Matemática Discreta

Licenciatura en Sistemas de Información

Docentes
Vaira, Stella - Fedonczuk, Miguel
Colliard, David - Cottonaro, Mariana - Froloff, Bárbara

FCyT - UADER

2025

Unidad 3: Álgebras booleanas.

Introducción. Definición: operaciones, propiedades. Ejemplos. Aplicaciones: redes lógicas.

- Nació en Lincoln (Inglaterra) en 1815
- A pesar de provenir de una familia humilde, Boole fue prácticamente autodidacta en matemáticas y lenguas. Aprendió latín, griego, francés y alemán por su cuenta.
- Comenzó a trabajar como maestro a los 16 años. En 1834, abrió su propia escuela en Lincoln.
- 1847: Publica “The Mathematical Analysis of Logic”, introduciendo las ideas básicas del álgebra booleana.
- 1849: Fue nombrado primer profesor de matemáticas en el Queen’s College Cork (ahora University College Cork), en Irlanda.
- 1854: Publica “An Investigation of the Laws of Thought”, su obra más influyente, donde desarrolla completamente el sistema lógico que lleva su nombre.

Su legado

El álgebra booleana es la base del diseño de circuitos digitales y sistemas de lógica computacional. Su trabajo es un pilar fundamental de la informática moderna y la lógica matemática.

FCyT Facultad de Ciencia y Tecnología

Claude Shannon fue un matemático, ingeniero eléctrico y criptógrafo estadounidense que se considera el “padre de la teoría de la información”.

- En 1937, tesis de maestría en el MIT: “A Symbolic Analysis of Relay and Switching Circuits”. Conecta los principios de álgebra booleana con la teoría de circuitos eléctricos. Base de la lógica digital moderna.
- Durante la Segunda Guerra Mundial, hizo avances claves en Criptografía. En 1948, publica “A Mathematical Theory of Communication”. Con ello, sentó las bases para la seguridad moderna de las comunicaciones. Fue el primero en formalizar y analizar la seguridad de los sistemas de cifrado y propuso el uso de un “cifrado de clave secreta”.
- En los años 50, Shannon desarrolló un concepto clave para la inteligencia artificial: el “juego de ajedrez”. Creó uno de los primeros programas de ajedrez en una computadora, estudió los autómatas y los sistemas que podían imitar el razonamiento humano, sentando las bases para los futuros desarrollos de la inteligencia artificial.

FCyT Facultad de Ciencia y Tecnología

Conjunto de partes

Dado el conjunto S, podemos enumerar todos los subconjuntos posibles de S, o dicho de otro modo todos los conjuntos incluidos en S. Construimos entonces un nuevo conjunto con todos esos conjuntos como elementos, este nuevo conjunto se llama *conjunto de partes de* S y se indica con $P(S)$.

Para $S = \{a\}$

$$P(S) = \{\emptyset, S\}$$

Para $S = \{a, b\}$

$$P(S) = \{\emptyset, \{a\}, \{b\}, S\}$$

Para $S = \{a, b, c\}$

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

Notemos que todos los elementos de $P(S)$ se escriben entre llaves porque son conjuntos, salvo el conjunto vacío que se escribe sin llaves. Por ejemplo para $S = \{a, b, c\}$: $\{a, b\} \in P(S)$.

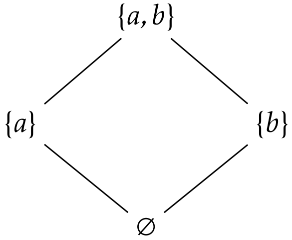
En general, si S tiene n elementos, ¿De cuántos elementos consta $P(S)$?

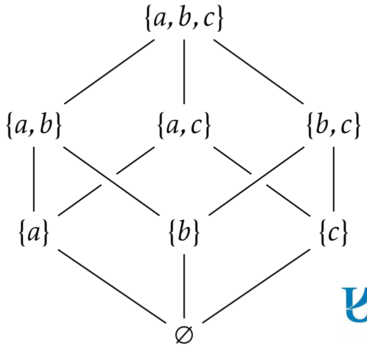
Álgebra de Boole de conjuntos

Sea S un conjunto, entonces $(P(S), \cup, \cap, ^c, \varnothing, S)$ es un *Álgebra de Boole*.

