a \vee b) \vee c = a \vee (b \vee c)$, $(a \wedge b) \wedge c = a \wedge (b \wedge c)$, para todo $a, b, c \in L$
4. Absorción: $a \vee (b \wedge a) = a$, $a \wedge (b \vee a) = a$, para todo $a, b \in L$

Parecería que las dos definiciones de retículo son totalmente independientes, que no tienen ninguna relación. Pero no es así, según se muestra en la siguiente Proposición.

→ <u>Proposición</u>: Las dos definiciones anteriores son equivalentes. En efecto,

Si $(L, \leq)$ es un retículo según la primera definición, considerando las operaciones

$$a \vee b = sup\,\{a, b\} \quad \text{y} \quad a \wedge b = inf\,\{a, b\}$$

se tiene que $(L, \vee, \wedge)$ es un retículo según la segunda definición.

Y si $(L, \vee, \wedge)$ es un retículo según la segunda definición, considerando la relación

$$a \leq b \Leftrightarrow a \vee b = b \Leftrightarrow a \wedge b = a$$

se tiene que $(L, \leq)$ es un retículo según la primera definición.

A partir de ahora, se utilizará cualquiera de las definiciones, sabiendo que son equivalentes

→ <u>Subretículos</u>.

Dado un retículo $(L, \leq)$, y S un subconjunto no vacío de L, se dice que $(S, \leq)$ es un subretículo de L si se verifica que:

1. $(S, \leq)$ es retículo
2. Para todo $a, b \in S$, se verifica que $sup_S\{a, b\} = sup_L\{a, b\}$ e $inf_S\{a, b\} = inf_L\{a, b\}$.

→ <u>Ejemplos</u>

$(D_n, /)$ es un subretículo de $(\mathbb{N}, /)$

$(S = \{1, 2, 3\}, /)$ no es subretículo de $(D_{12}, /)$

$(S = \{1, 2, 3, 4, 12\}, /)$ no es subretículo de $(D_{12}, /)$

$(S = \{1, 2, 3, 6\}, /)$ es subretículo de $(D_{12}, /)$

→ Homomorfismo de retículos.

1. Sean (A,R) y (B,S) conjuntos ordenados. La aplicación $f : A \longrightarrow B$ es un homomorfismo entre conjuntos ordenados si conserva el orden, es decir,
   si $a\,R\,b$, entonces $f(a)\,S\,f(b)$
2. Sean (L,R) y (M, S) retículos. La aplicación $f : L \longrightarrow M$ es un homomorfismo entre retículos si

   $f\,(sup_R\{a,b\}) = sup_S\{f(a), f(b)\}$ y $f\,(inf_R\{a,b\}) = inf_S\{f(a), f(b)\}$

3. Sean $(L, \vee, \wedge)$ y $(M, \vee', \wedge')$ retículos. La aplicación $f : L \longrightarrow M$ es un homomorfismo entre retículos si

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

Los diagramas de Hasse de retículos isomorfos tienen la misma estructura.

→ Propiedades de los retículos

Un retículo es acotado si posee elemento máximo y mínimo. En retículos genéricos, se designa por **1** al elemento máximo y por **0** al elemento mínimo. El **1** es el elemento neutro para la operación $\wedge$, y el **0** el elemento neutro para la operación $\vee$.

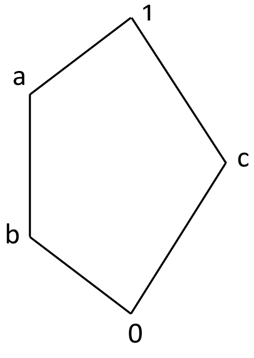
Un retículo $(L, \vee, \wedge)$ es distributivo si $\forall\ a,b,c \in L$ se verifica:

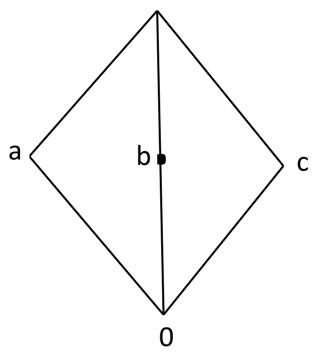
$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c) \quad \text{y} \quad a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$$

→ Ejemplos:

$(D_n,/)$ es distributivo para todo $n \in \mathbb{N}$.

