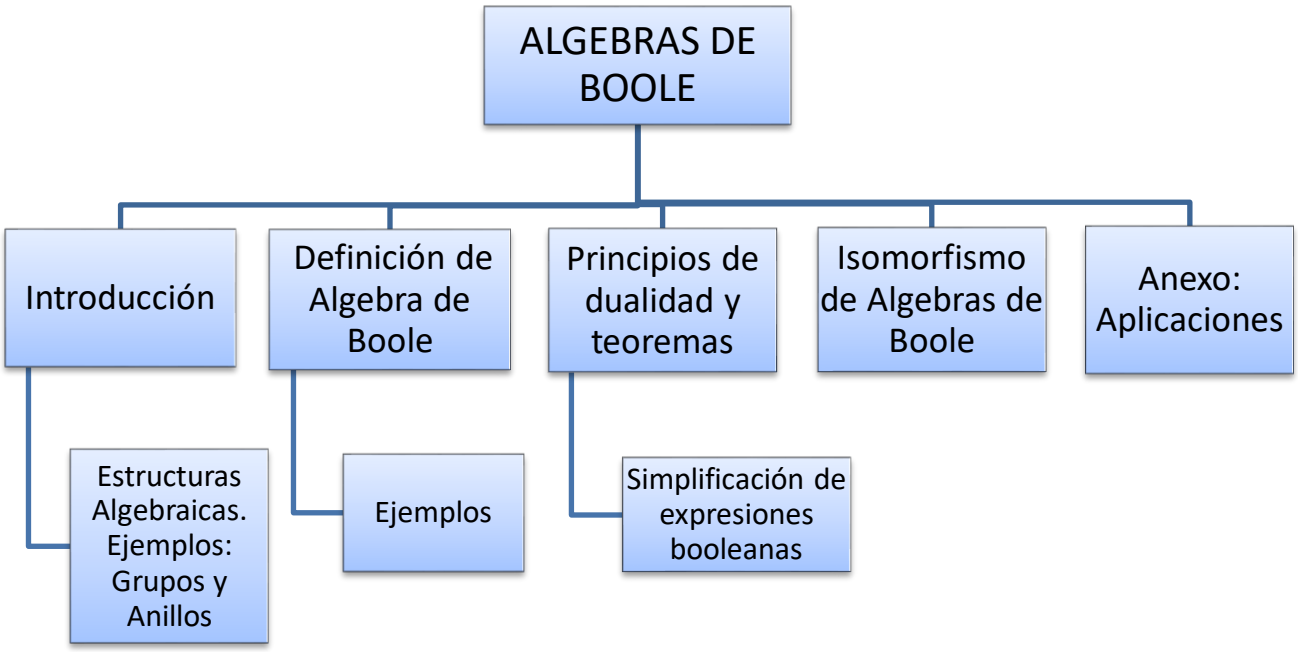
MATEMÁTICA I 2020

Capítulo 3

ALGEBRAS DE BOOLE

CONTENIDOS:



Matemático invitado: George Boole

En el siglo XIX, el matemático George Boole (1815-1864), en sus libros: "*The Mathematical Analysis of Logic*" (1847) y "*An Investigation of The Laws of Thought*" (1854), desarrolló la idea de que las proposiciones lógicas podían ser tratadas mediante herramientas matemáticas siguiendo el comportamiento de reglas algebraicas. Igual que en álgebra tradicional, también se trabaja con letras para denominar variables y formar ecuaciones para obtener el resultado de ciertas operaciones mediante una ecuación o expresión booleana.

Los trabajos de Boole y los de sus discípulos resultaron extraños en su época porque en aquel momento parecían no tener aplicaciones. A mediados del siglo XX el álgebra de Boole resultó de una gran importancia práctica, importancia que se ha ido incrementando

hasta nuestros días, en el manejo de información digital. Gracias a ella, Claude Shannon (1916-2001) pudo formular su teoría de la codificación y John Von Neumann (1903-1957) pudo enunciar el modelo de arquitectura que define la estructura interna de las computadoras desde la primera generación.

Por esto, Boole es hoy considerado uno de los fundadores de las Ciencias de la Computación y de la base teórica para la era digital.

1. Introducción

Definiremos en este capítulo las Algebras de Boole como una Estructura Algebraica.

Una **Estructura Algebraica** es un conjunto no vacío con una o más operaciones definidas en él.
Estas operaciones pueden ser **binarias** o **unarias**. Las operaciones binarias se realizan entre dos elementos del conjunto y las operaciones unarias son las que se aplican a un elemento del conjunto.

Formalmente: Dado un conjunto no vacío A,

- **una *operación binaria* en A es una función del producto cartesiano AxA en A, $f: AxA \rightarrow A$.**
  Decir que una operación es *binaria* en A es equivalente a decir que la operación es *cerrada* en A. Esto quiere decir que al realizar la operación entre dos elementos cualesquiera de A el resultado es también un elemento de A.
- **una *operación unaria* es una función de A en A, $f: A \rightarrow A$**
  Recordemos que, al estar definidas como función, todo par de elementos tiene un único correspondiente en el caso de las operaciones binarias y todo elemento de A tiene un único correspondiente para el caso de las unarias.

Hay distintas Estructuras Algebraicas que ya conocemos, el nombre que recibe cada estructura algebraica depende de las operaciones definidas en el conjunto y de las propiedades que tengan esas operaciones.

Si $\boldsymbol{A}$ es un conjunto con una operación \$, definida en él, que cumple las propiedades:

1) Cerrada o binaria: para cualesquiera a y b elementos de A, se cumple que: $a\$b \in A$

2)Asociativa: para cualesquiera $a,\ b$ y c elementos de A, se cumple que: $(a\$b)\$c = a\$(b\$c)$

3)Existencia de elemento neutro: existe un elemento n en A tal que para cualquier otro elemento a de A se cumple que $a\$n = n\$a = a$

4)Existencia de elemento opuesto: para cualquier elemento a de A existe un elemento a' en A tal que: $a\$a' = a'\$a = n$

Entonces decimos que A con la operación \$ tiene estructura de GRUPO o equivalentemente que el par (A, \$) es un GRUPO.

Si además cumple la propiedad:

5)Conmutativa: para cualesquiera a y b elementos de A, se cumple que: $a\$b = b\$a$

Tiene estructura de **GRUPO CONMUTATIVO O GRUPO ABELIANO.**

NOTA: la operación en este caso es \$, es sólo un símbolo para nombrar una operación cualquiera, así como A es el nombre de un conjunto que puede ser cualquiera.

En adelante analizaremos estas propiedades para conjuntos y operaciones particulares.

Ejemplo 1.1:

El conjunto $\mathbb{Z}$ de los números enteros con la operación suma, que escribimos: $(\mathbb{Z}, +)$ es un **Grupo Conmutativo**.

La operación suma tiene en este conjunto las siguientes propiedades:

►*Cerrada o binaria*: para cualquier par de números enteros su suma da un número entero:

$$Si\ a \in \mathbb{Z}\ y\ b \in \mathbb{Z}\ entonces\ a + b \in \mathbb{Z}$$

►*Asociativa:* para cualquier terna de números enteros el resultado de sumarlos da lo mismo asociando los dos primeros o los dos últimos:

$$Si\ a \in \mathbb{Z}\ y\ b \in \mathbb{Z}\ y\ c \in \mathbb{Z}\ \ entonces\ (a + b) + c = a + (b + c)$$

►*Existencia de elemento neutro*: ya que existe un **único** número tal que sumado a cualquier otro da como resultado el mismo número. El elemento neutro es el 0 pues existe el 0 en $\mathbb{Z}$ tal que: $si\ a \in \mathbb{Z}\ entonces\ \ a + 0 = 0 + a = a$

►*Existencia de elemento opuesto*: ya que para todo número entero existe otro, **único,** que sumado a él da como resultado el elemento neutro:

$$Si\ a \in \mathbb{Z}\ entonces\ \ a + (-a) = (-a) + a = 0$$

Por estas propiedades de la suma en $\mathbb{Z}$, decimos que $(\mathbb{Z}, +)$ tiene estructura de **Grupo**.

Además, la operación suma cumple la propiedad:

►*Conmutativa*: para cualquier par de números enteros el resultado de sumarlos da lo mismo en cualquier orden: $Si\ a \in \mathbb{Z}\ y\ b \in \mathbb{Z}\ \ entonces\ a + b = b + a$

Por eso decimos que $(\mathbb{Z}, +)$ tiene estructura de **Grupo conmutativo o Grupo abeliano**.

Ejemplos 1.2:

a) $(\mathbb{R}, +)$, los números reales con la suma son un **Grupo Conmutativo**.

b) $(\mathbb{Z}, .)$, los números enteros con la multiplicación **NO tienen estructura de Grupo.**
Se cumplen las propiedades: cerrada, asociativa, hay elemento neutro (en este caso es el 1, ya que todo número entero multiplicado por 1 da como resultado el mismo número).
Sin embargo, la existencia de un número que multiplicado por otro de como resultado el neutro, que en el caso de la operación suma llamamos opuesto y en este caso se llama inverso multiplicativo, **no se cumple**. Para todo número entero, debería existir un número que, multiplicado por él, dé 1, pero esto no se cumple.
Si a es un entero , distinto de 1 y -1, $a.\frac{1}{a} = 1$, pero $\frac{1}{a}$, no es un número entero.
Por ejemplo si tomamos $a = 3$, es un entero, pero al buscar un número que multiplicado por él de 1, tenemos que $3.\frac{1}{3} = 1$, pero $\frac{1}{3}$ no es un número entero.

c) $(\mathbb{N}, +)$, los números naturales con la suma **NO tienen estructura de Grupo**, ya que no tienen opuesto, el número $-a$ para cualquier a natural, no es un número natural.
Por ejemplo si tomamos $a = 4$, es un natural, pero al buscar un número que sumado a él de 0 (neutro de la operación suma), tenemos que $4 + (-4) = 0$, pero -4 no es un número natural.

d) Definimos en el conjunto de los números enteros una operación Δ de la siguiente manera:
Para todo par de enteros a y b , $a\Delta b = a + b + 2$, donde + es la suma usual en los enteros.
Entonces $(\mathbb{Z}, \Delta)$ es un **Grupo Conmutativo.**

Demostración: si a, b y c son números enteros:

Δ **es cerrada**: $a\Delta b = a + b + 2$ es un número entero.

