UNIVERSIDAD DE EL SALVADOR
FACULTAD MULTIDISCIPLINARIA ORIENTAL
DEPARTAMENTO DE CC.NN Y MATEMÁTICA
SECCIÓN DE MATEMÁTICA

TRABAJO DE GRADO

HOMOMORFISMOS ENTRE ÁLGEBRAS BOOLEANAS

PRESENTADO POR:
ANDRÉS ARMANDO PÉREZ TORRES
WENDY ADELY VÁSQUEZ LAZO

PARA OPTAR AL GRADO DE:
LICENCIADO EN MATEMÁTICA

DOCENTE ASESOR DIRECTOR
M.I. WILLIAM NOÉ MERLOS JUÁREZ

DOCENTE ASESOR ESPECIALISTA
M.I. TOBÍAS HUMBERTO MARTÍNEZ LOVO

CUIDAD UNIVERSITARIA ORIENTAL, DICIEMBRE DEL 2020

SAN MIGUEL EL SALVADOR CENTROAMÉRICA

UNIVERSIDAD DE EL SALVADOR

AUTORIDADES

MSC. ROGER ARMANDO ARIAS ALVARADO
RECTOR

PHD. RAÚL ERNESTO AZCÚNAGA LÓPEZ
VICE-RECTOR ACADÉMICO

ING. JUAN ROSA QUINTANILLA
VICE-RECTOR ADMINISTRATIVO

ING. FRANCISCO ALARCÓN
SECRETARIO GENERAL

LIC. RAFAEL HUMBERTO PEÑA MARÍN
FISCAL GENERAL

UNIVERSIDAD DE EL SALVADOR
FACULTAD MULTIDISCIPLINARIA ORIENTAL

AUTORIDADES

LIC. CRISTÓBAL HERNÁN RÍOS BENÍTEZ
DECANO

LIC. OSCAR VILLALOBOS
VICE-DECANO

LIC. ISRAEL LÓPEZ MIRANDA
SECRETARIO

Agradecimientos

Agradezco a Dios por ser mi guía y acompañarme en el transcurso de mi vida, brindándome paciencia y sabiduría para culminar con éxito mis metas propuestas.

A mis padres **José Andrés Pérez Méndez** y **Paula Torres de Pérez**, por ser mi pilar fundamental y haberme apoyado incondicionalmente, pese a las adversidades e inconvenientes que se presentaron.

Agradezco a mis tres hermanos y mis tres hermanas que me brindaron apoyo psicológico y económico para poder vencer los obstáculos y poder culminar mi carrera.

A mi compañera de tesis **Wendy Adely Vásquez Lazo**, por haber sido una excelente compañera y amiga durante la carrera y en el trabajo de grado.

Agradezco a mis asesores de tesis **M.I. Tobías Humberto Martínez Lovo** y **M.I. William Noé Merlos Juárez** quienes con sus experiencias, conocimientos y motivación me orientaron en la investigación.

Agradezco a todos los docentes que con su sabiduría, conocimientos y apoyo, motivaron desarrollarme como persona y profesionalmente en la Universidad de El Salvador FMO.

Andrés Armando Pérez Torres

Dios, tu amor y tu bondad no tienen fin, me has acompañado a lo largo de mi carrera, gracias por ser mi fortaleza en mis momentos de debilidad, también te agradezco por cada uno de mis logros que sin duda alguna son resultado de tu ayuda. Este trabajo de grado ha sido una gran bendición en todo sentido y te lo agradezco porque gracias a ti he cumplido está meta.

Dedico este logro a mis padres, mi papá **José Fredy Vásquez Vásquez** quien ha sido mi fuente de inspiración, dado que desde mis primeros años de vida he observado su entrega y pasión a su profesión, por ello mi mayor sueño era ser como él, mi mamá **Priscila Lazo de Vásquez** quien es mi confidente, mi mejor amiga, y quien me motiva a confiar y creer en Dios. A ambos les agradezco por el apoyo que me han brindado en todo momento y por sus consejos que siempre han sido mi fortaleza.

Agradezco, a mis hermanos **Yossely Cristely Vásquez Lazo** y **Gabriel Jossue Vásquez Lazo** porque me han apoyado en el transcurso de vida y mi carrera.

A **Andrés Armando Pérez Torres** por haber sido un excelente compañero y amigo en el transcurso de nuestra carrera, por su paciencia y por el apoyo que me ha brindado en la realización de nuestro trabajo de tesis.

A cada uno de los catedráticos que me han compartido sus conocimientos en el transcurso de mi formación y de manera especial, agradezco grandemente a mis asesores de trabajo de grado,**M.I. Tobías Humberto Martínez Lovo** asesor especialista y **M.I. William Noé Merlos Juárez** asesor director quienes con paciencia y sabiduría se han esforzado para ayudarme a llegar al punto en el que me encuentro.

A cada uno de mis compañeros y amigos, por todos los momentos que compartimos juntos, por todas esas tareas que realizamos juntos, por todas esas veces en las cuales me explicaron y apoyaron, gracias por esa confianza que en mi depositaron y por haber hecho de mi etapa universitaria un trayecto de vivencias que jamas olvidare.

A **Alexander Molina** por siempre motivarme y por apoyarme incondicionalmente en el transcurso de mi carrera y la realización de mi trabajo de tesis.