Los siguientes retículos no son distributivos, ya que $a \wedge (b \vee c) \neq (a \wedge b) \vee (a \wedge c)$





→ Teorema:
Un retículo es no distributivo si y sólo si tiene un subretículo isomorfo a uno de los dos retículos anteriores.

→ Definiciones:
Sea $(L, \vee, \wedge)$ un retículo acotado. Para todo $a \in L$ se dice que $a' \in L$ es complementario de a si $a \vee a' = \mathbf{1}$ y $a \wedge a' = \mathbf{0}$ (o lo que es equivalente , $sup\,\{a, a'\} = \mathbf{1}$ y $inf\,\{a, a'\} = \mathbf{0}$.

Un retículo acotado es complementario si todos sus elementos poseen complementario.

→ Ejemplos:

Los retículos $(\wp(S), \subseteq)$ y $B^n = \{0,1\}^n$ son complementarios y distributivos.
$(D_{20}, /)$ es acotado y distributivo, pero no es complementario
$(D_{30}, /)$ es acotado, distributivo y complementario.
Los retículos no distributivos del dibujo anterior son complementarios, pero, por ejemplo, el complementario del elemento c no es único.

→ Teorema:
En un retículo acotado y distributivo, el complementario, si existe, es único.

1.8. Álgebras de Boole

→ Definición: Un álgebra de Boole es un retículo acotado, complementario y distributivo.

→ Definición alternativa: Un álgebra de Boole es un conjunto A donde se han definido dos operaciones binarias:
Suma $\vee: A \times A \rightarrow A$ Producto: $\wedge: A \times A \rightarrow A$,

verificando las propiedades

Idempotente: $x \vee x = x$, $x \wedge x = x$

Conmutativa: $x \vee y = y \vee x$, $x \wedge y = y \wedge x$

Asociativa: $x \vee (y \vee z) = (x \vee y) \vee z$, $x \wedge (y \wedge z) = (x \wedge y) \wedge z$

Absorción: $x \vee (x \wedge y) = x$, $x \wedge (x \vee y) = x$

Existe elemento neutro: para la suma, elemento **0**, tal que $x \vee \mathbf{0} = x$

para el producto, elemento $\mathbf{1}$, tal que $x \wedge \mathbf{1} = x$

Para todo $x \in A$, existe un único $x' \in A$, llamado complementario de x, verificando $x \vee x' = \mathbf{1}$ y $x \wedge x' = \mathbf{0}$

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

→ Ejemplos:

- $(\wp(S), \cup, \cap)$ es un álgebra de Boole. Su correspondiente conjunto ordenado es $(\wp(S), \subseteq)$.

- El conjunto de Boole $(\{0,1\}, \vee, \wedge)$, con las operaciones definidas por la tabla siguiente es un álgebra de Boole.

x	y	$x \vee y$	$x \wedge y$
0	0	0	0
0	1	1	0
1	0	1	0
1	1	1	1

Su correspondiente conjunto ordenado: $(B, \leq)$, con $0 \leq 1$, $0' = 1$ y $1' = 0$

- $B^n = \{0,1\}^n = \{(x_1, x_2, \dots x_n) ; x_i \in B\}$ es una álgebra de Boole con las siguientes operaciones

$$(x_1, x_2, \dots x_n) \vee (y_1, y_2, \dots y_n) = (x_1 \vee y_1, \dots, x_n \vee y_n)$$
$$(x_1, x_2, \dots x_n) \wedge (y_1, y_2, \dots y_n) = (x_1 \wedge y_1, \dots, x_n \wedge y_n)$$