Δ **es asociativa**: $(a\Delta b)\Delta c = a\Delta(b\Delta c)$ porque $(a + b + 2) + c + 2 = a + (b + c + 2) + 2$

Δ **tiene neutro**: Buscamos un elemento $n \in \mathbb{Z}$ que cumpla que: $a\Delta n = n\Delta a = a$.

Como $a\Delta n = a + n + 2 = a$ entonces $n = a - a - 2$, $n = -2$.

Con ese valor de n, se cumple que:

$a\Delta(-2) = a + (-2) + 2 = a$ y que $(-2)\Delta a = (-2) + a + 2$

Entonces -2 es elemento neutro de $(\mathbb{Z}, \Delta)$

Δ **es conmutativa**: $a\Delta b = b\Delta a$ porque $a + b + 2 = b + a + 2$

Δ **tiene opuesto**: Para cada $a \in \mathbb{Z}$ buscamos un elemento $a' \in \mathbb{Z}$ que cumple que:

$a\Delta a' = a'\Delta a = -2$, lo igualamos a -2 porque es el elemento neutro para esta operación.

El número $-4 - a$ es opuesto de a en $(\mathbb{Z}, *)$, ya que

$a\Delta a' = a + a' + 2 = -2$ entonces $a' = -2 - 2 - a$, entonces $a' = -4 - a$.

Con ese valor de a' se cumple que:

$a\Delta(-4 - a) = a + (-4 - a) + 2 = -2$ y $(-4 - a)\Delta a = (-4 - a) + a + 2 = -2$

El número $-4 - a$ es opuesto de a en $(\mathbb{Z}, \Delta)$

Ejemplo 1.3:

Conjunto de partes.

Dado un conjunto $A = \{a, b, c\}$ podemos enumerar todos los subconjuntos posibles de *A*, o dicho de otro modo todos los conjuntos incluidos en *A.*

Construimos entonces un nuevo conjunto con todos esos conjuntos como elementos, este nuevo conjunto se llama ***conjunto de partes de A*** y se indica:

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

Notemos que todos los elementos de *P*(*A*) son conjuntos, por eso se escriben entre llaves, salvo el conjunto vacío, que no tiene elementos y se escribe sin llaves porque es el nombre del conjunto.

Es por eso que escribimos: $\{a, b\}$ "contenido en" *A* , $(\{a, b\} \subseteq A)$, $\{c\}$ "contenido en" *A*, $(\{c\} \subseteq A)$, son subconjuntos de A.

Y cada **uno de esos conjuntos es elemento de *P(A)***, por eso escribimos**:** $\{a, b\}$ *"pertenece a" P(A),* $(\{a, b\} \in P(A))$ *y también* $\{c\}$ *"pertenece a" P(A),* $(\{c\} \in P(A))$.

Por lo cual $\{\{a,b\},\{c\}\}$ *"está contenido en" P(A),* ya que es un conjunto formado por elementos de *P(A) .*

En general:

Dado un conjunto H, se define ***P*(H), el *conjunto de partes de* H,** que tiene como elementos todos los subconjuntos de H. Los *elementos* de *P*(H) son *conjuntos*, todos los que están contenidos en H, el vacío que está contenido en cualquier conjunto y el conjunto total H ($\emptyset \subseteq \boldsymbol{H}$, $\boldsymbol{H} \subseteq \boldsymbol{H}$)

***P*(H) =**$\{\boldsymbol{X}: \boldsymbol{X} \subseteq \boldsymbol{H}\}$, se lee: " el conjunto de los conjuntos X tales que X está contenido en H"

En palabras: *X* es un elemento de *P*(H) si y sólo si *X* está incluido en H

En símbolos: $X \in P(H) \Leftrightarrow X \subseteq H$

Si H es un conjunto finito (o sea tiene un número finito $\boldsymbol{n}$ de elementos), el número de elementos de *P*(H) es 2^n.

El conjunto vacío tiene 0 elementos, entonces si $H = \emptyset$, *P*(H)={∅}, el conjunto de partes del conjunto vacío tiene como único elemento al vacío, es el único subconjunto incluído en el vacío (porque $\emptyset \subseteq \emptyset$), también vale en este caso que tiene 2^0=1 elementos.

En el conjunto $\boldsymbol{P}(\boldsymbol{H})$, para H no vacío, la operación unión (∪)**cumple las siguientes propiedades para** A, B y C elementos de P(H):

Cerrada: $A \cup B$ es un elemento de P(H) ya que la unión de subconjuntos de un conjunto W es también un subconjunto de W

Asociativa: $A \cup (B \cup C) = (A \cup B) \cup C$, por la propiedad vista en la Capítulo 2.

Neutro: El ∅ es elemento de P(H), y para todo *A* en P(H), $A \cup \emptyset = A$ y $\emptyset \cup A = A$, así ∅ es el elemento neutro de la unión.

Conmutativa: $A \cup B = B \cup A$, por la propiedad vista en el Capítulo 2.

Pero ($\boldsymbol{P}(\boldsymbol{H})$,∪) **No es un grupo** ya que no existe el opuesto para cada subconjunto de H, no hay ningún elemento F en $P(H)$ que unido a otro elemento E no vacío de P(H) de como resultado el conjunto vacío (neutro de la unión).

Un **Anillo** es una terna ordenada $(\boldsymbol{A}, +, .)$ **,** donde **A** es un conjunto y **"+"** y **"."** son dos operaciones que cumplen:

1) $(\boldsymbol{A}, +)$ **es un grupo conmutativo**

2) La operación "." es una operación cerrada y asociativa.

Cerrada: para cualesquiera a y b elementos de A, se cumple que: $a.b \in A$

Asociativa: para cualesquiera $a,\ b$ y c elementos de A, se cumple que: $(a.b).c = a.(b.c)$

3) La operación "." es distributiva con respecto a "+".

Distributiva: para cualesquiera $a,\ b$ y c elementos de A, se cumple que:

$a.(b+c) = a.b + a.c \quad y \quad (b+c).a = b.a + c.a$

Ejemplo 1.4:

Tomemos el conjunto de los números reales con las operaciones suma y multiplicación, que escribimos: $(\mathbb{R}, +, .)$.

Como mencionamos en los ejemplos anteriores $(\mathbb{R}, +)$ tiene estructura de Grupo conmutativo.

La operación multiplicación tiene en este conjunto las siguientes propiedades:

► *Cerrada o binaria:* ya que para cualquier par de números reales su producto da un número real: $Si\ a \in \mathbb{R}\ y\ b \in \mathbb{R}\ entonces\ a.b \in \mathbb{R}$

► *Asociativa:* el producto es una operación asociativa ya que para cualquier terna de números reales el resultado de multiplicarlos da lo mismo asociando los dos primeros o los dos últimos: $Si\ a \in \mathbb{R}\ y\ b \in \mathbb{R}\ y\ c \in \mathbb{R}\ entonces\ (a.b).c = a.(b.c)$

► *Distributiva del producto con respecto a la suma:* ya que para cualquier terna de números reales el resultado de multiplicar uno de ellos por la suma de los otros dos da el mismo resultado que multiplicar cada uno de ellos y después sumarlos:

$Si\ a \in \mathbb{R}\ y\ b \in \mathbb{R}\ y\ c \in \mathbb{R}\ entonces\ a.(b+c) = a.b + a.c$ y $(b+c).a = b.a + c.a$

Decimos entonces que $(\mathbb{R}, +, .)$, por cumplir todas las propiedades antes mencionadas tiene estructura de **Anillo.**

Ejemplos 1.5:

a) $(\mathbb{Z}, +, .)$ es un **Anillo ya que** $(\mathbb{Z}, +)$ es un grupo conmutativo y la multiplicación en $\mathbb{Z}$ es cerrada, asociativa y distributiva con respecto a la suma.

b) $\mathbb{Q}$ es el conjunto de los números racionales o fraccionarios. Recordemos que los números racionales son aquellos que se escriben como cociente de enteros, es decir que $\mathbb{Q} = \{a: a = \frac{x}{y} \wedge\ x \in \mathbb{Z} \wedge y \in \mathbb{Z} \wedge y \neq 0\}$. En la terna $(\mathbb{Q}, +, .)$ las operaciones son la suma y el producto usuales, así $(\mathbb{Q}, +, .)$ es un **Anillo ya que** $(\mathbb{Q}, +)$ es un grupo conmutativo y la multiplicación es cerrada, asociativa y distributiva con respecto a la suma.

Ejemplo 1.6:

Tomemos el conjunto de los números racionales o fraccionarios con las operaciones suma y #, que escribimos: $(\mathbb{Q}, +, \#)$. Se define la operación # como: $a\#b = \frac{a.b}{2}$

Como mencionamos en los ejemplos anteriores $(\mathbb{Q}, +)$ tiene estructura de Grupo conmutativo.

La operación # tiene en este conjunto las siguientes propiedades:

► *Cerrada:* ya que para cualquier par de números racionales su producto dividido 2 da un número racional: $Si\ a \in \mathbb{Q}\ y\ b \in \mathbb{Q}\ entonces\ a\#b = \frac{a.b}{2} \in \mathbb{Q}$

Demostración: $a = \frac{x}{y}$, $b = \frac{z}{w}$, $y \neq 0, w \neq 0$, entonces $\frac{a.b}{2} = \frac{x}{y}.\frac{z}{w}.\frac{1}{2} = \frac{x.z}{y.w.2}$, $x.z$ es entero por ser producto de enteros y por la misma razón $y.w.2$ es entero. Además $y.w.2 \neq 0$. Por lo tanto $\frac{a.b}{2} \in \mathbb{Q}$

► *Asociativa:* # es una operación asociativa ya que:

$$Si\ a, b\ y\ c \in \mathbb{Q}\ \ entonces\ (a\#b)\#c = a\#(b\#c)$$

Demostración: sean $a = \frac{x}{y}$, $b = \frac{z}{w}$, $c = \frac{u}{m}$, $y \neq 0, w \neq 0, m \neq 0$, entonces

$$(a\#b)\#c = \left(\frac{x}{y}.\frac{z}{w}.\frac{1}{2}\right)\#c = \frac{x.z}{y.w.2}.\frac{u}{m}.\frac{1}{2} = \frac{x.z.u}{y.w.m.4}$$

$$a\#(b\#c) = a\#\left(\frac{z}{w}.\frac{u}{m}.\frac{1}{2}\right) = \frac{x}{y}.\frac{z.u}{w.m.2}.\frac{1}{2} = \frac{x.z.u}{y.w.m.4}$$