Wendy Adely Vásquez Lazo

Índice general

Agradecimientos IV

Resumen VIII

Introducción X

Justificación XII

Objetivos XIII

Antecedentes XIV

1. Lógica Proposicional 1

1.1. Proposición 1

1.2. Operadores lógicos y sus tablas de verdad. 2

1.3. Cuantificadores 15

1.4. Conjuntos 19

1.5. Álgebra booleana 28

1.6. Anillos booleanos 31

1.7. Campos de subconjuntos 44

1.8. Orden 45

2. Estructuras de Álgebras Booleanas 53

2.1. Ideales y filtros booleanos 53

2.2. Homomorfismos entre álgebras booleanas 78

2.3. Homomorfismos entre anillos booleanos 95

2.4. Cociente de anillos booleanos 98

3. Aplicaciones del Álgebra Booleana **108**

3.1. Compuertas Lógicas 108

3.1.1. *Compuertas AND de dos entradas* 110

3.1.2. *Compuertas AND de varias entradas* 111

3.1.3. *Compuertas OR de dos entradas* 112

3.1.4. *Compuertas OR de varias entradas* 113

3.1.5. *Compuertas NOT o Inversores* 115

3.1.6. *Compuerta YES* 116

3.1.7. *Compuertas NAND de dos entradas* 117

3.1.8. *Compuertas NAND de varias entradas* 118

3.1.9. *Compuertas NOR de dos entradas* 119

3.1.10. Compuertas NOR de varias entradas 121

3.1.11. Compuertas OR exclusivas o XOR 122

3.1.12. Compuertas NOR exclusivas o XNOR 122

3.1.13. *Operaciones booleanas* 123

3.2. El código genético y $\mathbb{Z}_2^6$ 134

Bibliografía **141**

Resumen

La conexión de las álgebras booleanas a través de homomorfismos. Se da inicio a partir de la Lógica Proposicional, definiendo sus operadores y conectivos lógicos, así como también los cuantificadores, teoría de conjuntos, un poco de álgebra proposicional y álgebra de conjuntos. Posteriormente se da paso al estudio del Álgebra Booleana definiendo el álgebra booleana, su estructura, propiedades, también se definirá una subálgebra booleana, anillos booleanos, ideales booleanos, ideales maximales, los homomorfismos de álgebras, sus propiedades, el concepto booleano de filtro y el cociente de anillos booleanos. Cuando se habla sobre aplicaciones del álgebra booleana es común escuchar que las álgebras booleanas son la base de la información digital, y que son parte fundamental de los circuitos electrónicos, debido a que el funcionamiento de las computadoras está basado en la estructura booleana del sistema binario. Pero, no es natural imaginar que dentro de los organismos vivos se pudiera hacer uso de estructuras booleanas. Es así, como se finaliza con el estudio de las compuertas lógicas y también se describe brevemente un modelo del código genético dado en términos de álgebras booleanas y $\mathbb{Z}_2^6$.

Palabras claves: Homomorfismo booleano, isomorfismo booleano, álgebra booleana, anillo booleano, ideal booleano, filtros, cociente booleano, circuitos lógicos, retículo y código genético.

Abstract

The connection of Boolean algebras through homomorphisms. It starts from Propositional Logic, defining its logical connectives and operators, as well as quantifiers, set theory, a bit of propositional algebra and set algebra. Subsequently, the study of Boolean Algebra is given, defining the Boolean algebra, its structure, properties, a Boolean subalgebra, Boolean rings, Boolean ideals, maximum ideals, the homomorphisms of algebras, their properties, the

Boolean concept of filter and the Boolean ring quotient. When talking about applications of Boolean algebra, it is common to hear that Boolean algebras are the basis of digital information, and that they are a fundamental part of electronic circuits, because the operation of computers is based on the Boolean structure of the binary system. But, it is not natural to imagine that within living organisms one could make use of Boolean structures. This is how the study of logic gates ends and a model of the given genetic code is also briefly described in terms of Boolean algebras and $\mathbb{Z}_2^6$.

Keywords: Boolean homomorphism, Boolean isomorphism, Boolean algebra, Boolean ring, Boolean ideal, filters, Boolean quotient, logic circuits, lattice, and genetic code.

Introducción

El álgebra booleana o álgebra de Boole es la notación algebraica usada para el tratamiento de variables binarias. Cubre los estudios de toda variable que solo tenga 2 resultados posibles, complementarias y excluyentes entre sí. Por ejemplo, las variables cuya única posibilidad es verdadero o falso, correcto o incorrecto, encendido o apagado son el objeto de estudio del álgebra booleana.

El álgebra booleana fue introducida en 1854 por el matemático ingles George Boole (1815 - 1864), quien fue un autodidacta erudito de la época. Su inquietud surgió de una disputa existente entre Augustus De Morgan y William Hamilton, acerca de los parámetros que definen a este sistema lógico.

George Boole argumentó que la definición de los valores numéricos 0 y 1 corresponde, en el campo de la lógica, a la interpretación nada y universo respectivamente. La intención de George Boole fue definir, a través de las propiedades del álgebra, las expresiones de la lógica proposicional necesarias para tratar con variables de tipo binario.

El presente trabajo denominado **Homomorfismos entre álgebras booleanas** está enfocado en el análisis de las conexiones entre álgebras booleanas mediante homomorfismos y su estructura, para ello el trabajo se divide en tres capítulos los cuales se han planteado de la siguiente forma:

El Capítulo 1 denominado **Lógica proposicional** describe los operadores fundamentales del álgebra booleana, dando inicio con breves definiciones sobre la lógica proposicional las cuales son definición de proposición, operadores lógicos, tablas de verdad para operadores lógicos así como sus definiciones, definiciones sobre los cuantificadores, leyes de De Morgan, finalizando con definiciones y ejemplos de álgebra booleana.

En el Capítulo 2 denominado **Estructuras de álgebras booleanas** se pretende presentar las diferentes propiedades del álgebra boolena, así como analizar las conexiones entre álgebras boolenas mediante homomorfismos, para ello se estudiarán los ideales booleanos, ideales maximales booleanos, conceptos booleanos de filtros, homomorfismos de anillos booleanos y cociente de anillos booleanos.

En el Capítulo 3 denominado **Aplicaciones del álgebra booleana**, se estudian las compuertas lógicas que son de gran utilidad en los circuitos lógicos (o digitales), debido a que son la base de la electrónica digital moderna. Otra aplicación importante del álgebra booleana se encuentra en la genética, es por ello que se presenta un breve estudio del ARNm en términos del álgebra booleana y $\mathbb{Z}_2^6$.

Justificación

La investigación denominada " **Homomorfismos entre álgebras booleanas** " tiene como objetivo principal analizar las conexiones de las álgebras booleanas mediante homomorfismos así como su estructura.

En el desarrollo del tema se hace la presentación de estructuras booleanas como son anillos y álgebras booleanas, después de haber recordado algunas definiciones de lógica proposicional y propiedades conjuntistas llegando hasta estudiar los homomorfismos de álgebras booleanas.

Esta presentación de estructuras booleanas nos sirve para el estudio de homomorfismos booleanos ya que un homomorfismo booleano es un mapeo que preserva estructuras entre álgebras booleanas.

Los motivos que nos llevaron a investigar los "homomorfismos entre álgebras booleanas", se centran en que a través de los homomorfismos booleanos podemos conocer la estructura booleana, y además nos permite conocer diferentes casos que ocurren al mapear dos álgebras boolenas.

Este trabajo fue diseñado con la finalidad de que pueda ser de utilidad para los estudiantes, profesionales y aficionados que deseen conocer sobre el álgebra booleana.

Objetivos

Objetivo general: Analizar las conexiones entre álgebras booleanas mediante homomorfismos así como su estructura.

Objetivos específicos:

- Describir los operadores fundamentales del álgebra booleana (Simbología, expresiones matemáticas, tabla de verdad).
- Presentar las diferentes propiedades de las álgebras booleanas.
- Analizar las conexiones entre álgebras booleanas mediante homomorfismos.
- Implementar y simplificar circuitos lógicos empleando diferentes leyes del álgebra booleana y definiciones de De Morgan.
- Escribir la expresión booleana para las compuertas lógicas y las combinaciones de compuertas lógicas.
- Describir una reciente e ilustrativa representación de ARNm en términos del álgebra booleana y $\mathbb{Z}_2^6$.

Antecedentes

El álgebra de Boole se inventó en el año de 1854, por el matemático inglés George Boole. Primero declaró la idea del álgebra de Boole en su libro " Una investigación de las leyes del pensamiento". Después de esto, el álgebra de Boole es bien conocida como la forma perfecta para representar los circuitos lógicos digitales.

A fines del siglo XIX, los científicos Jevons, Schroder y Huntington utilizaron este concepto para términos modernos.