Posee un primer elemento $\varnothing$ y un último elemento S. Existe una relación de orden que se establece entre sus elementos, que en este caso es la *inclusión*. La misma constituye una *relación de orden parcial*. ¿Por qué?

Esta relación entre sus elementos puede representarse mediante un *Diagrama de Hasse*:





Actividad 1

a. Listar los elementos de $P(S)$ para $S = \{a, b, c, d\}$.
b. Establecer una relación de sus elementos con el sistema binario.
c. Analizar cómo es su diagrama de Hasse.

Relación de divisibilidad entre dos números naturales
Si x y y son números naturales, diremos que "x divide a y", y se denota $x|y$, si y sólo si existe un número natural k tal que $y = kx$.

Diremos "x es un divisor(factor) de y", "y es un múltiplo de x" o "y es divisible por x"

Por ejemplo:
$5|15$ porque $15 = 5 \cdot 3$, y por lo cual $3|15$
$1|14$ porque $14 = 1 \cdot 14$, y también $14|14$

Con $D(n)$, denotamos al conjunto de divisores de $n \in \mathbb{N}$.
Ejemplo: $D(10) = \{1, 2, 5, 10\}$

Número natural libre de cuadrados
Un número natural se dice *libre de cuadrados*, si ningún cuadrado mayor a 1 lo divide.
Por ejemplo: 30 es libre de cuadrados, pero 75 no lo es.

FCyT Facultad de Ciencia y Tecnología

Álgebra de Boole de los divisores de n

Sea n un número natural libre de cuadrados, entonces $(D(n), \vee, \wedge, \backsim, 1, n)$ es un *Álgebra de Boole*.

Posee un primer elemento 1 y un último elemento n. La relación de orden que se establece entre sus elementos es la *divisibilidad*. La misma constituye una *relación de orden parcial*. ¿Por qué?

En toda Álgebra de Boole intervienen dos operaciones binarias y una unaria (pensar en el ejemplo anterior cuáles son). En este caso, para dos elementos x e y:

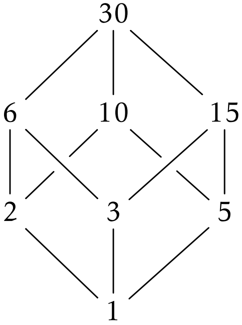
- $x \vee y = mcm(x, y)$
- $x \wedge y = mcd(x, y)$
- $\backsim x = cociente(n, x)$
  (se lee "vilella x")

Ejemplo 1

Sea $n = 30$, $D(30) = \{1, 2, 3, 5, 6, 10, 15, 30\}$

Para $x = 6$ e $y = 10$:

- $x \vee y = mcm(6, 10) = 30$
- $x \wedge y = mcd(6, 10) = 2$
- $\backsim x = cociente(30, 6) = 5$



Todo Álgebra de Boole verifica las siguientes propiedades.
Sean A, B y C elementos de $P(S)$, podemos expresar dichas propiedades en términos de los dos ejemplos anteriores:

1. Ley del doble complemento

$(A^c)^c = A$	$\backsim(\backsim x) = x$

2. Leyes de De Morgan

$(A \cup B)^c = B^c \cap A^c$	$\backsim(x \vee y) = \backsim x \wedge \backsim y$
$(A \cap B)^c = B^c \cup A^c$	$\backsim(x \wedge y) = \backsim x \vee \backsim y$

3. Leyes conmutativas

$A \cup B = B \cup A$	$x \vee y = y \vee x$
$A \cap B = B \cap A$	$x \wedge y = y \wedge x$

4. Leyes asociativas

$A \cup (B \cup C) = (A \cup B) \cup C$	$x \vee (y \vee z) = (x \vee y) \vee z$
$A \cap (B \cap C) = (A \cap B) \cup C$	$x \wedge (y \wedge z) = (x \wedge y) \wedge z$