Entonces $(a\#b)\#c = a\#(b\#c)$

► *Distributiva de # con respecto a la suma:* ya que

$$Si\ a, b\ y\ c \in \mathbb{Q}\ entonces\ a\#(b + c) = a\#b + a\#c$$

Demostración: sean $a = \frac{x}{y}$, $b = \frac{z}{w}$, $c = \frac{u}{m}$, $y \neq 0, w \neq 0, m \neq 0$, entonces

$$a\#(b + c) = a\#\left(\frac{z}{w} + \frac{u}{m}\right) = a\#\left(\frac{zm + uw}{w.m}\right) = \frac{x}{y}.\frac{zm + uw}{w.m}.\frac{1}{2} = \frac{x.z.m + x.u.w}{y.w.m.2}$$

$$a\#b + a\#c = \left(\frac{x}{y}.\frac{z}{w}.\frac{1}{2}\right) + \left(\frac{x}{y}.\frac{u}{m}.\frac{1}{2}\right) = \frac{xz}{y.w.2} + \frac{xu}{y.m.2} = \frac{x.z.m + x.u.w}{y.w.m.2}$$

Entonces $a\#(b+c) = a\#b + a\#c$. Del mismo modo se muestra que $(b+c)\#a = b\#a + c\#a$

Decimos entonces que $(\mathbb{Q}, +, \#)$, por cumplir todas las propiedades antes mencionadas tiene estructura de **Anillo.**

Ejemplo 1.7:

Tomemos el conjunto de los números enteros con la operación $, definida como:

$$a\#b = b - a + 2$$

Vamos a demostrar que la operación es binaria pero no conmutativa ni asociativa en $\mathbb{Z}$.

Cerrada o binaria: para todo par de números enteros $a\#b = b - a + 2$ es un número entero por ser suma y resta de enteros.

No conmutativa: $a\#b = b - a + 2$ y $b\#a = a - b + 2$

Estas expresiones son aparentemente distintas, sin embargo hay casos donde son iguales, si $a = b$, $a - a + 2 = a - a + 2$.

Entonces debemos dar un contraejemplo para mostrar al menos un caso donde no se cumple:

Si $a = 3 \ y \ b = 5$ tenemos que: $3\#5 = 5 - 3 + 2 = 4$, y $5\#3 = 3 - 5 + 2 = 0$

Por lo tanto la propiedad conmutativa no se cumple porque mostramos al menos un par de números enteros para los cuales no es cierta la igualdad.

No asociativa: $a\#(b\#c) = a\#(c - b + 2) = c - b + 2 - a + 2$ y

$(a\#b)\#c = (b - a + 2)\#c = c - (b - a + 2) + 2 = c - b + a$

Estas expresiones son aparentemente distintas, sin embargo hay casos donde son iguales, si $a = 2$, $c - b + 2 - 2 + 2 = c - b + 2$.

Entonces debemos dar un contraejemplo para mostrar al menos un caso donde no se cumple:

Si $a = 3$, $b = 5 \ y \ c = 1$ tenemos que:

$3\#(5\#1) = 1 - 5 + 2 - 3 + 2 = -3$, y $(3\#5)\#1 = 1 - 5 + 2 = -2$

Por lo tanto, la propiedad asociativa no se cumple porque mostramos al menos una terna de números enteros para los cuales no es cierta la igualdad.

OBSERVACIÓN IMPORTANTE: usamos números para mostrar que la propiedad NO SE CUMPLE PARA TODOS LOS NÚMEROS, por eso se llama contraejemplo. Cuando

queremos mostrar que una propiedad sí se cumple, como en los ejemplos anteriores, usamos letras que representan cualquier número o elemento del conjunto.

Estos ejemplos nos muestran que las estructuras algebraicas no son más que una manera de clasificar conjuntos con determinadas operaciones.
Hay muchas más estructuras algebraicas como los Anillos con unidad, los Dominios de Integridad, los Cuerpos, etc. que no son objeto de estudio de este curso. En lo que sigue estudiaremos la estructura algebraica Algebra de Boole.

Ejercicios:
Salvo aclaración en contrario, los símbolos +, - y . se referirán a las operaciones usuales de suma, resta y producto respectivamente, en el conjunto de números que se indique.

1) En $\mathbb{R}$, se define la operación $ como: $a\$b = a - b + a.b$
   Analizar si la operación es cerrada y conmutativa en $\mathbb{R}$.

2) Analizar si $(\mathbb{N}, .)$ es grupo conmutativo.

3) Sea H un conjunto y (P(H), ∩) el conjunto de Partes de H con la operación intersección. Analizar si (P(H), ∩) es un grupo conmutativo.

4) Demostrar que $(\mathbb{R} - \{0\}, .)$ es un grupo conmutativo. Indique por qué $(\mathbb{R}, .)$ no es un grupo.

5) Sea $E = \{x: x \in \mathbb{Z} \wedge x\ es\ par\}$. Demostrar que (E,+,.) es un anillo.

6) Sea ⊗ , la operación definida sobre los números enteros como: $a \otimes b = 2.a.b$. Demostrar que $(\mathbb{Z}, +, \otimes)$ es un anillo

7) En el conjunto P de los números pares se definen dos operaciones, una de ellas es la suma usual y la otra (#) está definida en la forma: si $x, y \in P$, $x\#y = \frac{x.y}{2}$
Demostrar que (P, +, #) tiene estructura de anillo.

2. Álgebras de Boole

Definición:

Un **Algebra de Boole** es una estructura algebraica formada por un conjunto B, con al menos dos elementos distintos (***primer y último elementos***), designados en forma general con los símbolos 0 y 1, dos *operaciones binarias*: ∨ (denominada *supremo*) y ∧ (denominada *ínfimo*), y una **operación unaria**: ´ (denominada *complemento*), con las siguientes propiedades para elementos cualesquiera $x, y, z \ en \ B$:

$(B1)$ $x \vee y = y \vee x$ conmutatividad de ∨

$(B2)$ $x \wedge y = y \wedge x$ conmutatividad de ∧

$(B3)$ $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ distributividad de ∧ con respecto a ∨

$(B4)$ $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$ distributividad de ∨ con respecto a ∧

$(B5)$ $x \vee 0 = x$ 0 elemento neutro de la operación ∨

$(B6)$ $x \wedge 1 = x$ 1 elemento neutro de la operación ∧

$(B7)$ $x \vee x' = 1$

$(B8)$ $x \wedge x' = 0$

Un Algebra de Boole también se indica como $\mathcal{B}$ = (B, ∨,∧, ´, 0, 1) cuando sea necesario referirse a las operaciones y al primer y último elemento.

Otra notación: Se utiliza también el símbolo + para indicar el supremo ∨ y el símbolo . para indicar el ínfimo ∧ **, aunque al igual que en la multiplicación usual en $\mathbb{R}$ suele ponerse un elemento al lado del otro omitiendo el punto.** Con esta notación los axiomas se transforman en:

$(B1)$ $x + y = y + x$ conmutatividad de $+$

$(B2)$ $xy = yx$ conmutatividad de .

$(B3)$ $x(y + z) = (xy) + (xz)$ distributividad de . con respecto a $+$

$(B4)$ $x + (yz) = (x + y)(x + z)$ distributividad de $+$ con respecto a .

$(B5)$ $x + 0 = x$ 0 elemento neutro de la operación $+$

$(B6)$ $x1 = x$ 1 elemento neutro de la operación .

$(B7)$ $x + x' = 1$

$(B8)$ $xx' = 0$

Usaremos en adelante esta última notación cuando nos estemos refiriendo a elementos de un álgebra de Boole cualquiera.

Observaciones:

1) Los axiomas son válidos para cualesquiera elementos del álgebra, esto quiere decir que por ejemplo: $(xy) + (xy)' = 1$ por el Axioma 7. Lo que dice el axioma es que un elemento supremo su complemento da 1, no importa como se llame el elemento.

Del mismo modo $x + y'$ no tiene por qué dar 1 porque y' no es el complemento de x.

También por Axioma 5 $[(xy') + z] + 0 = [(xy') + z]$, porque lo que dice el axioma es que cualquier elemento supremo el 0 da el mismo elemento.

2) El 0 y el 1 son símbolos para indicar primero y último elementos en la definición de un álgebra de Boole general. En cada ejemplo particular primer y último elementos serán los que correspondan de acuerdo con el tipo de elementos de cada caso, como se verá en los ejemplos siguientes.

3) También son válidas la asociatividad de $+$ y de .:

$$x + (y + z) = (x + y) + z$$

$$x(yz) = (xy)z$$

Estas propiedades se presentan como axiomas en algunos textos, pero pueden deducirse de los axiomas dados, demostración que no incluiremos en este curso.

4) El supremo y el ínfimo son operaciones binarias, es decir funciones de B×B en B; el complemento, como operación unaria, es una función de B en B. El hecho de que sean funciones asegura que para todo par *x, y* de elementos de B, *x+y* ∈ B, *xy* ∈B y son *únicos* y que el complemento ***x´*** ∈B y es *único.*

Proposición: Sea $x \in B$, si existe un elemento $a \in B$ que cumple que $xa = 0$ y $x + a = 1$ entonces $a = x'$, es decir que a es el complemento de x.

Esta proposición asegura que el complemento de un elemento es único.

Demostración:

Sea $x \in B$, si existe un elemento $a \in B$ que cumple que $xa = 0$ y $x + a = 1$

Podemos escribir

$$a \underbrace{=}_{Por\ B5} a + 0 \underbrace{=}_{Por\ B8} a + xx' \underbrace{=}_{Por\ B4} (a + x)(a + x') \underbrace{=}_{Por\ B1} (x + a)(a + x')$$

$$\underset{Por\ hipótesis}{=} 1(a+x') \underset{Por\ B6}{=} a+x'$$

$$x' \underset{Por\ B5}{=} x'+0 \underset{Por\ hipótesis}{=} x'+xa \underset{Por\ B4}{=} (x'+x)(x'+a) \underset{Por\ B1}{=} (x+x')(x'+a)$$

$$\underset{Por\ B7}{=} 1(x'+a) \underset{Por\ B6}{=} x'+a \underset{Por\ B1}{=} a+x'$$

Llegamos entonces a que: $a = a + x'$ y $x' = a + x'$ entonces $a = x'$

Esto nos dice que si x∈ B y un elemento a ∈ B cumple B7 y B8 entonces a es el complemento de x.