En la década de 1940, Claude Shannon en su tesis doctoral titulada "A Symbolic Analysis of Relay and Switching Circuits" logró establecer una relación entre las álgebras de Boole con los circuitos digitales, estableciendo así, la base de la electrónica digital moderna.

La síntesis lógica de las herramientas modernas de automatización electrónica se representa de manera eficiente mediante el uso de funciones booleanas conocidas como " Diagramas de decisión binario".

El álgebra de Boole permite sólo dos estados en un circuito lógico, como verdadero y falso, alto y bajo, sí y no, abierto y cerrado o 0 y 1.

En el 2007, el grupo de investigadores formado por R. Grau, M. Chavez, R. Sanchez, E. Morgado, G. Casas e I. Bonet construyeron un modelo matemático del código genético, basado en un álgebra de Boole particular, la cual facilita la comprensión de la lógica subyacente en el código genético. Más específicamente, este modelo refleja una fuerte conexión entre los ordenes del código genético y las propiedades físico-químicas de los aminoácidos.

Capítulo 1

Lógica Proposicional

En el presente capítulo se enuncian definiciones, ejemplos, teoremas, lemas, sobre lógica proposicional y álgebra booleana.

1.1. Proposición

Definición 1.1 *Una proposición p es una oración que tiene exactamente un valor de verdad: verdadero que denotamos con v, o un valor falso que denotamos con f.*

Tabla 1

Posibles valores de la proposición p.

$\boldsymbol{p}$
v
f

Ejemplo 1.1 *Las siguientes oraciones son proposiciones verdaderas:*

1. *Los números pares son divisibles por dos.*
2. *La capital de Rusia es Moscú.*

Ejemplo 1.2 *Las siguientes oraciones son proposiciones falsas:*

1. *4 es divisor de 15.*
2. *En el año 2019 Hitler era el presidente de los Estados Unidos.*

Ejemplo 1.3 *Las siguientes oraciones no son proposiciones:*

1. *¿Cómo te llamas?.*
2. *¡Estás muy guapa!.*

1.2. Operadores lógicos y sus tablas de verdad.

Los operadores lógicos contribuyen en la construcción del álgebra proposicional y las tablas de verdad son representaciones gráficas, en forma de arreglos, que sirven para analizar los posibles valores de verdad que puede tener una proposición. En general, para "n" proposiciones, se pueden presentar 2^n posibilidades.

Tabla 2

Operadores lógicos más recurrentes.

Operador lógico	**Símbolo**
Conjunción o conjuntor	$\wedge$
Disyunción o disyuntor	$\vee$
Condicional o implicador	$\longrightarrow$
Coimplicador o bicondicionador	$\longleftrightarrow$
Negador	$\neg$

A continuación se presentan las definiciones de los operadores lógicos y sus correspondientes tablas de verdad.

Definición 1.2 *La negación de una proposición p, denotada por $\neg p$, es la proposición "no p". La proposición $\neg p$ es verdadera exactamente cuando p es falso.*

Tabla 3

Valores de verdad correspondiente a la negación.

$\boldsymbol{p}$	$\boldsymbol{\neg p}$
v	f
f	v

A la izquierda se encuentran los dos valores de verdad posibles de p, con los correspondientes valores de verdad de $\neg p$ a la derecha.

Ejemplo 1.4 *Encontrar la negación de las siguientes oraciones:*

1. *Hay vida en el planeta Tierra.*

2. *Todos los jugadores de baloncesto son altos.*

3. $1 + 5 = 6$.

Solución:

1. No hay vida en el planeta Tierra.

2. Algunos jugadores de baloncesto no son altos.

3. $1 + 5 \neq 6$.

Definición 1.3 *Dadas dos proposiciones p y q, la conjunción de p y q denotada por $p \wedge q$, es la proposición "p y q". $p \wedge q$ es cierto exactamente cuando p y q son verdaderos.*

Tabla 4

Tabla correspondiente a la conjunción de p y q.

$\boldsymbol{p}$	$\boldsymbol{q}$	$\boldsymbol{p \wedge q}$
v	v	v
v	f	f
f	v	f
f	f	f

En las columnas p y q se enumeran las cuatro posibles combinaciones de valores de verdad para p y q, y en la columna de $p \wedge q$ se encuentra el valor de verdad asociada por $p \wedge q$.

Por ejemplo, las entradas de la tercera fila nos dicen que, si p es falsa y q es verdadera, entonces $p \wedge q$ es falsa. De hecho, la única manera de obtener una v en la columna de $p \wedge q$ es que sean verdaderas p y q, como se indica en la tabla de verdad.

Ejemplo 1.5 *Encontrar:*

1. $(p \wedge q)$ *donde, p: Hay vida en el planeta Tierra y q:No hay vida en Europa.*
2. $(p \wedge (\neg q))$ *donde, p: Aterrizó un hombre en la luna y q: El programa lunar tripulado está vivo.*
3. $((\neg p) \wedge (\neg q))$ *donde,* $p : 1 + 4 < 5$ *y* $q : 1 + 4 = 5$.

Solución:

1. $p \wedge q$: Hay vida en el planeta Tierra, pero no en Europa.
2. $p \wedge (\neg q)$: A pesar de que ha aterrizado al menos un hombre en la luna, el programa lunar tripulado está muerto.
3. $(\neg p) \wedge (\neg q) : 1 + 4 > 5$.

Definición 1.4 *Dadas dos proposiciones p y q, la disyunción de p y q denotada por* $p \vee q$*, es la proposición "p o q".* $p \vee q$ *es cierto exactamente cuando al menos p o q es verdadera.*

Tabla 5

Tabla correspondiente a la disyunción

$\boldsymbol{p}$	$\boldsymbol{q}$	$\boldsymbol{p \vee q}$
v	v	v
v	f	v
f	v	v
f	f	f

En las columnas p y q se enumeran las cuatro posibles combinaciones de valores de verdad para p y q, y en la columna de $p \vee q$ se encuentra el valor de verdad asociado por $p \vee q$. La única manera de obtener una f en la columna $p \vee q$ es que sean falsas p y q, tal como se indica en la tabla de verdad.

Ejemplo 1.6 *Encontrar:*

1. $(p \vee q)$ *donde, p: Hay vida en la Tierra, q: Todos los patos son negros.*

2. $(p \vee \neg q)$ *donde, p: Hay leones que son blancos y q: Todos los lobos son negros.*

3. $(p \vee q) \wedge (\neg p)$ *donde, p:* $x = y$ *y q:* $x < y$.

Solución:

1. $p \vee q$: Hay vida en la Tierra o, todos los patos son negros.

2. $p \vee (\neg q)$: Hay leones blancos o, existe al menos un lobo que no es negro.

3. $(p \vee q) \wedge (\neg p)$: $x < y$.

Definición 1.5 *Una tautología t es una forma proposicional que es verdadera para cada asignación de valores de verdad a sus componentes, mientras que una contradicción c es una forma proposicional que es falsa para cada asignación de valores de verdad a sus componentes.*

Ejemplo 1.7 *Probar que* $(p \vee q) \vee ((\neg p) \wedge (\neg q))$ *es una tautología.*

Prueba.