Como retículo: elemento mínimo $(0, 0, \dots 0)$, elemento máximo $(1, 1, \dots, 1)$

$$(x_1, x_2, \dots x_n)' = (x_1', x_2', \dots x_n')$$

Su correspondiente conjunto ordenado:$(B^n, \leq_{Prod})$

- $(D_n, /)$ es un álgebra de Boole si y sólo si $n = p_1 \cdot p_2 \cdot \dots \cdot p_k$, con p_i números primos distintos dos a dos y distintos de 1. Su correspondiente conjunto con dos operaciones $(D_n, \vee, \wedge)$

→ Teorema: Si $(A, \vee, \wedge)$ es un álgebra de Boole, entonces se verifican las siguientes propiedades:

- Absorción del neutro: $1 \vee x = 1$, $0 \wedge x = 0$
- Involutiva: $(x')' = x$ (el complementario de cada elemento es único)
- Leyes de De Morgan: $(x \vee y)' = x' \wedge y'$ $(x \wedge y)' = x' \vee y'$

1.9. Isomorfismos de álgebras de Boole

→ Definición : Dos álgebras de Boole son isomorfas si son isomorfas como conjuntos ordenados.

→ Teorema: Si $(A, \vee, \wedge)$ es un álgebra de Boole finita, entonces existe $n \in \mathbb{N}$ tal que $card(A) = 2^n$.

→ Teorema: Si $(A, \vee, \wedge)$ es un álgebra de Boole finita, con $card(A) = 2^n$ entonces $(A, \vee, \wedge)$ es isomorfo a $(\wp(S), \cup, \cap)$, para cualquier conjunto S tal que $card(S) = n$, y es isomorfa también a $(B^n, \vee, \wedge)$

→ Ejemplo: Dibujar los diagramas de Hasse de $(\wp(\{a, b, c\}), \cup, \cap)$, $(B^3, \vee, \wedge)$ y (D_{42}, mcm, mcd)

1.10. Variables booleanas. Funciones booleanas

→ Definición: Una variable booleana es una variable que toma dos valores. Ejemplos: $\{1,0\}$, $\{verdadero, falso\}$, $\{SI, NO\}$, $\{Blanco, Negro\}$, $\{+,-\}$…

→ Definición: Una función booleana de n variables es una aplicación $f: B^n \longrightarrow B$.
Cualquier sucesión de 2^n ceros y unos es el conjunto de valores de una función booleana.
Se pueden definir $2^{(2^n)}$ funciones booleanas de n variables distintas.

→ Definición: Si $f: B^n \longrightarrow B$, llamamos conjunto de verdad o conjunto de unos de la función f, al conjunto $S(f) = \{(x_1, \dots, x_n) \in B^n ;\ f(x_1, \dots, x_n) = 1\}$.

→ Tablas de verdad: representación de una función booleana

x_1	x_2	…	x_n	$f(x_1, \dots, x_n)$
0	0	…	0	$f(0, 0, \dots, 0)$
0	0	…	1	$f(0, 0, \dots, 1)$
…	…	…	…	…
0	1	…	0	$f(0, 1, \dots, x_n)$
1	0	…	0	$f(1, 0, \dots, x_n)$
…	…	…	…	…
1	1	…	1	$f(1, 1, \dots, 1)$

Una función booleana queda totalmente determinada por su tabla de verdad, y por su conjunto de verdad.