5) Toda álgebra de Boole *finita* (es decir B es un conjunto finito) admite una representación mediante un diagrama de Hasse y los elementos en el nivel inmediato superior al 0 se denominan ***átomos***.

Un átomo es un elemento a del álgebra tal que para cualquier otro elemento b del álgebra $ab = a$ o $ab = 0$

En general el diagrama de Hasse de un algebra $\mathcal{B}$ se construye ubicando en el nivel inferior al 0 y luego se ordenarán los elementos según las operaciones supremo e ínfimo del algebra correspondiente. El diagrama de Hasse es una representación gráfica de la relación entre elementos de un conjunto que le da un **orden** de acuerdo al criterio con el que se los relaciona.

Lo mostraremos en los ejemplos a continuación.

Ejemplo 2.1

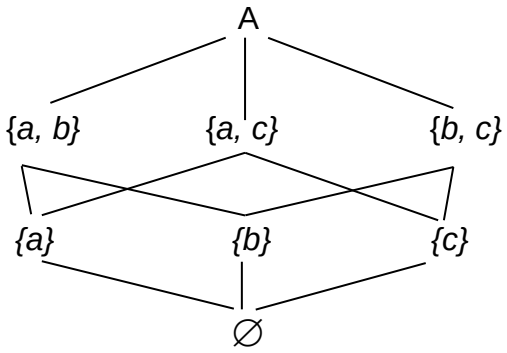
Dado un conjunto H, el conjunto *P(*H) con la ***unión*** como supremo, la ***intersección*** como ínfimo , el ***complemento*** para conjuntos, el vacío $\varnothing$ ***como primer elemento*** y ***H como último elemento*****,** $\Pi = (\boldsymbol{P}(\boldsymbol{H}), \cup, \cap, \ ^{c}, \emptyset, \boldsymbol{H})$ **es un álgebra de Boole**, usualmente llamada ***Álgebra de Partes*** de un conjunto.

Si el conjunto H es finito Π admite una representación por un diagrama de Hasse como se muestra en la figura, los conjuntos unitarios (los que tienen sólo un elemento) son sus átomos.

a) Si tomamos el conjunto $A = \{a, b, c\}$ su conjunto de partes es:

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

Su diagrama de Hasse se representa como sigue:



Algunos ejemplos de construcción:
Como: $\{a\} \cup \{b\} = \{a, b\}$
en el diagrama aparece: $\{a, b\}$ sobre $\{a\}$ y $\{b\}$

Como $\{a, c\} \cap \{b, c\} = \{c\}$
en el diagrama aparece: $\{a, c\}$ y $\{b, c\}$ sobre $\{c\}$

Este diagrama ordena los elementos de *P(A) por inclusión.*

Por ejemplo: como $\{c\} \subseteq \{a, c\}$ entonces en el diagrama aparece: $\{a, c\}$ sobre $\{c\}$

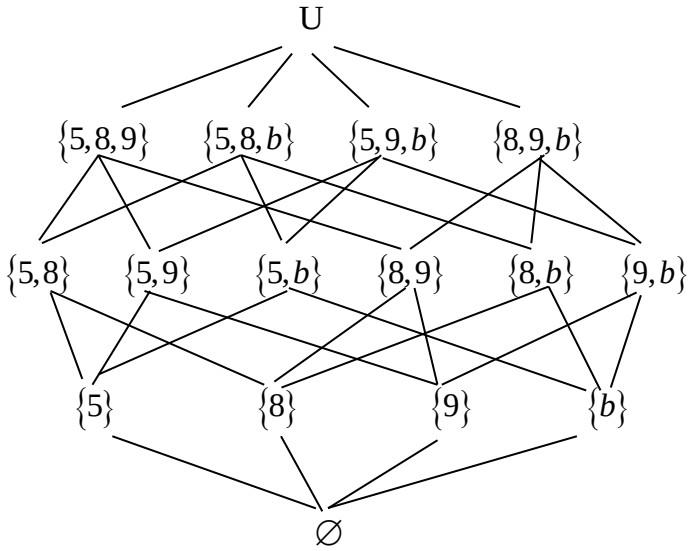
Como $\{c\} \subseteq \{a, c\}$ y $\{a, c\} \subseteq \{a, b, c\}$ entonces aparece: $\{a, b, c\}$ sobre $\{a, c\}$ sobre $\{c\}$

En este caso sus átomos son: *{a}, {b}, {c}*

b) Si tomamos el conjunto $U = \{5,8,9, b\}$, el conjunto *P(U)*, de partes de *U* es:

$P(U) = \{\emptyset, \{5\}, \{8\}, \{9\}, \{b\}, \{5,8\}, \{5,9\}, \{5, b\}, \{8,9\}, \{8, b\}, \{9, b\}, \{5,8,9\}, \{5,8, b\}, \{5,9, b\}, \{8,9, b\}, U\}$

Su diagrama de Hasse es:



En ese ejemplo los átomos son $\{5\}$, $\{8\}$, $\{9\}$ y $\{b\}$.

En la figura se representan los conjuntos por niveles de acuerdo con el número de elementos.

Las líneas de abajo hacia arriba indican la inclusión al nivel inmediato siguiente, se omiten las líneas por transitividad. También indican las uniones al nivel inmediato superior, por ejemplo $\{\mathbf{8},\mathbf{9}\} \cup \{\mathbf{8},\boldsymbol{b}\} \cup \{\mathbf{9},\boldsymbol{b}\} = \{\mathbf{8},\mathbf{9},\boldsymbol{b}\}$**.**

De arriba hacia abajo indican las intersecciones al nivel inmediato inferior como $\{\mathbf{5},\mathbf{8},\boldsymbol{b}\} \cap \{\mathbf{5},\mathbf{9},\boldsymbol{b}\} = \{\mathbf{5},\boldsymbol{b}\}$

Esta representación recibe el nombre de ***diagrama de Hasse*** de *P*(U).

Ejemplo 2.2

a) Sea $M = \{[p], [\sim p],\ \top,\ \bot\}$, el conjunto formado por:

$[p]$ que representa todas las proposiciones del conjunto M equivalentes con p

$[\sim p]$ que representa todas las proposiciones del conjunto M equivalentes con $\sim p$

$\top$ que representa todas las proposiciones que son tautologías

$\bot$ que representa todas las proposiciones que son contradicciones

Definimos en el conjunto M, las operaciones $\wedge$, conjunción, $\vee$, disyunción y $\sim$, negación.

Esto quiere decir que como $p \equiv p \wedge p$, decimos que $[p] = [p \wedge p]$. En consecuencia, tomar $[p]$, que se lee "la clase de todas las proposiciones equivalentes con p" , nos permite poner signo igual en lugar de equivalente.

Del mismo modo, por ejemplo $\sim p \vee p \equiv p \vee \sim p$, decimos entonces que $[\sim p \vee p] = [p \vee \sim p]$ y podemos notar a todas las tautologías con el símbolo $\top = [\sim p \vee p] = [p \vee \sim p]$

Entonces el conjunto $\boldsymbol{\Phi} = (\boldsymbol{M},\ \vee,\ \wedge\ \sim,\ \bot,\ \top)$ es un Algebra de Boole, llamada el **Algebra de Boole del cálculo proposicional** de una letra proposicional**.** Donde las operaciones binarias de ínfimo y supremo son la conjunción y la disyunción respectivamente, la operación unaria complemento es la negación y el **0** es la clase de las contradicciones($\bot$) y el **1** es la clase de las tautologías($\top$).

Este conjunto de proposiciones es cerrado bajo los conectivos conjunción, disyunción y negación cumple las propiedades (B1) a (B8).

Notemos que hemos tomado las clases de las proposiciones para poder tener igualdad, ya que por ejemplo $p \wedge q$ y $q \wedge p$ **no** son ***iguales*** sino lógicamente equivalentes.

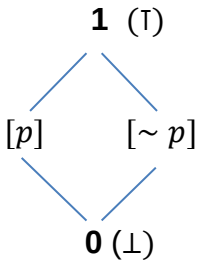
Para obtener el ***Álgebra de Boole del cálculo proposicional*** se define:

$[p \vee q] = [p] \vee [q]$

$[p \wedge q] = [p] \wedge [q]$

$[\sim p] = \sim [p]$

El diagrama de Hasse de este Algebra correspondiente a la generada por una proposición o en general una letra proposicional es:



Observemos que, así como en el diagrama del conjunto de partes de un conjunto, las líneas de abajo hacia arriba indican las uniones al nivel inmediato superior, en este caso indican la disyunción entre los elementos del álgebra.
De arriba hacia abajo, en el diagrama del conjunto de partes indican las intersecciones al nivel inmediato inferior, en este caso indican las conjunciones.

Este diagrama ordena los elementos del conjunto de proposiciones *por implicación,* ya que $[p] \rightarrow ([p] \vee [q])$ es siempre verdadero para cualesquiera $[p]$ y $[q]$.