5. Leyes distributivas

$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$

6. Leyes de idempotencia

$A \cup A = A$ $\qquad$ $x \vee x = x$

$A \cap A = A$ $\qquad$ $x \wedge x = x$

7. Leyes de identidad

$A \cup \emptyset = A$ $\qquad$ $x \vee 1 = x$

$A \cap S = A$ $\qquad$ $x \wedge n = x$

8. Leyes de los inversos

$A \cup A^c = S$ $\qquad$ $x \vee \backsim x = n$

$A \cap A^c = \emptyset$ $\qquad$ $x \wedge \backsim x = 1$

9. Leyes de dominación

$A \cup S = S$ $\qquad$ $x \vee n = n$

$A \cap \emptyset = \emptyset$ $\qquad$ $x \wedge 1 = 1$

10. Leyes de absorción

$A \cup (A \cap B) = A$ $\qquad$ $x \vee (x \wedge y) = x$

$A \cap (A \cup B) = A$ $\qquad$ $x \wedge (x \vee y) = x$

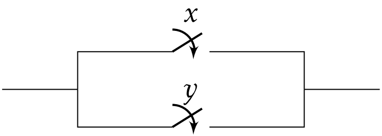
FCyT Facultad de Ciencia y Tecnología

Álgebra de los interruptores

Supongamos que los valores de entrada 1, 0 corresponden respectivamente a las posiciones ON y OFF de los interruptores de un circuito mientras que los valores 1, 0 del interior representan la salida o no de corriente.

Entonces + representa un circuito con dos interruptores en paralelo y $\cdot$ representa un circuito con dos interruptores en serie, x e y variables o estados que pueden tomar valores 1 (ON, pasa corriente) ó 0 (OFF, no pasa corriente):

Circuito en serie $x \cdot y = xy$



Circuito en paralelo $x + y$

Funciones de conmutación

Un interruptor eléctrico puede encenderse (pasa la corriente) o apagarse (no pasa la corriente). De esta manera, como todo dispositivo de dos estados, se relaciona con la lógica de dos valores de verdad.

En programación, los valores booleanos 1 y 0 son aquellos que representan un estado true (verdadero) o false (falso), respectivamente.

Sea $B = \{0, 1\}$, el conjunto de valores booleanos, definimos en dicho conjunto la suma, multiplicación y complemento:

1. $0 + 0 = 0$; $0 + 1 = 1$; $1 + 0 = 1$; $1 + 1 = 1$
2. $0 \cdot 0 = 0$; $0 \cdot 1 = 0$; $1 \cdot 0 = 0$; $1 \cdot 1 = 1$
3. $\bar{0} = 1$; $\bar{1} = 0$

Una variable x es una *variable booleana* si x toma valores de B.

Observaciones:

1. $x + x = x$; $x \cdot x = x$ (Propiedades de idempotencia)
2. $x + y = 0 \Leftrightarrow x = y = 0$
3. $x \cdot y = 1 \Leftrightarrow x = y = 1$

FCyT Facultad de Ciencia y Tecnología

Funciones booleanas

Sea $n \in \mathbb{Z}^+$, $B^n = \{(b_1, b_2, \ldots, b_n)/b_i \in \{0,1\}, \forall i\}$. Es decir, B^n está formado por las n-uplas de componentes 0 o 1.
Una función $f : B^n \to B$ es una función *función booleana*, también llamada *función de conmutación*.

En general, ¿cuántas filas posee una tabla de $f : B^n \to B$?

Ejemplo 2

$f : B^3 \to B$ definida por $f(x,y,z) = xy + z$

x	y	z	$f(x,y,z) = xy + z$
0	0	0	$0 \cdot 0 + 0 = 0$
0	0	1	$0 \cdot 0 + 1 = 1$
0	1	0	$0 \cdot 1 + 0 = 0$
0	1	1	$0 \cdot 1 + 1 = 1$
1	0	0	$1 \cdot 0 + 0 = 0$
1	0	1	$1 \cdot 0 + 1 = 1$
1	1	0	$1 \cdot 1 + 0 = 1$
1	1	1	$1 \cdot 1 + 1 = 1$

FCyT Facultad de Ciencia y Tecnología

Actividad 2

Completar la tabla con el recorrido de las siguientes funciones:

x	y	z	$h(x,y,z) = x + z$	$m(x,y,z) = xy\bar{z}$
0	0	0		
0	0	1		
0	1	0		
0	1	1		
1	0	0		
1	0	1		
1	1	0		
1	1	1		

Actividad 3

Construir la tabla para la función booleana $j(x,y) = xy + \bar{x}$.