Para realizar la prueba se hace uso de las tablas de verdad para esta forma proposicional, conociendo la conjunción, disyunción y negación.

Tabla 6

Tabla de verdad para la proposición.

p	q	$p \vee q$	$\neg p$	$\neg q$	$(\neg p) \wedge (\neg q)$	$(p \vee q) \vee ((\neg p) \wedge (\neg q))$
v	v	v	f	f	f	v
f	v	v	v	f	f	v
v	f	v	f	v	f	v
f	f	f	v	v	v	v

Como en la última columna todos sus valores son verdaderos, entonces podemos concluir que es una tautología. ■

Definición 1.6 *Dos formas proposicionales son equivalentes si y sólo si, tienen las mismas tablas de verdad.*

Definición 1.7 *Para las proposiciones p y q, la condición $p \to q$ es la proposición "si p, entonces q". La proposición p es llamada el antecedente, o hipótesis, y q es llamada la consecuente, o conclusión. La oración condicional $p \to q$ es verdadera si y sólo si, p es falso o q es verdadero.*

Tabla 7

Tabla de verdad correspondiente al condicional de las proposiciones p y q.

$\boldsymbol{p}$	$\boldsymbol{q}$	$\boldsymbol{p \to q}$
v	v	v
f	v	v
v	f	f
f	f	v

En las columnas p y q se enumeran las cuatro posibles combinaciones de valores de verdad para p y q, y en la columna $p \to q$ se encuentra el valor de verdad asociado por $p \to q$. El condicional sólo es falso cuando el antecedente es verdadero y el consecuente es falso.

Ejemplo 1.8 *Conteste si la oración es verdadera o falsa.*

1. *Si* $1 + 1 = 3$, *entonces* $1 + 2 = 3$.

2. *Si la tierra es redonda, entonces marte es plano.*

3. *Si la tierra es redonda, marte es redondo.*

Solución:

1. Verdadero, dado que $1 + 1 = 3$ es falso pero $1 + 2 = 3$ es verdadero.

2. Falso, dado que es cierto que la tierra es redonda pero no es cierto que marte es plano.

3. Verdadero, dado que la tierra y marte son redondos.

Definición 1.8 *Sean p y q proposiciones.*

1. *El recíproco de $p \to q$ es $q \to p$.*

2. *El contrarrecíproco de $p \to q$ es $(\neg q) \to (\neg p)$.*

Teorema 1.1 *Para las proposiciones p y q:*

1. *$p \to q$ es equivalente a su contrarrecíproco $(\neg q) \to (\neg p)$.*

2. *$p \to q$ no es equivalente a su recíproco $q \to p$.*

Prueba.

La prueba se realiza haciendo uso de las tablas de verdad.

1. Probando que $p \longrightarrow q \equiv (\neg q) \longrightarrow (\neg p)$.

Tablo 8

Tabla de verdad correspondiente a la equivalencia del inciso 1.

$\boldsymbol{p}$	$\boldsymbol{q}$	$\boldsymbol{\neg p}$	$\boldsymbol{\neg q}$	$\boldsymbol{p \longrightarrow q}$	$\boldsymbol{(\neg q) \longrightarrow (\neg p)}$
v	v	f	f	v	v
v	f	f	v	f	f
f	v	v	f	v	v
f	f	v	v	v	v

Así, como los valores de la columna de $p \longrightarrow q$ son los mismos valores de la columna de $q \longrightarrow (\neg p)$, se puede concluir que $p \longrightarrow q \equiv (\neg q) \longrightarrow (\neg p)$.

2. Probando que $p \longrightarrow q$ no es equivalente a su recíproco.

Tabla 9

tabla de verdad correspondiente a la equivalencia del inciso 2.

p	q	$p \longrightarrow q$	$q \longrightarrow p$
v	v	v	v
v	f	f	v
f	v	v	f
f	f	v	v

Así, como los valores de la columna de $p \longrightarrow q$ no son los mismos de la columna de $q \longrightarrow p$, se puede concluir que $p \longrightarrow q$ no es equivalente a $q \longrightarrow p$. ■

Definición 1.9 *Para las proposiciones p y q, la oración bicondicional $p \leftrightarrow q$ es la proposición "p si y sólo si q", $p \leftrightarrow q$ es cierto exactamente cuando p y q tienen los mismos valores de verdad. También escribimos p si y sólo si q.*

Tabla 10

Tabla de verdad correspondiente al bicondicional para las proposiciones p y q.

p	q	$p \leftrightarrow q$
v	v	v
f	v	f
v	f	f
f	f	v

El bicondicional es verdadero sólo si ambas proposiciones poseen idénticos valores de verdad y es falso sólo si ambas proposiciones poseen diferentes valores de verdad.

Definición 1.10 *El álgebra de proposiciones es una cuádrupla $(A, \wedge, \vee, \neg)$ donde A es un conjunto de proposiciones formada por equivalencias lógicas, las cuales nos permiten simplificar un problema y expresarlo en forma más sencilla.*

Las principales leyes son las siguientes:

1. *Ley de no contradicción*

$$\neg(p \wedge \neg p) \equiv t.$$

   "Una proposición no puede ser falsa y verdadera a la vez ".

2. *Ley del tercio excluido*

$$(p \vee \neg p) \equiv t.$$

   "Una proposición o es verdadera o es falsa no existe una tercera posibilidad".

3. *Leyes de idempotencia*

$$p \vee p \equiv p,$$

$$p \wedge p \equiv p.$$

4. *Leyes conmutativas*

$$p \vee q \equiv q \vee p,$$

$$p \wedge q \equiv q \wedge p.$$

5. *Ley de la doble negación*

$$\neg(\neg p) \equiv p.$$

6. *Leyes asociativas*

$$(p \vee q) \vee r \equiv p \vee (q \vee r),$$

$$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r).$$

7. *Leyes distributivas*

$$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r),$$

$$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r).$$

8. *Leyes de identidad*

$$p \vee t \equiv t,$$

$$p \vee c \equiv p,$$

$$p \wedge t \equiv p,$$

$$p \wedge c \equiv c.$$

9. *Leyes del complemento*

$$p \vee \neg p \equiv t,$$

$$p \wedge \neg p \equiv c.$$

10. *Leyes de absorción*

$$p \wedge (p \vee q) \equiv p,$$

$$p \vee (p \wedge q) \equiv p,$$

$$p \wedge (\neg p \vee q) \equiv p \wedge q,$$

$$p \vee (\neg p \wedge q) \equiv p \vee q.$$

11. *Leyes de De Morgan*

$$\neg(p \vee q) \equiv (\neg p) \wedge (\neg q),$$

$$\neg(p \wedge q) \equiv (\neg p) \vee (\neg q).$$

Teorema 1.2 *Para las proposiciones p, q y r:*

1. *$p \to q$ es equivalente a $(\neg p) \vee q$.*

2. *$p \leftrightarrow q$ es equivalente a $(p \to q) \wedge (q \to p)$.*

3. *$\neg(p \to q)$ es equivalente a $p \wedge (\neg q)$.*

4. *$\neg(p \wedge q)$ es equivalente a $p \to (\neg q)$ y a $q \to (\neg p)$.*

5. *$p \to (q \to r)$ es equivalente a $(p \wedge q) \to r$.*

6. *$p \to (q \wedge r)$ es equivalente a $(p \to q) \wedge (p \to r)$.*

7. *$(p \vee q) \to r$ es equivalente a $(p \to r) \wedge (q \to r)$.*

Prueba.