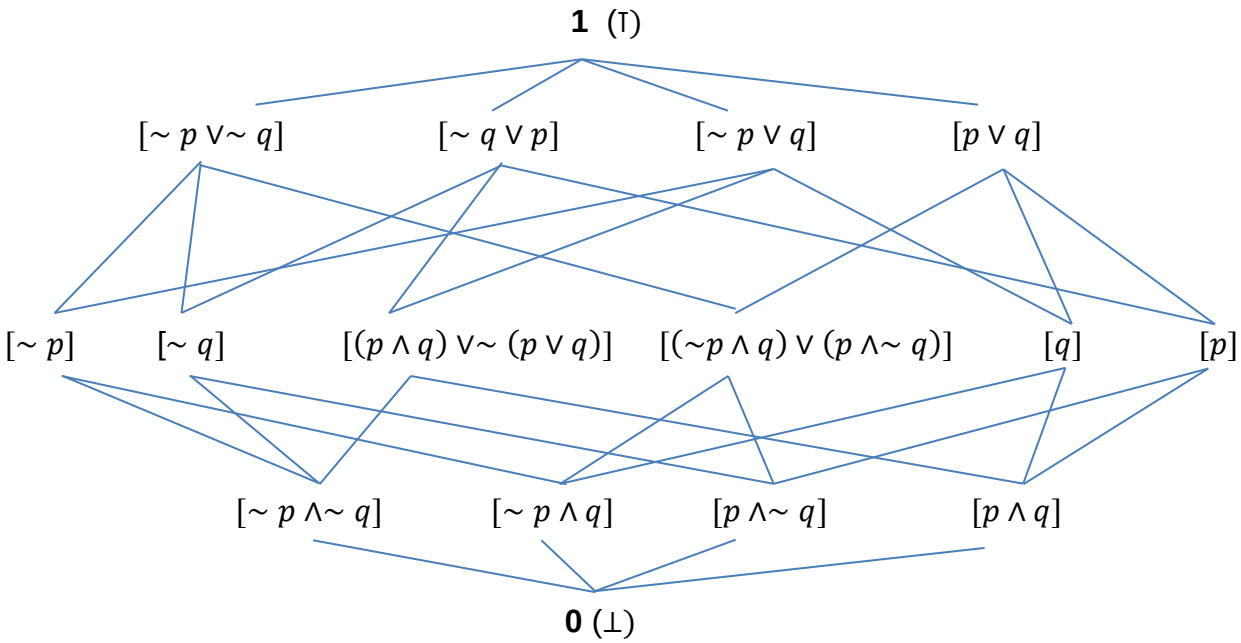
Esto quiere decir que toda vez que para un par de proposiciones w y m si $[w] \rightarrow [m]$ entonces en el diagrama aparece:

$$\begin{matrix} [m] \\ | \\ [w] \end{matrix}$$

b) Sea W el conjunto formado por dos letras proposicionales y todas las proposiciones formadas por sus negaciones, disyunciones y conjunciones: $W = \{[p],\ [q],\ [\sim p],\ [\sim q],\ [p \vee q],\ [p \vee \sim q],\ [\sim p \vee q],\ [\sim p \vee \sim q],\ [p \wedge q],\ [p \wedge \sim q],\ [\sim p \wedge q],\ [\sim p \wedge \sim q],\ [(p \wedge q) \vee \sim (p \vee q)],\ [(\sim p \wedge q) \vee (p \wedge \sim q)],\ \top,\ \bot\}$

Entonces el conjunto $\boldsymbol{\Delta} = (W,\ \wedge,\ \vee,\ \sim,\ \bot,\ \top)$ es un Algebra de Boole, llamada el **Algebra de Boole del cálculo proposicional** de dos letras proposicionales**.**

El diagrama de Hasse de este Algebra es:



Ejemplo 2.3

El conjunto B=$\{0,1\}$ con las operaciones ∨ ***e*** ∧ dadas por las tablas:

∨	0	1
0	0	1
1	1	1

∧	0	1
0	0	0
1	0	1

Y la operación complemento definida por: 0´=1, 1´= 0, es un álgebra de Boole.

El diagrama de Hasse de este Algebra $\mathcal{B}$ = (B, ∨,∧, ´, 0, 1) es:

Ejemplo 2.4

Sea $B^2 = \{0,1\}^2 = \{(x,y): x \in \{0,1\} \wedge y \in \{0,1\}\}$, es decir que B^2 es el conjunto de los pares ordenados que toman valor 0 o valor 1, es el producto cartesiano BxB.

Se definen las operaciones ∨,∧, ´ :

$$(x,y) \vee (w,z) = (x \vee w, y \vee z)$$

∨ definido en B=$\{0,1\}$

$$(x,y) \wedge (w,z) = (x \wedge w, y \wedge z)$$

∧ definido en B=$\{0,1\}$

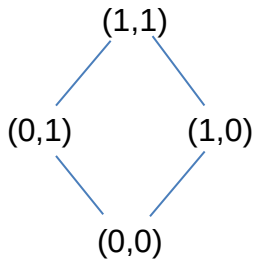
$$(x,y)' = (x', y')$$

′ definido en B=$\{0,1\}$

El (0,0) (neutro para ∨) es el 0 y el (1,1) (neutro para ∧) es el 1.

Así definida $\boldsymbol{\Omega} = (B^2, \vee, \wedge, ', (0,0), (1,1))$ es un Algebra de Boole.

Su diagrama de Hasse es:



Ejemplo 2.5

En general, el conjunto $B^n = \{0,1\}^n = \{(x_1, x_2, \dots, x_n) : x_i \in \{0,1\} \wedge 1 \leq i \leq n \wedge n \in \mathbb{N}\}$, es decir, B^n es el conjunto de las n-uplas, donde cada componente toma valor 0 o valor 1, con las operaciones ∨,∧, ´ :

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

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

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

Donde $(0,0,\dots,0)$ es el 0 y $(1,1,\dots,1)$ es el 1, es un Algebra de Boole.

Ejercicios

8) Sean A, B y C elementos de un Algebra de Boole $\boldsymbol{G} = (\boldsymbol{F}, +, ., ', \mathbf{0}, \mathbf{1})$ indique si las siguientes igualdades son verdaderas o falsas, señalando los axiomas usados:

a) $A + (AC) = (A + A)(A + C)$

b) $AB + 0 = AB$

c) $CB1 = CB$

d) $(AB)' + AB = 0$

e) $CA(CA)' + B = B$

f) $CA + 0 = 0$

g) $(AB)' + AB + CC' = 1$

9) Sea $H = \{a, b, c, d, e\}$ y sea $\Pi = (P(H), \cup, \cap, \ ^c, \emptyset, H)$ el álgebra de Boole de partes de *H.*
Los siguientes conjuntos son elementos de *P(H):* $\{b\}, \{c\}, \{d\}, \{b, c\}, \{c, d\}, \{b, d\}, \{b, c, d\}, \{b, d, e\}, \{b, c, d, e\}$. Represente la parte del diagrama de Hasse donde aparecen esos elementos.

10) Sea W el conjunto formado por las clases de 3 letras proposicionales $[p], [q], [r]$ y sus conjunciones, disyunciones y negaciones. Sea $\Lambda = (W, \vee, \wedge, \sim, \bot, \top)$ el álgebra de Boole del cálculo proposicional.
Las siguientes proposiciones son elementos de *W:* $[p \wedge q]$, $[q \wedge r]$, $[p], [q], [r], [q \vee r]$. Represente la parte del diagrama de Hasse donde aparecen esos elementos.

---

3. Principio de Dualidad y teoremas en un álgebra de Boole

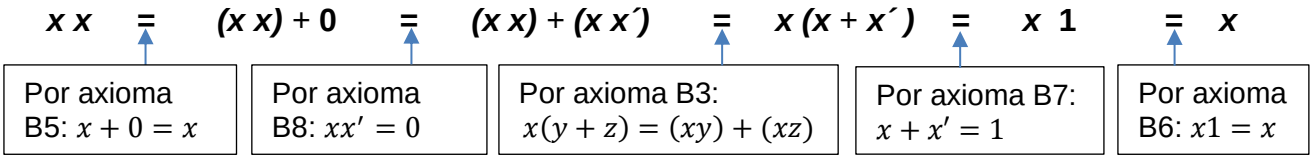
Dualidad:

El enunciado ***dual*** de una proposición en un álgebra de Boole $\mathcal{B}$ = (B,+,., ´, 0, 1) es el que se obtiene intercambiando las operaciones + e . y los elementos **0** y **1** en la proposición original. En la definición (B1) y (B2) son duales una de la otra, lo mismo (B3) y (B4), (B5) y (B6), (B7) y (B8). Por la simetría de estos axiomas que definen un álgebra de Boole $\mathcal{B}$ = (B,+,.., 0, 1) , cualquier proposición en B es verdadera si y sólo si su dual lo es. Este hecho se conoce como ***principio de dualidad***.

Teorema 1. (*Leyes de Idempotencia*). Sea $\mathcal{B}$ = (B,+,., ´, 0, 1) un álgebra de Boole, entonces para cualquier $x \in$ B se cumple que: $\boldsymbol{x + x = x}$, $\boldsymbol{x\,x = x}$

Demostración:

Queremos ver que ***x x = x.*** Partiremos entonces de la expresión ***x x :***

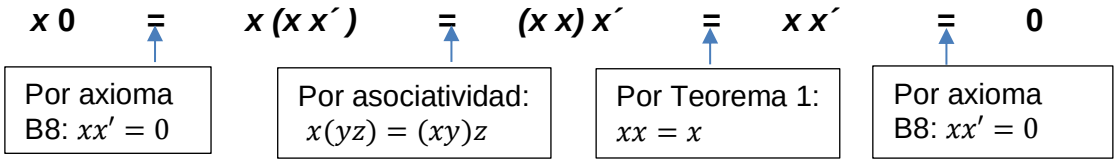


Y por dualidad vale también ***x + x=x.***

Teorema 2. (*Leyes de acotación*). Sea $\mathcal{B}$ = (B,+,., ´, 0, 1) un álgebra de Boole, entonces para cualquier $x \in$ B, se cumple que: ***x* +1 = 1** , ***x* 0 = 0**

Demostración:

Vamos a probar que ***x* 0 = 0**, entonces partimos de la expresión ***x* 0:**

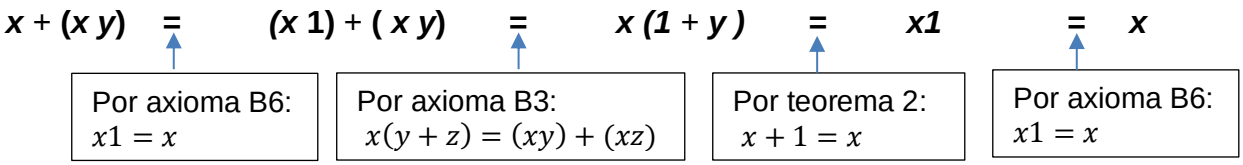


Por dualidad también vale: ***x*+1 = 1.**

Teorema 3. (*Leyes de absorción*). Sea $\mathcal{B}$ = (B,+,., ´, 0, 1) un álgebra de Boole, entonces para cualesquiera $x \in$ B, $y \in$ B, se cumple que: ***x* + (*x y*) = *x* , *x* (*x*+*y*) = *x***

Demostración:

Vamos a demostrar ***x* + (*x y*) = *x.*** Partimos de la expresión: ***x* + (*x y*):**



Por dualidad también es verdadero ***x* (*x*+*y*) = *x* .**

Teorema 4. (*Involución*). Sea $\mathcal{B}$ = (B,+,., ´, 0, 1) un álgebra de Boole, entonces para cualquier $x \in$ B, se cumple que: ***(x')' = x***

Demostración:

El enunciado dice que el complemento de ***x´*** es ***x.***

Es importante notar que el complemento de un elemento del álgebra es único (observación 4), esto quiere decir que si encontramos un elemento a que cumpla los axiomas B7 y B8:

x'+a* = 1 *y* *x' a*= 0 entonces *a es el complemento de x'.