Actividad 4

Analizar cómo está conformada cada tabla de las funciones $f_1(x,y,z) = \mathbf{1}$ y $f_0(x,y,z,w) = \mathbf{0}$.

FCyT
Facultad de Ciencia y Tecnología

Igualdad entre funciones booleanas

Para $n \in \mathbb{Z}^+$, $n \geq 2$, sean $f, g : B^n \to B$ dos funciones booleanas de n variables booleanas $x_1, x_2, \ldots, x_n$. Decimos que f y g son iguales (escribimos $f = g$) si las columnas para f y g (en sus respectivas tablas de función) para las mismas entradas $(x_1, x_2, \ldots, x_n)$ son exactamente las mismas.

Actividad 5

Probar que $f(x,y,z) = xy + z$ y $g(x,y,z) = \overline{(\bar{x} + \bar{y})\bar{z}}$ son iguales.

x	y	z	$f(x,y,z)$	$g(x, y, z)$
0	0	0	0	
0	0	1	1	
0	1	0	0	
0	1	1	1	
1	0	0	0	
1	0	1	1	
1	1	0	1	
1	1	1	1	

Funciones booleanas complementarias

Para $n \in \mathbb{Z}^+$, $n \geq 2$, sean $f : B^n \to B$ un función booleana, entonces el complemento de f, que se denota $\bar{f}$, es la función booleana definida sobre B^n como:

$$\bar{f}(x_1, x_2, \ldots, x_n) = \overline{f(x_1, x_2, \ldots, x_n)}$$

Ejemplo 3

x	y	z	$f(x,y,z) = xy + z$	$\bar{f}(x,y,z) = \overline{xy + z}$
0	0	0	0	
0	0	1	1	
0	1	0	0	
0	1	1	1	
1	0	0	0	
1	0	1	1	
1	1	0	1	
1	1	1	1	

FCyT Facultad de Ciencia y Tecnología

Adición y multiplicación de funciones booleanas

Para $n \in \mathbb{Z}^+$, $n \geq 2$, sean $f, g : B^n \to B$ dos funciones booleanas de n variables booleanas $x_1, x_2, \ldots, x_n$. Definimos la adición y multiplicación entre funciones booleanas como:

- $(f + g)(x_1, x_2, \ldots, x_n) = f(x_1, x_2, \ldots, x_n) + g(x_1, x_2, \ldots, x_n)$
- $(f \cdot g)(x_1, x_2, \ldots, x_n) = f(x_1, x_2, \ldots, x_n) \cdot g(x_1, x_2, \ldots, x_n)$

De esta manera hemos definido tres operaciones:
complemento (unaria), adición y multiplicación (binarias).

En la siguiente tabla se establecen las Leyes que verifican las funciones booleanas, como consecuencia de sus operaciones definidas.

Observar que en cada ley numerada, aparece una propiedad (s) y su dual (s^d), que surge de intercambiar las operaciones.