1. Se probará que $p \to q \equiv (\neg p) \vee q$.

   Tabla 11

   Tabla correspondiente a la equivalencia del inciso 1.

$\boldsymbol{p}$	$\boldsymbol{q}$	$\boldsymbol{\neg p}$	$\boldsymbol{p \to q}$	$\boldsymbol{(\neg p) \vee q}$
v	v	f	v	v
v	f	f	f	f
f	v	v	v	v
f	f	v	v	v

   En la tabla de verdad se puede observar que las columnas $p \longrightarrow q$ y $(\neg p) \vee q$ tienen los mismos valores de verdad, entonces por 1.6 podemos concluir que $p \to q \equiv (\neg p) \vee q$.

2. Se probará que $p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$.

   Tabla 12

   Tabla de verdad correspondiente a la equivalencia del inciso 2.

$\boldsymbol{p}$	$\boldsymbol{q}$	$\boldsymbol{p \to q}$	$\boldsymbol{q \to p}$	$\boldsymbol{p \leftrightarrow q}$	$\boldsymbol{(p \to q) \wedge (q \to p)}$
v	v	v	v	v	v
v	f	f	v	f	f
f	v	v	f	f	f
f	f	v	v	v	v

En la tabla de verdad se puede observar que las columnas $p \leftrightarrow q$ y $(p \rightarrow q) \wedge (q \rightarrow p)$ tienen los mismos valores de verdad, entonces por 1.6 podemos concluir que:

$$p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p).$$

3. Se probará que $\neg(p \rightarrow q) \equiv p \wedge (\neg q)$.

Tabla 13

Tabla de verdad correspondiente a equivalencia del inciso 3.

$\boldsymbol{p}$	$\boldsymbol{q}$	$\boldsymbol{\neg q}$	$\boldsymbol{p \rightarrow q}$	$\boldsymbol{\neg(p \rightarrow q)}$	$\boldsymbol{p \wedge (\neg q)}$
v	v	f	v	f	f
v	f	v	f	v	v
f	v	f	v	f	f
f	f	v	v	f	f

En la tabla de verdad se puede observar que los valores de verdad correspondientes a la columna $\neg(p \rightarrow q)$ son iguales a los de la columna $p \wedge (\neg q)$, entonces por 1.6 podemos concluir que: $\neg(p \rightarrow q) \equiv p \wedge (\neg q)$.

4. Se probará que $\neg(p \wedge q) \equiv p \rightarrow (\neg q)$ y $\neg(p \wedge q) \equiv q \rightarrow (\neg p)$.

Tabla 14

Tabla de verdad correspondiente a la equivalencia del inciso 4.

$\boldsymbol{p}$	$\boldsymbol{q}$	$\boldsymbol{\neg p}$	$\boldsymbol{\neg q}$	$\boldsymbol{p \wedge q}$	$\boldsymbol{\neg(p \wedge q)}$	$\boldsymbol{p \rightarrow (\neg q)}$	$\boldsymbol{q \rightarrow (\neg p)}$
v	v	f	f	v	f	f	f
v	f	f	v	f	v	v	v
f	v	v	f	f	v	v	v
f	f	v	v	f	v	v	v

En la tabla de verdad que se realizó, se observa que las columnas $\neg(p \wedge q)$, $p \rightarrow (\neg q)$ y $q \rightarrow (\neg p)$ tienen los mismos valores de verdad, por lo cual, por 1.6 se puede concluir que:

$$\neg(p \wedge q) \equiv p \rightarrow (\neg q)$$

y

$$\neg(p \wedge q) \equiv q \rightarrow (\neg p).$$

5. Se probará que $p \rightarrow (q \rightarrow r) \equiv (p \wedge q) \rightarrow r$.

Tabla 15

Tabla de verdad correspondiente a la equivalencia del inciso 5.

$\boldsymbol{p}$	$\boldsymbol{q}$	$\boldsymbol{r}$	$\boldsymbol{p \wedge q}$	$\boldsymbol{q \rightarrow r}$	$\boldsymbol{(p \wedge q) \rightarrow r}$	$\boldsymbol{p \rightarrow (q \rightarrow r)}$
v	v	v	v	v	v	v
v	f	v	f	v	v	v
v	v	f	v	f	f	f
v	f	f	f	v	v	v
f	v	v	f	v	v	v
f	f	v	f	v	v	v
f	v	f	f	f	v	v
f	f	f	f	f	v	v

En la tabla de verdad que se realizó, se observa que las columnas $p \rightarrow (q \rightarrow r)$ y $(p \wedge q) \rightarrow r$ tienen los mismos valores de verdad, por lo cual, por 1.6 se puede concluir que:

$$p \rightarrow (q \rightarrow r) \equiv (p \wedge q) \rightarrow r.$$

6. Se probará que $p \to (q \wedge r) \equiv (p \to q) \wedge (p \to r)$.

Tabla 16

Tabla de verdad correspondiente a la equivalencia del inciso 6.

$\boldsymbol{p}$	$\boldsymbol{q}$	$\boldsymbol{r}$	$\boldsymbol{q \wedge r}$	$\boldsymbol{p \to q}$	$\boldsymbol{p \to r}$	$\boldsymbol{p \to (q \wedge r)}$	$\boldsymbol{(p \to q) \wedge (p \to r)}$
v	v	v	v	v	v	v	v
v	f	v	f	f	v	f	f
v	v	f	f	v	f	f	f
v	f	f	f	f	f	f	f
f	v	v	v	v	v	v	v
f	f	v	f	v	v	v	v
f	v	f	f	v	v	v	v
f	f	f	f	v	v	v	v

En la tabla de verdad se puede observar que los valores de verdad correspondientes a la columna $p \to (q \wedge r)$ son iguales a los de la columna $(p \to q) \wedge (p \to r)$, entonces por 1.6 podemos concluir que: $p \to (q \wedge r) \equiv (p \to q) \wedge (p \to r)$.

7. Se probará que $(p \vee q) \to r \equiv (p \to r) \wedge (q \to r)$.

Tabla 17

Tabla de verdad correspondiente a la equivalencia del inciso 7.