Sabemos por axioma B7 que un elemento supremo su complemento es 1: ***x* + *x´* = 1**

Sabemos por axioma B8 que un elemento ínfimo su complemento es 0: ***x x´*= 0**

Entonces, por los axiomas B1 y B2 también sabemos que: ***x´* + *x* = 1** , ***x´ x* = 0.**

Entonces ***x*** cumple los axiomas ***B7 y B8,*** es el complemento de ***x'***, y se escribe:

(x ')'*= *x

Teorema 5. (*Leyes de De Morgan*). Sea $\mathcal{B}$ = (B,+,., ´, 0, 1) un álgebra de Boole, entonces para $x \in$ B , $y \in$ B,

$$(x + y)' = x'y'$$

$$(xy)' = x' + y'$$

Demostración:

Con la misma idea que en la demostración anterior, teniendo en cuenta que el complemento es único, veremos que: **1)** ***(x +y) + (x' y')=1*** *y que* ***2)*** ***(x +y) (x' y')=0.***

Si esto se cumple quiere decir que ***(x' y')*** *es el complemento de* ***(x +y)***

1) Veremos que ***(x +y) + (x' y') = 1***

$$(x+y) + (x'\ y') = [(x+y)+x']\ [(x+y)+y'] = [(x+x')+y]\ [x+(y+y')] =$$

Por axioma B4: $x + (yz) = (x + y)(x + z)$

Por asociatividad: $x + (y + z) = (x + y) + z$ y Axioma B1: $x + y = y + x$

$$= (1+y)\ (x+1) = 1\ 1 = 1$$

Por axioma B7: $x + x' = 1$

Por Teorema 2: $x + 1 = 1$

Por Teorema 1: $xx = x$

2) Veremos que $(x+y)\ (x'\ y') = 0$

$(x+y)\ (x'\ y') = [x(x'y')] + [y(x'y')] = [(x\,x')\ y'] + [x'(y\ y')] =$

Por axioma B5: $x(y+z) = (xy) + (xz)$

Por asociatividad: $x(yz) = (xy)z$ y Axioma B2: $xy = yx$

$= (0y') + (x'0) = 0\ 0 = 0$

Por axioma B8: $xx' = 0$

Por Teorema 2: $x\,\mathbf{0} = 0$

Por Teorema 1: $xx = x$

Por lo tanto se tiene que $(x'\ y')$ *es el complemento de* $(x+y)$, es decir que:

$(x+y)' = (x'\ y')$.

Y por dualidad también vale que: $(x\ y)' = (x' + y')$

Relación entre teoría de conjuntos, lógica matemática y álgebra booleana y sus notaciones

La lógica matemática y el álgebra booleana son herramientas fundamentales de la computación que se apoyan en las leyes de la teoría de conjuntos para explicar teoremas matemáticos o bien para simplificar expresiones booleanas. En la tabla siguiente se presenta una comparación entre las leyes de la teoría de conjuntos, algunas equivalencias lógicas usadas en lógica matemática para la demostración de teoremas y algunas leyes del álgebra booleana que se utilizan en la simplificación de funciones booleanas que veremos a continuación.

		Teoría de Conjuntos A, B y C conjuntos	**Lógica** p, q, r proposiciones	**Algebra de Boole** x, y, z elementos de un álgebra de Boole
OPERACIONES	Igualdad	$A = B$	$p \Leftrightarrow q \ o\ p \equiv q$ Entonces $[p] = [q]$	$x = y$
		Unión: $A \cup B$	Disyunción: $p \vee q$	Supremo: $x + y$
		Intersección: $A \cap B$	Conjunción: $p \wedge q$	Infimo: xy
		Complemento: A^c	Negación: $\sim p$	Complemento: x'
AXIOMAS Y PROPIEDADES	Axiomas B1 y B2: Leyes conmutativas	$A \cup B = B \cup A$ $A \cap B = B \cap A$	$p \vee q \equiv q \vee p$ $p \wedge q \equiv q \wedge p$	$x + y = y + x$ $xy = yx$
	Axiomas B3 y B4: Leyes distributivas	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$ $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$	$x(y + z) = (xy) + (xz)$ $x + (yz) = (x + y)(x + z)$
	Axiomas B5 y B6: Neutros	$A \cup \emptyset = A$ $A \cap U = A$	$p \vee \perp \equiv p$ $p \wedge \top \equiv p$	$x + 0 = x$ $x1 = x$
	Axiomas B7 y B8: Complementos	$A \cup A^c = U$ $A \cap A^c = \emptyset$	$p \vee \sim p \equiv \top$ $p \wedge \sim p \equiv \perp$	$x + x' = 1$ $xx' = 0$
	Leyes asociativas	$A \cup (B \cup C) = (A \cup B) \cup C$ $A \cap (B \cap C) = (A \cap B) \cap C$	$p \vee (q \vee r) \equiv (p \vee q) \vee r$ $p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$	$x + (y + z) = (x + y) + z$ $x(yz) = (xy)z$
	Teorema 1: Leyes de idempotencia	$A \cup A = A$ $A \cap A = A$	$p \vee p \equiv p$ $p \wedge p \equiv p$	$x + x = x$ $xx = x$
	Teorema 2: Leyes de acotación	$A \cup U = U$ $A \cap \emptyset = \emptyset$	$p \vee \top \equiv \top$ $p \wedge \perp \equiv \perp$	$x + 1 = 1$ $x0 = 0$
	Teorema 3: Leyes de absorción	$A \cup (A \cap B) = A$ $A \cap (A \cup B) = A$	$p \vee (p \wedge q) \equiv p$ $p \wedge (p \vee q) \equiv p$	$x + (xy) = x$ $x(x + y) = x$
	Teorema 4: Involución	$(A^c)^c = A$	$\sim (\sim p) \equiv p$	$(x')' = x$
	Teorema 5: Leyes de Morgan	$(A \cup B)^c = A^c \cap B^c$ $(A \cap B)^c = A^c \cup B^c$	$\sim (p \vee q) \equiv \sim p \wedge \sim q$ $\sim (p \wedge q) \equiv \sim p \vee \sim q$	$(x + y)' = x'y'$ $(xy)' = x' + y'$

En la tabla hay que observar que las leyes de la lógica matemática y el álgebra booleana son formalmente las mismas que las de la teoría de conjuntos, además las operaciones equivalentes se denotan de manera diferente en cada una.

Simplificación de expresiones booleanas mediante teoremas del Algebra de Boole.

Las variables booleanas son variables que toman valores 0 o 1.

Las ***funciones booleanas*** son funciones con dominio en B^n y codominio en B: $f: B^n \to B$.

Es decir que las funciones booleanas también toman valor 0 o 1, dependiendo de los valores de sus variables.

Se llama ***conjunto de verdad*** de una función booleana f al conjunto de elementos del dominio para los cuales la función vale 1: $\boldsymbol{V(f) = \{(x_1, x_2, \dots, x_n) \in B^n : f(x_1, x_2, \dots, x_n) = 1\}}$

Así, una función booleana puede representarse mediante una tabla de verdad, por ejemplo, para una función de dos variables, tenemos:

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

Esta función puede representarse con una **expresión booleana**, donde aparecen los valores de las variables del conjunto de verdad de f , es decir los valores para los cuales f vale 1.

Por ejemplo si tenemos la función booleana dada por la siguiente tabla:

x	y	$f(x,y)$
0	0	**0**
0	1	**1**
1	0	**0**
1	1	**1**

La función puede representarse como $f(x,y) = x'y + xy$. Es decir que la función queda definida por su conjunto de verdad.

Esta expresión a su vez puede simplificarse usando los axiomas y teoremas del algebra de Boole:

$$x'y + xy = (x' + x)y = 1y = y$$

Por axioma B5: $x(y+z) = (xy) + (xz)$

Por axioma B7: $x' + x = 1$

Por axioma B6: $x1 = x$

Ejemplo 3.1:

Una fábrica de refrescos desea que un sistema automático saque de la banda de transportación un refresco que no cumple con los requisitos mínimos de calidad, y para esto se cuenta con cuatro sensores en diferentes puntos del sistema de transportación para revisar aspectos importantes de calidad. Si los sensores son A, B, C y D y el sistema F es el que determina cuando sacará el refresco, tenemos el siguiente grupo de señales:

A	B	C	D	F
0	0	0	0	0
0	0	0	1	1
0	0	1	0	0
0	0	1	1	1
0	1	0	0	0
0	1	0	1	0
0	1	1	0	0
0	1	1	1	0
1	0	0	0	0
1	0	0	1	1
1	0	1	0	1
1	0	1	1	1
1	1	0	0	0
1	1	0	1	0
1	1	1	0	0
1	1	1	1	0

En la tabla anterior se muestran todas las posibles combinaciones de valores 0 o 1, de las variables.

La tabla indica que cuando F=1 es refresco debe ser retirado.

Esto implica que el refresco será extraído de la banda de transportación en cualquiera de los siguientes casos, ya que para cualquiera de ellos se tiene que F = 1:

A = 0 y B = 0 y C = 0 y D = 1, es decir cuando A’ =1 y B’ =1 y C’ =1 y D = 1

A = 0 y B = 0 y C = 1 y D = 1, es decir cuando A’ =1 y B’ =1 y C =1 y D = 1

A = 1 y B = 0 y C = 0 y D = 1, es decir cuando A =1 y B’ =1 y C’ =1 y D = 1

A = 1 y B = 0 y C = 1 y D = 1, es decir cuando A =1 y B’ =1 y C =1 y D = 1

A = 1 y B = 0 y C = 1 y D = 0, es decir cuando A =1 y B’ =1 y C =1 y D’ = 1

La función booleana que equivale a la tabla anterior es:

F = A'B'C'D + A'B'CD + AB'C'D + AB'CD + AB'CD'

La función booleana indica solamente los casos en donde el refresco será extraído, pero existen varios casos más en donde se dejará pasar porque cumple con los requisitos mínimos de calidad.