FCyT Facultad de Ciencia y Tecnología

1)	$\overline{\overline{f}} = f$	$\overline{\overline{x}} = x$	Ley del *doble complemento*
2)	$\overline{f+g} = \overline{f}\,\overline{g}$ $\overline{fg} = \overline{f} + \overline{g}$	$\overline{x+y} = \overline{x}\,\overline{y}$ $\overline{xy} = \overline{x} + \overline{y}$	Leyes de *DeMorgan*
3)	$f + g = g + f$ $fg = gf$	$x + y = y + x$ $xy = yx$	Leyes *conmutativas*
4)	$f + (g + h) = (f + g) + h$ $f(gh) = (fg)h$	$x + (y + z) = (x + y) + z$ $x(yz) = (xy)z$	Leyes *asociativas*
5)	$f + gh = (f + g)(f + h)$ $f(g + h) = fg + fh$	$x + yz = (x + y)(x + z)$ $x(y + z) = xy + xz$	Leyes *distributivas*
6)	$f + f = f$ $ff = f$	$x + x = x$ $xx = x$	Leyes de *idempotencia*
7)	$f + \mathbf{0} = f$ $f \cdot \mathbf{1} = f$	$x + 0 = x$ $x \cdot 1 = x$	Leyes de *identidad*
8)	$f + \overline{f} = \mathbf{1}$ $f\overline{f} = \mathbf{0}$	$x + \overline{x} = 1$ $x\overline{x} = 0$	Leyes de los *inversos*
9)	$f + \mathbf{1} = \mathbf{1}$ $f \cdot \mathbf{0} = \mathbf{0}$	$x + 1 = 1$ $x \cdot 0 = 0$	Leyes de *dominación*
10)	$f + fg = f$ $f(f + g) = f$	$x + xy = x$ $x(x + y) = x$	Leyes de *absorción*

Las leyes de las funciones booleanas nos permiten simplificar (o expandir) expresiones booleanas. Como por ejemplo:

$$xy + (x+y)\bar{z} + y \overset{L5}{=} xy + x\bar{z} + y\bar{z} + y \overset{L10}{=} y + x\bar{z}$$

$L5$: Leyes distributivas
$L10$: Leyes de absorción

También nos permiten representar una adición como una multiplicación, y viceversa. Como por ejemplo:

$$y + x\bar{z} \overset{L5}{=} (y+x)(y+\bar{z})$$

Forma Normal Disyuntiva (fnd)

Para $n \in \mathbb{Z}^+$, si $f : B^n \to B$ es una función booleana sobre las n variables booleanas $x_1, x_2, \ldots, x_n$, entonces:

1. Cada x_i, o su complemento $\bar{x}_i$, es un literal.
2. Una expresión de la forma $y_1 y_2 \cdots y_n$ donde $y_i = x_i$ o $y_i = \bar{x}_i$, es una conjunción fundamental.
3. Una representación de f como una adición de conjunciones fundamentales es una forma normal disyuntiva (fnd) de la función booleana.

Observación: La fnd de toda función booleana, en su expresión más simple, es única.

Ejemplo 4

- $f(x, y, z) = xyz + yz + z$ no está expresada en su fnd, no posee conjunciones fundamentales en todos sus términos.
- $g(x, y, z) = xyz + \bar{x}y\bar{z}$ está en su fnd, cada término posee los tres literales.

FCyT
Facultad de Ciencia y Tecnología

Toda función booleana puede expresarse como una ADICIÓN DE CONJUNCIONES FUNDAMENTALES, y la misma, tiene su representación como una ADICIÓN DE MINTÉRMINOS.

Ejemplo 5

$$\begin{aligned} f(x,y,z) &= xy + yz \\ &= xy1 + 1yz \\ &= xy(z+\bar{z}) + (x+\bar{x})yz \\ &= xyz + xy\bar{z} + xyz + \bar{x}yz \\ f(x,y,z) &= xyz + xy\bar{z} + \bar{x}yz \quad (fnd) \end{aligned}$$

et	x	y	z	f	$conj.f.$	et
0	0	0	0	0		
1	0	0	1	0		
2	0	1	0	0		
3	0	1	1	1	$\bar{x}yz$	3
4	1	0	0	0		
5	1	0	1	0		
6	1	1	0	1	$xy\bar{z}$	6
7	1	1	1	1	xyz	7

$$f(x,y,z) = xyz + xy\bar{z} + \bar{x}yz = \sum m(3,6,7)$$

Forma Normal Conjuntiva (fnc)

Para $n \in \mathbb{Z}^+$, si $f : B^n \to B$ es una función booleana sobre las n variables booleanas $x_1, x_2, \ldots, x_n$, entonces:

1. Cada x_i, o su complemento $\bar{x}_i$, es un literal.
2. Una expresión de la forma $(y_1 + y_2 + \cdots + y_n)$ donde $y_i = x_i$ o $y_i = \bar{x}_i$, es una disyunción fundamental.
3. Una representación de f como una multiplicación de disyunciones fundamentales es una forma normal conjuntiva (fnc) de la función booleana.