$\boldsymbol{p}$	$\boldsymbol{q}$	$\boldsymbol{r}$	$\boldsymbol{p \vee q}$	$\boldsymbol{p \to r}$	$\boldsymbol{q \to r}$	$\boldsymbol{(p \vee q) \to r}$	$\boldsymbol{(p \to r) \wedge (q \to r)}$
v	v	v	v	v	v	v	v
v	f	v	v	v	v	v	v
v	v	f	v	f	f	f	f
v	f	f	v	f	v	f	f
f	v	v	v	v	v	v	v
f	f	v	f	v	v	v	v
f	v	f	v	v	f	f	f
f	f	f	f	v	v	v	v

En la tabla de verdad se puede visualizar que los valores de verdad obtenidos en la columna $(p \vee q) \to r$ son los mismos valores obtenidos en la columna $(p \to r) \wedge (q \to r)$, entonces por 1.6 podemos concluir que:

$$(p \vee q) \to r \equiv (p \to r) \wedge (q \to r). \qquad \blacksquare$$

1.3. Cuantificadores

Cuando se habla de cuantificadores en la lógica, la teoría de conjuntos y las matemáticas en general, se hace referencia a aquellos símbolos utilizados en una proposición lógica para indicar "CUÁNTOS" elementos de un conjunto dado cumplen con cierta propiedad.

Los cuantificadores permiten la construcción de proposiciones a partir de funciones proposicionales, bien sea particularizando o generalizando. Por ejemplo, si consideramos la función proposicional:

$$P(x) : x \text{ es menor que dos.}$$

Esto podría particularizarse así: "Existe un número real que es menor que dos", o generalizarlo diciendo: "*Todos los números reales son menores que dos*".

Tabla 18

Tabla de los cuantificadores más utilizados

Cuantificador lógico	**Símbolo**
Universal	$\forall$
Existencial	$\exists$
Negación del universal	$\neg[\forall x \in A, P(x)] \equiv \exists x \in A \vert \neg P(x)$
Negación del existencial	$\neg[\exists x \in A / P(x)] \equiv \forall x \in A, \neg P(x)$

A continuación se dan unas definiciones sobre dichos cuantificadores lógicos.

Definición 1.11 *El cuantificador universal es la operación lógica que es verdadera cuando todos los valores de x, pertenecientes al conjunto con el cual se relaciona, son verdaderos. Se denota con el símbolo $\forall$ y se lee "para todo", y la expresión $\forall x$ se lee "para cada x", "todos los x".*

Ejemplo 1.9 *Sea* $A = \{1, 2, 3, 4, 5, 6\}$*. Determinar el valor de verdad de* $\forall x \in A,\ x^2 < 34$*.*

Solución:

Evaluamos $x^2 < 34$ para cada elemento de A.

Para $x = 1$.

$$1^2 < 34 \Longrightarrow 1 < 34..............(v)$$

Para $x = 2$.

$$2^2 < 34 \Longrightarrow 4 < 34..............(v)$$

Para $x = 3$.

$$3^2 < 34 \Longrightarrow 9 < 34..............(v)$$

Para $x = 4$.

$$4^2 < 34 \Longrightarrow 16 < 34..............(v)$$

Para $x = 5$.

$$5^2 < 34 \Longrightarrow 25 < 34..............(v)$$

Para $x = 6$.

$$6^2 < 34 \Longrightarrow 36 < 34..............(f)$$

La proposición $\forall x \in A,\ x^2 < 34$ es falsa, ya que no todos los elementos de A satisfacen la desigualdad.

Definición 1.12 *El cuantificador existencial es la operación lógica que es verdadera cuando al menos un valor de* x *pertenece al conjunto con el cual se relaciona, es verdadero. Se denota con el símbolo* $\exists$ *y se lee "existe", y la expresión* $\exists x$ *se lee "existe por lo menos un* x*", "hay un* x*" o "algunos* x*".*

Ejemplo 1.10 *Sea* $A = \{1, 2, 3, 4, 5, 6\}$*. Determinar el valor de verdad de:*

$$\exists x \in A \mid x^2 - x = 15.$$

Solución:

Evaluamos $x^2 - x = 15$ hasta encontrar un valor de A que satisfaga la igualdad.

Para $x = 1$.

$$1^2 - 1 = 1 - 1 = 0 \neq 15 .... (f)$$

Para $x = 2$.

$$2^2 - 2 = 4 - 2 = 2 \neq 15 .... (f)$$

Para $x = 3$.

$$3^2 - 3 = 9 - 3 = 6 \neq 15 .... (f)$$

Para $x = 4$.

$$4^2 - 4 = 16 - 4 = 12 \neq 15 .... (f)$$

Para $x = 5$.

$$5^2 - 5 = 25 - 5 = 20 \neq 15 .... (f)$$

Para $x = 6$.

$$6^2 - 6 = 36 - 6 = 30 \neq 15 .... (f)$$

La proposición es falsa, ya que no existe por lo menos un valor de A que haga verdadera la igualdad $x^2 - x = 15$.

Teorema 1.3 *La negación de los cuantificadores se realiza negando la función proposicional $P(x)$ y cambiando el cuantificador universal por el cuantificador existencial, o viceversa. Así:*

1. $\neg(\forall x)P(x)$ *es equivalente a* $(\exists x)(\neg P(x))$

2. $\neg(\exists x)P(x)$ *es equivalente a* $(\forall x)(\neg P(x))$

Prueba.

Para literal 1. Se quiere probar que $\neg(\forall x)P(x)$ es equivalente a $(\exists x)(\neg P(x))$, sea U el universo (El universo es el conjunto formado por todos los objetos de estudio en un contexto dado). La proposición $\neg(\forall x)P(x)$ es cierto en U.

$$\begin{aligned}\neg(\forall x)P(x) \text{ es verdadero en } U &\iff (\exists x)P(x) \text{ es falso en } U\\ &\iff (\exists x)(\neg P(x)) \text{ es verdadero en } U\end{aligned}$$

Para literal 2. Se quiere probar que $\neg(\exists x)P(x)$ es equivalente a $(\forall x)(\neg P(x))$, sea U el universo (El universo es el conjunto formado por todos los objetos de estudio en un contexto dado). La proposición $\neg(\exists x)P(x)$ es verdadera en U.

$$\begin{aligned}\neg(\exists x)P(x) \text{ es verdadero en } U &\iff (\forall x)P(x) \text{ es falso en } U\\ &\iff (\forall x)(\neg P(x)) \text{ es verdadero en } U\end{aligned}$$

■

Ejemplo 1.11 *Simbolizar y negar la siguiente proposición:*

"*Todos los números enteros son impares*".

Solución:

Sean el dominio $\mathbb{Z}$ y la función proposicional $P(x)$ tal que x es un número impar. Simbolizando mediante el cuantificador universal se tiene entonces que:

$$\forall x \in \mathbb{Z}, P(x).$$

Negando el cuantificador universal tenemos entonces que:

$$\neg[\forall x \in \mathbb{Z}, P(x)] \equiv \exists x \in \mathbb{Z} \mid \neg P(x).$$

Lo cual se lee como: Existe al menos un número entero x que no es impar.

Definición 1.13 *La proposición $(\exists! x)P(x)$ se lee "existe una x única tal que $P(x)$" y es cierto si y sólo si, el conjunto de verdad de $P(x)$ tiene exactamente un elemento. El símbolo $\exists!$ se llama el cuantificador existencial único.*

1.4. Conjuntos

Por un conjunto entendemos una colección de objetos. Los objetos individuales se llaman elementos del conjunto, si un conjunto tiene un número finito de elementos entonces se llama conjunto finito, en caso contrario se llama conjunto infinito.