Observemos que podemos simplificar la expresión booleana para extraer los refrescos usando los axiomas y teoremas del algebra de Boole:

A'B'C'D + A'B'CD + AB'C'D + AB'CD + AB'CD' = A'B'D(C'+C) + AB'D(C'+C) + AB'CD' =

Por axioma B3: $x(y+z) = (xy) + (xz)$

= A'B'D(1) + AB'D(1) + AB'CD' = A'B'D + AB'D + AB'CD' = B'D(A'+A) + AB'CD' =

Por axioma B7: $x + x' = 1$

Por axioma B6: $x1 = x$

Por axioma B3: $x(y+z) = (xy) + (xz)$

= B'D(1) + AB'CD' = B'D + AB'CD'

Por axioma B7: $x + x' = 1$

Por axioma B6: $x1 = x$

De esta forma hemos obtenido una expresión simplificada de la función original

Esto nos dice que: F = A'B'C'D + A'B'CD + AB'C'D + AB'CD + AB'CD' = B'D + AB'CD'

Así podemos decir que el refresco se sacará de la cinta cuando:

B=0 y D=1 o cuando A=1 y B=0 y C=1 y D=0

Ejemplo 3.2:

Simplificar la expresión booleana: A'B+(ABC)'+C(B'+A)

A'B+(ABC)'+C(B'+A) = Por Leyes de De Morgan: $(xy)' = x' + y'$

A'B+(A'+B'+C')+C(B'+A) = Por axioma B3: $x(y+z) = xy + xz$

A'B+(A'+B'+C')+CB'+CA= Por axioma B1: $x + y = y + x$ y Por leyes asociativas: $x + (y+z) = (x+y) + z$

(A'B+A') + C' + (B'+CB') + CA =	Por axioma B5: $x1 = x$ Aplicado a: (A'B+A')=A'B+A'1 y (B'+CB')=B'1+CB'
A'B+A'1 + C' + B'1+CB' + CA =	Por axioma B3: $x(y+z) = xy + xz$ y Por axioma B1: $x + y = y + x$
A'(B+1) + B'(1+C) + C'+CA =	Por Axioma B6: $x + 1 = 1$ y Por axioma B4: $x + (yz) = (x + y)(x + z)$
A'1 + B'1 + [(C'+C)(C'+A)] =	Por Axioma B5: $x1 = x$ y Por axioma B8: $x + x' = 1$
A' + B' + [1(C' + A)] =	Por Axioma B5: $x1 = x$
A' + B' + (C' + A) =	Por axioma B1: $x + y = y + x$ y Por leyes asociativas: $x + (y + z) = (x + y) + z$
(A' + A) + (B' + C') =	Por axioma B8: $x + x' = 1$
1 + (B' + C') =	Por Axioma B6: $x + 1 = 1$

1

La expresión booleana en su forma más simple es 1, y este resultado indica que si se sustituyen las diferentes combinaciones con los valores binarios 0 o 1 de las variables A, B y C en la expresión inicial, entonces el resultado será siempre igual a 1 (lo que se conoce en lógica matemática como tautología).

En general luego de un proceso de simplificación el resultado no siempre es 1, en cambio lo que se espera es obtener una expresión más simple conformada por menos variables.

Cuando se plantea un problema, la expresión booleana no es necesariamente la óptima, en el sentido de que sea la más sencilla de implementar mediante compuertas lógicas, por eso el proceso de simplificación es muy importante, para implementar circuitos más claros.

El proceso de simplificación siempre se hace usando axiomas y teoremas, existen métodos que los aplican usando algoritmos, en este curso haremos sólo la aplicación directa de los axiomas y teoremas. En general la simplificación se hace para dejar la expresión como una

suma de productos o como un producto de sumas, dependiendo de la manera de hacer su implementación posterior.

En este curso entenderemos como expresión simplificada, aquella que esté expresada como suma de productos (los productos entre variables o sus complementos) y que éstos sean el mínimo número posible.

Así, la expresión: **XYZ+X'YZ+WZ** es una suma de productos pero no está simplificada.

Entonces: **XYZ+X'YZ+WZ = (X+X')YZ+WZ = 1YZ+WZ = YZ+WZ** está simplificada.

Por axioma B3: $x(y+z)=xy+xz$	Por axioma B8: $x+x'=1$	Por Axioma B5: $x1=x$

Observemos que podríamos escribir **YZ+WZ=(Y+W)Z** pero en este caso no es una suma de productos.

Ejercicios

11) Sean $B=\mathbb{Z}, +$ la suma usual de enteros, . el producto usual de enteros y para cada $a \in \mathbb{Z},$ se define $a'=-a$. ¿Es $H=(B,+,.,',0,1)$ un álgebra booleana?

12) Demostrar que si 0 y 1 son el primer y último elemento de un Algebra de Boole, entonces $1'=0$ y $0'=1$

13) a) Probar la Ley de De Morgan: $(xy)'=x'+y'$

b) Expresar las Leyes de De Morgan en los conjuntos y en el cálculo proposicional, con los símbolos y operaciones que corresponden en cada caso

14) Si x,y,z,w son variables de un Álgebra de Boole, simplificar (hasta su mínima expresión) las siguientes expresiones, indicando las propiedades usadas:

a) $x+xy+x(x+y)=$

b) $x'+[(x\,x')']=$

c) $x(y+x')'=$

d) $[x(y'y)]+[y(x+x')]=$

e) $y'xy+y'x+ywx'+yww=$

f) $[(x+y)'+z'][z'+(x+(yz)')'] =$

15) Si x, y, z son variables de un Álgebra de Boole, demostrar que:

a) $x'y'z + x'yz + xy'z + xyz + xyz' = z + xy$

b) $x + (y+0)' + y'z = x + y'$

c) $x + y' + (xy+0)' = y'$

d) $x + (y+1)' + xy = x$

e) $((zx)'zx)' + xy + xy' = 1$

f) $x((y'+x)' + (y'+y)') = 0$

16) a) Definir la expresión booleana que representa la siguiente función:

A	B	C	F(A,B,C)
0	0	0	1
0	0	1	0
0	1	0	0
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	1
1	1	1	0

b) Simplificar la expresión hallada.

17) a) Definir la expresión booleana que representa la siguiente función:

A	B	C	D	F(A,B,C,D)
0	0	0	0	1
0	0	0	1	0
0	0	1	0	1
0	0	1	1	0
0	1	0	0	1
0	1	0	1	1
0	1	1	0	1
0	1	1	1	1
1	0	0	0	0
1	0	0	1	0
1	0	1	0	0
1	0	1	1	0
1	1	0	0	0
1	1	0	1	1
1	1	1	0	0
1	1	1	1	1

b) Simplificar la expresión hallada.

---

4. Isomorfismo de álgebras de Boole

Definición

Sean $\mathcal{B}_1$ = (B_1,+,., ´, 0, 1) y $\mathcal{B}_2$ = (B_2,+,., ´, 0, 1) dos álgebras de Boole. Un ***isomorfismo*** entre $\mathcal{B}_1$ y $\mathcal{B}_2$ es una función biyectiva $f: B_1 \to B_2$ que cumple las siguientes propiedades:

Para todo par $x \in B_1, y \in B_1$: i) $f(x+y) = f(x) + f(y)$

ii) $f(xy) = f(x)f(y)$

iii) $f(x') = [f(x)]'$

Es decir que la imagen por f del supremo $x+y$ entre x e y es igual al supremo $f(x)+f(y)$ entre $f(x)$ y $f(y)$, la imagen por f del ínfimo xy es el ínfimo $f(x)f(y)$ entre sus imágenes y la imagen por f de x' (el complemento de x) es igual al complemento $[f(x)]'$ de su imagen, siendo x e y elementos de B_1 y $f(x)$ y $f(y)$ elementos de B_2.

Un isomorfismo es una biyección que conserva las operaciones. Cuando existe tal isomorfismo entre B_1 y B_2, se dice que $\mathcal{B}_1$ y $\mathcal{B}_2$ son ***isomorfas.***

$\mathcal{B}_1$ y $\mathcal{B}_2$ tienen elementos distintos pero tienen *la misma forma*, sus diagramas de Hasse coinciden.

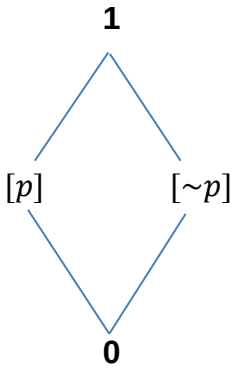
Ejemplo 4.1

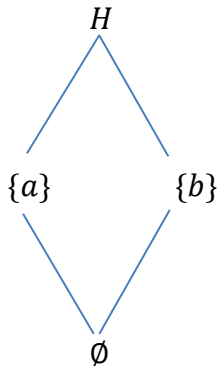
Sea $P(H)$ el conjunto de partes de H, siendo $H = \{a, b\}$, entonces $P(H) = \{\emptyset, \{a\}, \{b\}, H\}$ y el conjunto B formado por las proposiciones $[p]$, $[\sim p]$, con primer elemento $0 = [p \wedge \sim p]$ y último $1 = [p \vee \sim p]$.

La función $f: B \longrightarrow P(H)$ dada por:

$f(0) = \emptyset$, $f([p]) = \{a\}$, $f([\sim p]) = \{b\}$, $f(1) = H$ es un isomorfismo entre las álgebras de Boole $\mathcal{B}_1 = (B, \vee, \wedge, \sim, 0, 1)$ y $\mathcal{B}_2 = (P(H), \cup, \cap, {}^c, \emptyset, H)$.

Se observa que sus respectivos diagramas de Hasse coinciden:





Nótese que en $P(H)$ el 0 es el conjunto ∅ y el 1 es el conjunto H, mientras que en B el **0 y el 1** son símbolos que representan una contradicción y una tautología respectivamente.

Teorema 6. Sea $\mathcal{B}$ = (B,+,., ´, 0, 1) un álgebra de Boole, con B finito.

Entonces existe un conjunto U tal que $\mathcal{B}$ = (B,+,., ´, 0, 1) es isomorfa al álgebra de partes $\Pi = (\boldsymbol{P}(\boldsymbol{U}),\cup,\cap, \ ^{\boldsymbol{c}}, \emptyset, \boldsymbol{U})$.