→ Teorema: Si $f_1: B^n \to B$ y $f_2: B^n \to B$ son funciones booleanas, entonces también son funciones booleanas:

- La suma: $f = f_1 \vee f_2$: $B^n \to B$, tal que $f(x) = (f_1 \vee f_2)(x) = f_1(x) \vee f_2(x)$

- El producto : $f = f_1 \wedge f_2$: $B^n \to B$, tal que $f(x) = (f_1 \wedge f_2)(x) = f_1(x) \wedge f_2(x)$

Además, los conjuntos de verdad son:

$S(f_1 \vee f_2) = S(f_1) \cup S(f_2)$ $\qquad$ $S(f_1 \wedge f_2) = S(f_1) \cap S(f_2)$

1.11. Expresiones booleanas

→ Definición: Se define una expresión de Boole, o expresión booleana en las n variables $\{x_1, \dots, x_n\}$ de forma recursiva:

1. $x_1, \dots, x_n$ son expresiones de Boole.
2. Los símbolos $1, 0$ son expresiones de Boole.
3. Si $\mathrm{E}_1(\mathrm{x}_1, \dots, \mathrm{x}_\mathrm{n})$, $\mathrm{E}_2(\mathrm{x}_1, \dots, \mathrm{x}_\mathrm{n})$ son expresiones de Boole, entonces $\mathrm{E}_1(\mathrm{x}_1, \dots, \mathrm{x}_\mathrm{n}) \vee \mathrm{E}_2(\mathrm{x}_1, \dots, \mathrm{x}_\mathrm{n})$, $\mathrm{E}_1(\mathrm{x}_1, \dots, \mathrm{x}_\mathrm{n}) \wedge \mathrm{E}_2(\mathrm{x}_1, \dots, \mathrm{x}_\mathrm{n})$, $\left(\mathrm{E}_1(\mathrm{x}_1, \dots, \mathrm{x}_\mathrm{n})\right)'$ son expresiones de Boole.
4. No existen expresiones de Boole que no puedan obtenerse por las reglas anteriores.

→ Propiedad: Si $\mathrm{E}(\mathrm{x}_1, \dots, \mathrm{x}_\mathrm{n})$ es una expresión de Boole en n variables, entonces define una función booleana $f(\mathrm{x}_1, \dots, \mathrm{x}_\mathrm{m}) = \mathrm{E}(\mathrm{x}_1, \dots, \mathrm{x}_\mathrm{n})$ en m variables, con $m \geq n$. Se dice que $\mathrm{E}(\mathrm{x}_1, \dots, \mathrm{x}_\mathrm{n})$ es una expresión que representa a $f(\mathrm{x}_1, \dots, \mathrm{x}_\mathrm{m})$.

→ Propiedad: Si $f: B^n \to B$ es una función booleana, entonces existe una expresión booleana $\mathrm{E}(\mathrm{x}_1, \dots, \mathrm{x}_\mathrm{n})$ que representa a f .

Para toda $x = (x_1, \dots, x_n) \in S(f) = \{\mathrm{x} \in B^n ;\ \ f(x) = 1\}$, se define el producto elemental asociado a x , como

$E_x = E_{(x_1,\dots,x_n)} = E_{x_1} \wedge E_{x_2} \dots \wedge E_{x_n}$,

$$\text{con} \quad E_{x_i} = \begin{cases} x_i\,, & si\ \ x_i = 1 \\ x_i{}'\,, & si\ \ x_i = 0 \end{cases} \quad \text{para todo } i \in \{x_1, \dots, x_n\}$$

Entonces, una expresión de Boole que representa a f en forma de "suma de productos elementales" es

$$E(f) = \bigvee_{x \in S(f)} E_x$$

1.12. Simplificación de expresiones booleanas

→ Una función booleana puede tener varias expresiones que la representen y lo ideal es encontrar la más simple de todas ellas.

→La expresión como suma de productos elementales no es la más simple, en general, pero sí es el punto de partida de todos los métodos de simplificación. Estos métodos se basan en la búsqueda de pares de productos elementales que difieran solamente en una variable.

→ Definición: Las expresiones de Boole $\mathrm{E}_1\,(\mathrm{x}_1, \dots, \mathrm{x}_\mathrm{n})$ y $\mathrm{E}_2\,(\mathrm{x}_1, \dots, \mathrm{x}_\mathrm{n})$ son equivalentes si representan la misma función de Boole.