Denotaremos usualmente a los conjuntos con letras mayúsculas y a sus elementos con letras minúsculas. Denotemos el hecho de que b sea un elemento del conjunto B por $b \in B$. La expresión "$b \in B$" se lee "b es un elemento de B", "b pertenece a B" o "b está en B".

Definición 1.14 *Un conjunto A es un subconjunto de un conjunto B, lo que se denota por $A \subset B$, si todo elemento de A es también un elemento de B. Véase Fig. 1.1.*

$A \subset B$ se lee a menudo "A está contenido en B".

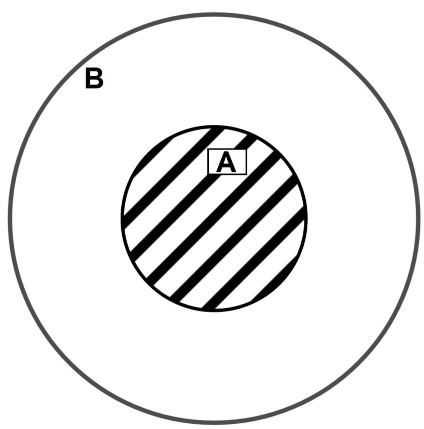


Figura 1.1: Ilustración de $A \subset B$.
Fuente: Creación propia en GeoGebra.

La definición de subconjunto implica que un conjunto es un conjunto de sí mismo. Por tanto, $A \subset A$ es siempre cierto. Los diagramas pueden ayudar a visualizar las relaciones entre conjuntos. Por ejemplo, en la figura 1.1, A es todo el interior del circulo pequeño y se ilustra la relación $A \subset B$.

Dos conjuntos son iguales si y sólo si son idénticos, es decir, si y sólo si ambos están compuestos de, exactamente, los mismos elementos. Así, $A = B$ si y sólo si $A \subset B$ y $B \subset A$.

Ejemplo 1.12 *Sea P el conjunto de los números pares: $P = \{2, 4, 6, 8, 10, \ldots\}$.*

El conjunto P está contenido en el conjunto de los números naturales $N = \{1, 2, 3, 4, 5, 6, \ldots\}$, dado que todos los elementos de P están incluidos en N. Está relación se expresa como $P \subset N$.

Definición 1.15 *La **intersección** de A y B, escrita $A \cap B$, es el conjunto de elementos que están en ambos A y B. Es decir, $x \in A \cap B$ si y sólo si $x \in A$ y $x \in B$. Véase Fig. 1.2.*

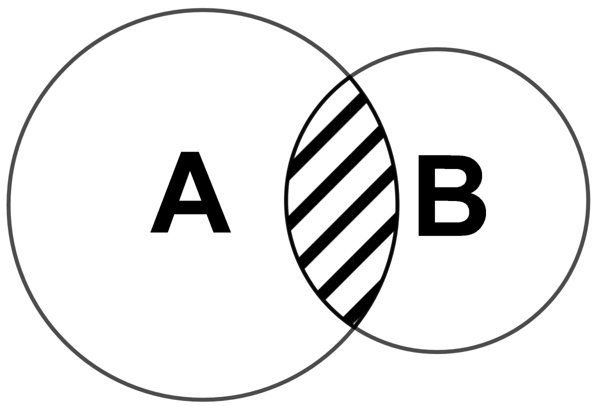


Figura 1.2: Ilustración de $A \cap B$.
Fuente: Creación propia en GeoGebra.

Ejemplo 1.13 *Ilustrar la intersección de los conjuntos:*

$$A = \{a, f, h, k, e, y, i, g, b, o, s, t, u\}, V = \{k, a, c, d, e, j, i, m, p, o, l, u, n\}.$$

Solución:

Se sabe por la definición que la intersección son todos aquellos elementos que ambos conjuntos A y V tengan en común, en otras palabras, son todos aquellos elementos que están tanto en A como en V, así, se tiene entonces que:

$$A \cap V = \{a, e, i, o, u\}.$$

Ahora, en la figura 1.3 se observa de manera ilustrativa dicha intersección.

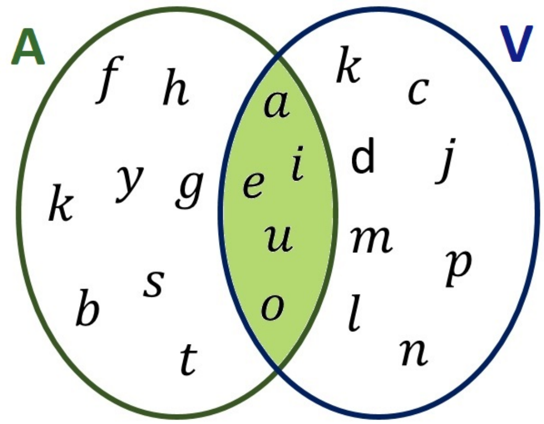


Figura 1.3: Intersección de los conjuntos A y V.
Fuente: Creación propia en Paint.

Definición 1.16 *La **unión** de A y B, escrita $A \cup B$, es el conjunto de elementos que están en A o en B. Es decir, $x \in A \cup B$ si y sólo si, $x \in A$ ó $x \in B$. Véase Fig. 1.4.*

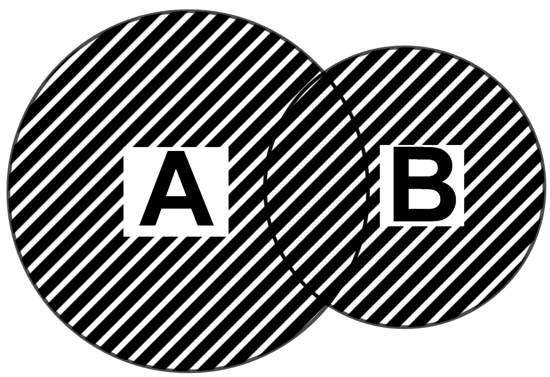


Figura 1.4: Ilustración de $A \cup B$.
Fuente: Creación propia en GeoGebra.

Ejemplo 1.14 *Ilustrar la unión de los conjuntos:*

$$Z = \{1, 2, 3, 4, 5, 6, 7, 8, 11\}, W = \{8, 12, 5, 13, 7, 9, 10\}.$$

Solución:

Se sabe por la definición que la unión son todos aquellos elementos que están en Z y W, así, se tiene entonces que:

$$Z \cup W = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13\}.$$

Ahora, en la figura se observa de manera ilustrativa dicha unión.

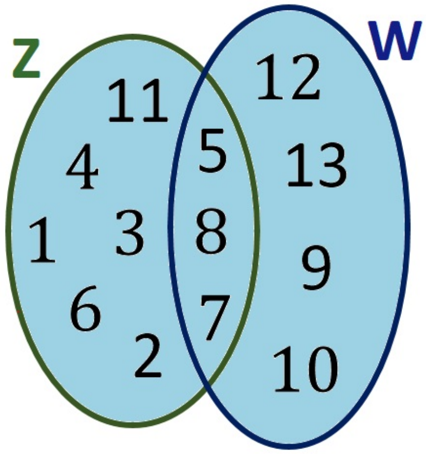


Figura 1.5: Unión de los conjuntos Z y W.
Fuente: Creación propia en Paint.