Sin hacer una demostración formal del teorema, podemos ver que:

Llamemos $A_{\mathrm{B}} = \{b_1, b_2, \ldots b_n\}$ al conjunto de átomos de $\mathcal{B}$

Tomemos un conjunto $\boldsymbol{U} = \{x_1, x_2, \ldots x_n\}$, con la misma cantidad de elementos que los átomos de $\mathcal{B}$

Entonces el conjunto de los átomos del álgebra $\Pi(\boldsymbol{P}(\boldsymbol{U}),\cup,\cap, \ ^{\boldsymbol{c}}, \emptyset, \boldsymbol{U})$, que podemos llamar $A_{\Pi} = \{\{x_1\}, \{x_2\}, \ldots \{x_n\}\}$

Podemos construir la función que a cada átomo b_i de B le asigna el conjunto unitario $\{x_i\}$.

A partir de ahí se construye una biyección f entre B y $\boldsymbol{P}(\boldsymbol{U})$, respetando las propiedades.

Así f resulta ser un isomorfismo entre las álgebras y decimos que $\mathcal{B}$ es isomorfa al álgebra de partes Π.

Teorema 7.(Corolario del Teorema 6).

El número de elementos de un álgebra de Boole finita es una potencia de dos, 2^n con n>0.

Demostración:

Si $\mathcal{B}$ = (B,+,., ´, 0, 1) es un álgebra de Boole y B es finito, por el teorema anterior existe un conjunto *U* tal que $\mathcal{B}$ es isomorfa al álgebra de partes $\boldsymbol{\Pi} = (\boldsymbol{P}(\boldsymbol{U}), \cup, \cap, \ ^{\boldsymbol{c}}, \emptyset, \boldsymbol{U})$**.**

Por existir una función biyectiva $f: B \to P(U)$, B y $P(U)$ tienen la misma cantidad de elementos y como ya vimos que si U tiene *n* elementos, *P*(U) tiene 2^n elementos, se concluye que B también tiene 2^n elementos.

El número *n* debe ser mayor que 0 porque B tiene por lo menos dos elementos: el primero y el último.

Observación.

La condición enunciada en el Teorema 7 es necesaria, por lo que si el número de elementos de un conjunto *no* es una potencia de dos, se puede concluir que tal conjunto *no* es un álgebra de Boole.

La condición ***no*** es suficiente, el hecho de que un conjunto tenga 2^n elementos, con $n \geq 1$, ***no*** asegura que sea un álgebra de Boole.

Ejercicios

18) Sea $f: B_1 \to B_2$ un isomorfismo de algebras booleanas. Si llamamos 0_1 y 0_2 al 0 de B_1 y B_2 respectivamente y 1_1 y 1_2 al 1 de B_1 y B_2 respectivamente, demostrar que $f(0_1) = 0_2$ y $f(1_1) = 1_2$

19) a) Hallar un isomorfismo entre $\boldsymbol{\Omega} = (B^2, \vee, \wedge, ', (0,0), (1,1))$ y el álgebra de Boole de partes de un conjunto. Hacer los diagramas de Hasse de ambas álgebras.

b) Hallar un isomorfismo entre $\boldsymbol{\Omega} = (B^3, \vee, \wedge, ', (0,0,0), (1,1,1))$ y el álgebra de Boole de partes de un conjunto. Hacer los diagramas de Hasse de ambas álgebras.

Anexo

Una aplicación: Los circuitos y las puertas lógicas

Una aplicación del álgebra de Boole es el álgebra de circuitos de conmutación. Un *circuito de conmutación* es una red eléctrica formada por interruptores conectados por cable,

con dos estados que son *cerrado* y *abierto*, a los que se les asigna, respectivamente, los valores 1 y 0, y dos terminales ***s*** y *t*.

La corriente eléctrica fluye de ***s*** a ***t*** a través del punto donde está localizado un interruptor si y sólo si éste está cerrado

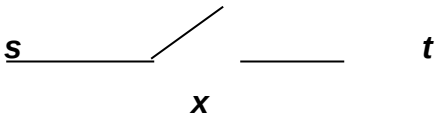


figura 1

En la figura 1 se muestra un circuito con un solo interruptor.

El circuito de la figura 2 está cerrado si y sólo si *x* o *y* están cerrados. Esta combinación de interruptores se indica con $x + y$, y se dice que los interruptores *x*, *y* están *en paralelo*

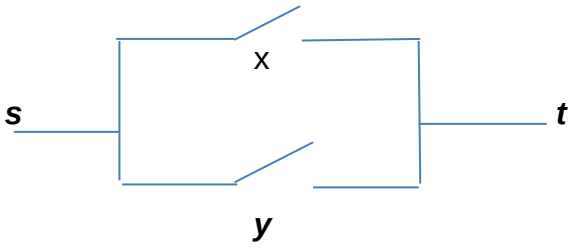


figura 2

Dos interruptores *x* e *y* están *en serie* si están conectados como en la figura 3

figura 3

En este caso el circuito está cerrado si y sólo si ambos *x* e *y* lo están, esta combinación de interruptores se indica con xy.

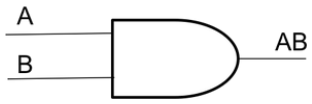
La operación ***supremo*** es la conexión en paralelo y el ***ínfimo*** es la conexión en serie. Los valores que pueden tomar los interruptores son sólo dos: {ON, OFF} o bien {1,0}. Si dos interruptores operan en tal forma que cuando uno está abierto el otro está cerrado, y viceversa entonces se designará uno de ellos con una letra y el otro por su ***complemento***.

Se indica con **0** al circuito que está siempre abierto y con **1** al que está siempre cerrado.

Con estas operaciones el conjunto de circuitos de conmutación es un álgebra de Boole y tiene todas sus propiedades.

En el diseño actual de redes eléctricas los interruptores se reemplazan por otros dispositivos llamados ***puertas lógicas***, que se corresponden con las operaciones booleanas “+”, “.” y “ ‘ “ (complemento).

Las ***puertas lógicas*** que estudian en distintas materias, son dispositivos que desarrollan las expresiones booleanas, por ejemplo, la puerta AND, representa la expresión AB, siendo A y B elementos del álgebra:



Un circuito es un conjunto de puertas lógicas interconectadas, que también admiten una representación gráfica, con tablas de verdad o como una función booleana. Estos circuitos implementan funciones esenciales de una computadora.

Los teoremas que hemos probado se derivan de los axiomas enunciados en la definición de Algebras de Boole y nos permitirán simplificar expresiones booleanas transformándolas en otras más sencillas, que pueden implementarse en circuitos más claros, con menos costo y más eficientes.

Gran cantidad de sistemas de control, también conocidos como digitales, usan señales binarias y éstas son un falso o un verdadero que proviene de sensores que mandan la información al circuito de control, que lleva a cabo la evaluación para obtener un valor que indicará si se lleva a cabo o no una determinada actividad, como encender un foco, arrancar un equipo de ventilación en un cine o ejecutar una operación matemática en una computadora.

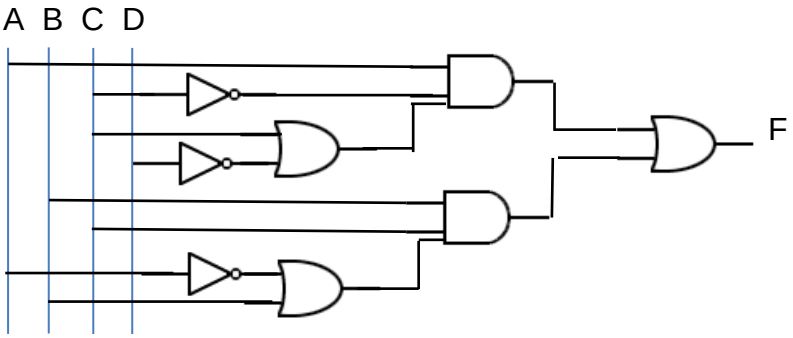
Para resolver un problema práctico en el cual se desea automatizar un proceso, es necesario realizar un análisis detallado de lo que se quiere lograr, así como de los tipos de sensores necesarios para obtener las señales. Una vez que se conoce esto se plantea el funcionamiento del circuito lógico en una expresión matemática, la cual recibe el nombre de función booleana, y cada una de las variables que integran esta función representa un sensor que provee al circuito de una señal de entrada.

Las simplificaciones sirven para diseñar un sistema de puertas lógicas lo más sencillo posible.

Por ejemplo, la función:

F(A,B,C,D)=AC’(C+D’)+BC(A’+B)

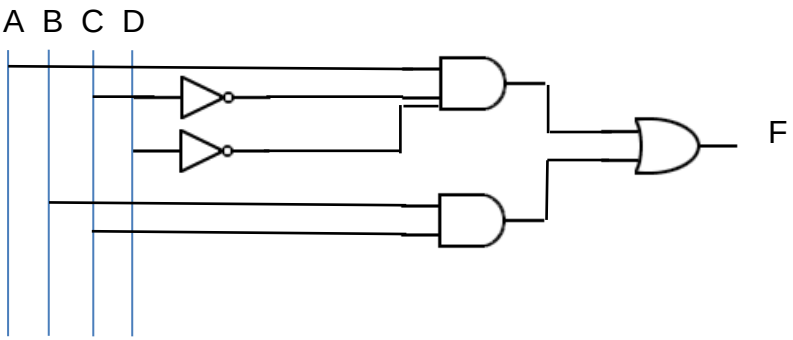
Puede representarse mediante puertas lógicas como sigue:



Si ahora realizamos una simplificación, tendríamos:

AC'(C+D') + BC(A'+B) =	Por axioma B3: $x(y+z) = xy + xz$
AC'C + AC'D' + BCA' + BCB =	Por axioma B7: $xx' = 0$ y Por axioma B2: $xy = yx$
A0 + AC'D' + BCA'+CBB =	Por Teorema 2: $x0 = 0$ y Por Teorema 1: $xx = x$
0 + AC'D' + BCA' + CB =	Por Axioma B5: $x + 0 = x$ y Por axioma B3: $x(y+z) = xy + xz$ y Por axioma B2: $xy = yx$
AC'D' + BC(A'+1) =	Por Axioma B6: $x + 1 = 1$ Por Axioma B5: $x1 = x$
AC'D' + BC	

Entonces, su representación con puertas lógicas es:



Bibliografía

- *Ramón Espinosa Armenta,* ***Matemática Discreta,*** Editorial Alfaomega, Mexico, 2010*.*
- *Elliott Mendelson,* ***Boolean Algebra and Switching Circuits****, McGraw-Hill.*