Observación: La fnc de toda función booleana, en su expresión más simple, es única.

Ejemplo 6

- $f(x, y, z) = (x + y)(x + \bar{y} + z)$ no está expresada en su fnc, no posee disyunciones fundamentales en todos sus factores.
- $g(x, y, z) = (x + y + z)(x + \bar{y} + \bar{z})$ está en su fnc, cada factor posee los tres literales.

FCyT
Facultad de Ciencia y Tecnología

Problema dual: fnd $\longleftrightarrow$ fnc

- conjunciones fundamentales $\longleftrightarrow$ disyunciones fundamentales

$$(xyz) \longleftrightarrow (x + y + z)$$

- buscamos c.f. tales que f=1 $\longleftrightarrow$ buscamos d.f. tales que f=0

- forma normal disyuntiva $\longleftrightarrow$ forma normal conjuntiva

- adición de mintérminos $\longleftrightarrow$ multiplicación de maxtérminos

Expresión de una función booleana como una MULTIPLICACIÓN DE DISYUNCIONES FUNDAMENTALES y una MULTIPLICACIÓN DE MAXTÉRMINOS.

Ejemplo 7

$$
\begin{aligned}
f(x,y,z) &= xy + yz = y(x+z) \\
&= ((y+0)+0)(x+z+0) \\
&= ((y + x\cdot\bar{x}) + z\cdot\bar{z})((x+z)+y\cdot\bar{y}) \\
&= (y + x\cdot\bar{x} + z)(y + x\bar{x} + \bar{z})(x+z+y)(x+z+\bar{y}) \\
&= (y+x+z)(y+\bar{x}+z)(y+x+\bar{z})(y+\bar{x}+\bar{z})(x+z+y)(x+z+\bar{y}) \\
&= (x+y+z)(\bar{x}+y+z)(x+y+\bar{z})(\bar{x}+y+\bar{z})(x+\bar{y}+z)
\end{aligned}
$$

$$f(x,y,z) = (x+y+z)(\bar{x}+y+z)(x+y+\bar{z})(\bar{x}+y+\bar{z})(x+\bar{y}+z)$$

FCyT
Facultad de Ciencia y Tecnología

et	x	y	z	f	$disy.f.$	et
0	0	0	0	0	$x+y+z$	0
1	0	0	1	0	$x+y+\bar{z}$	1
2	0	1	0	0	$x+\bar{y}+z$	2
3	0	1	1	1		
4	1	0	0	0	$\bar{x}+y+z$	4
5	1	0	1	0	$\bar{x}+y+\bar{z}$	5
6	1	1	0	1		
7	1	1	1	1		

$$f(x,y,z) = (x+y+z)(\bar{x}+y+z)(x+y+\bar{z})(\bar{x}+y+\bar{z})(x+\bar{y}+z)$$

$$f(x,y,z) = \prod M(0,1,2,4,5)$$

FCyT Facultad de Ciencia y Tecnología

Actividad 6

Hallar la expresión más simple de cada una de las siguientes funciones:

- $f(x,y,z) = \sum m(1,3,5,7)$
- $g(x,y,z) = \prod M(4,6,7)$

et	x	y	z	f	$conj.f.$	g	$disy.f.$
0	0	0	0				
1	0	0	1				
2	0	1	0				
3	0	1	1				
4	1	0	0				
5	1	0	1				
6	1	1	0				
7	1	1	1				

- $f(x,y,z) =$
- $g(x,y,z) =$

FCyT
Facultad de Ciencia y Tecnología

Actividades propuestas

Para realizar las actividades prácticas correspondientes a este apartado te sugerimos realizar los ejercicios del 1 al 13 de la sección 15.1 (Página 743) del libro *Matemática Discreta de Ralph Grimaldi* que se encuentra en el campus virtual.