→ Teorema: Si $\mathrm{E}\,(\mathrm{x}_1, \dots, \mathrm{x}_\mathrm{n})$ es una expresión de Boole en n variables y z es una variable, entonces las expresiones $\mathrm{E}\,(\mathrm{x}_1, \dots, \mathrm{x}_\mathrm{n})$ y

$$E^*\,(\mathrm{x}_1, \dots, \mathrm{x}_\mathrm{n}, z) = \big(z \wedge \mathrm{E}\,(\mathrm{x}_1, \dots, \mathrm{x}_\mathrm{n})\big) \vee \big(z' \wedge \mathrm{E}\,(\mathrm{x}_1, \dots, \mathrm{x}_\mathrm{n})\big)$$

son expresiones equivalentes como expresiones de $n + 1$ variables.

1.13. Mapas de Karnaugh

Dada una expresión de Boole de n variables, su mapa de Karnaugh es una cuadrícula formada por 2^n cuadrados, de tal forma que cada cuadrado representa a un elemento $x \in B^n$.

	y	y'
x	11	10
x'	01	00

	y	y	y'	y'
x	110	111	101	100
x'	010	011	001	000
	z'	z	z	z'

	y	y	y'	y'	
x	1100	1110	1010	1000	t'
x	1101	1111	1011	1001	t
x'	0101	0111	0011	0001	t
x'	0100	0110	0010	0000	t'
	z'	z	z	z'	

En los cuadrados correspondientes a los elementos $x \in B^n$ tales que $f(x) = 1$ se escribe un 1, y en el resto un 0.

Para simplificar una expresión booleana E se procede de la siguiente forma:

1. Se consideran todos los rectángulos simples, del mayor tamaño posible, que recubran la zona de unos del mapa de Karnaugh, aunque se solapen.

2. Se eliminan los rectángulos simples que estén contenidos en la unión de otros, de forma que la zona de unos quede recubierta por el menor número de rectángulos del mayor tamaño posible.
3. La suma de las expresiones correspondientes a los rectángulos que quedan al final del proceso es una expresión simplificada de la expresión original.
4. La expresión simplificada depende de las elecciones efectuadas en el proceso, por lo que no es necesariamente única.

1.14. Método de Quine-McCluskey

El Método de Quine-McCluskey consiste en agrupar sistemáticamente productos que difieren en una única variable, pero en vez de utilizar productos elementales, se utilizan los elementos de $S(f)$. El proceso es el siguiente:

1. Se forma una lista con los unos de la función $S(f)$, por bloques, ordenados de mayor a menor según el número de unos que contienen.
2. Se compara cada elemento de cada bloque con todos los del bloque inmediatamente inferior. Si dos elementos se diferencian en un único dígito, se les asigna el mismo índice. Se forma otra lista reduciendo las filas con el mismo índice, sustituyendo la variable que toma distinto valor por un guion.
3. Se repite el paso 2 con la nueva lista y se continúa este proceso. Finaliza el proceso cuando las filas que quedan no son comparables, porque se diferencian en más de un dígito.
4. Se consideran las filas no comparables entre sí de todas las listas, es decir, las que no tienen índice. Se recogen los resultados en otra tabla cuyas columnas son los $x \in B$ con $f(x) = 1$ y cuyas filas son las expresiones no comparables.
5. Se marcan las coincidencias entre filas y columnas, y se elige un único elemento de cada columna con el siguiente criterio:
   Primero se eligen aquéllos para los que existe una única posibilidad.
   Para los restantes se elige la menor cantidad posible de entre aquéllos con mayor cantidad de guiones.
   Una fila es redundante si sus elementos están incluidos en las restantes filas.
6. La expresión de Boole en forma de "suma de productos mínima" es la correspondiente a la suma de los productos elementales asociados a las filas no redundantes, que dependerá de las elecciones hechas en el proceso.