Definición 1.17 *La* ***diferencia*** *de A y B, escrita $A - B$, es el conjunto de elementos que están en A y no están en B. Es decir, $x \in A - B$ si y sólo si $x \in A$ y $x \notin B$. Véase Fig. 1.6.*

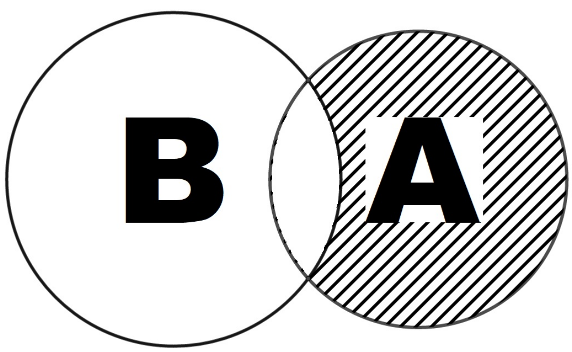


Figura 1.6: Ilustración de $A - B$.
Fuente: Creación propia en GeoGebra.

Ejemplo 1.15 *Sean los conjuntos $A = \{1, 2, 3, 5, 6\}$ y $B = \{2, 4, 6, 7, 8\}$. Encontrar $A - B$ y $B - A$.*

Solución:

1. Encontrando la diferencia de $A - B$.

   Por la definición de diferencia se tiene que, $A - B$ es el conjunto formado por todos aquellos elementos que están en A y que no están en B, lo cual será $A - B = \{1, 5, 3\}$, esto se observa en la figura 1.7.

2. Encontrando la diferencia de $B - A$.

   Por la definición de diferencia se tiene que, $B - A$ es el conjunto formado por todos aquellos elementos que están en B y que no están en A, lo cual será $B - A = \{4, 7, 8\}$, esto se observa en la figura 1.7.

En la siguiente ilustración se presentan los conjuntos A y B.

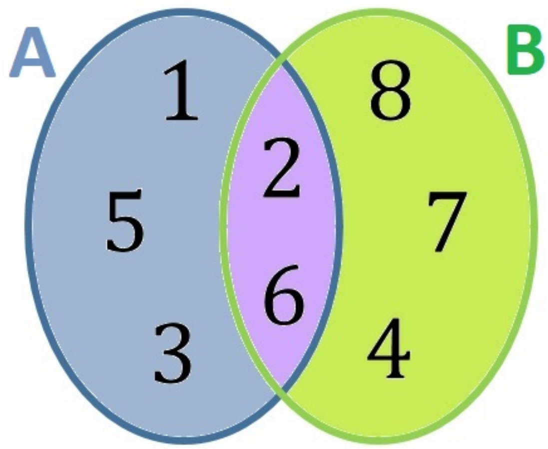


Figura 1.7: Ilustración de los conjuntos A y B.
Fuente: Creación propia en Paint.

Definición 1.18 *Los conjuntos A y B son disjuntos si y sólo si, $A \cap B = \emptyset$. Véase Fig. 1.8.*

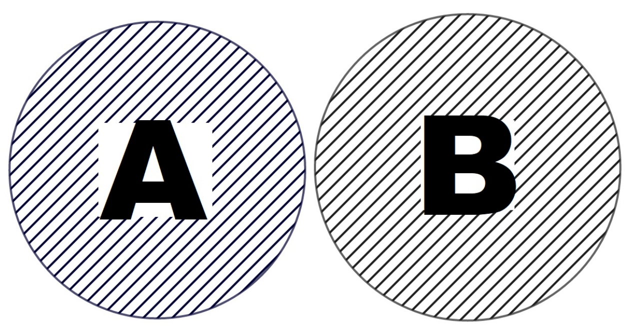


Figura 1.8: Ilustración de $A \cap B = \emptyset$.
Fuente: Creación propia en GeoGebra.

Ejemplo 1.16 *Sean $A = \{1, 3, 5, 7\}$ y $M = \{2, 4, 6, 8\}$, se tiene que $A \cap M = \emptyset$, pues no hay elementos en A que también estén en M. Véase 1.9.*

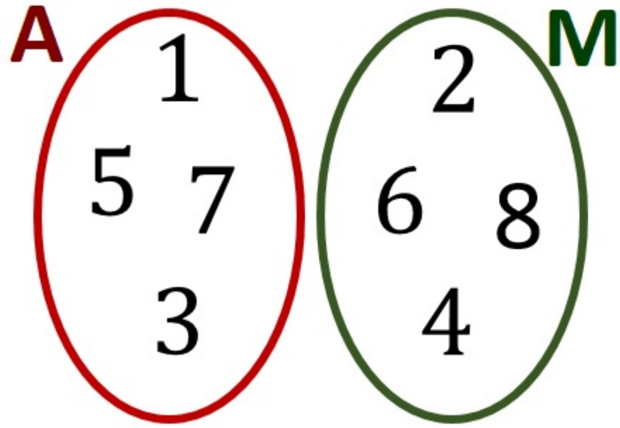


Figura 1.9: Ilustración de los conjuntos A y M.
Fuente: Creación propia en Paint.

Definición 1.19 *Sea U el universo y $A \subseteq U$. El complemento de A es $A^c = U - A$. Véase Fig. 1.10.*

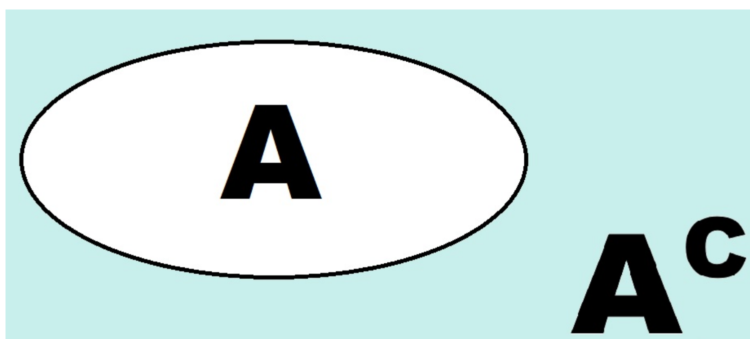


Figura 1.10: Ilustración de $A^C = U - A$.
Fuente: Creación propia en Paint.

Ejemplo 1.17 *Dados los conjuntos $A = \{7, 5, 9, 1, 15\}$ y $U = \{2, 7, 6, 1, 3, 15, 4, 9, 10, 5\}$. Encontrar A^C.*

Solución:

Por la definición de complemento se tiene que $A^C = U - A$, lo cual significa que A^C es lo que le falta al conjunto A para ser el conjunto universal U, entonces $A^C = \{2, 4, 6, 3, 10\}$.

En la Figura 1.11 se puede observar la representación de los conjuntos.

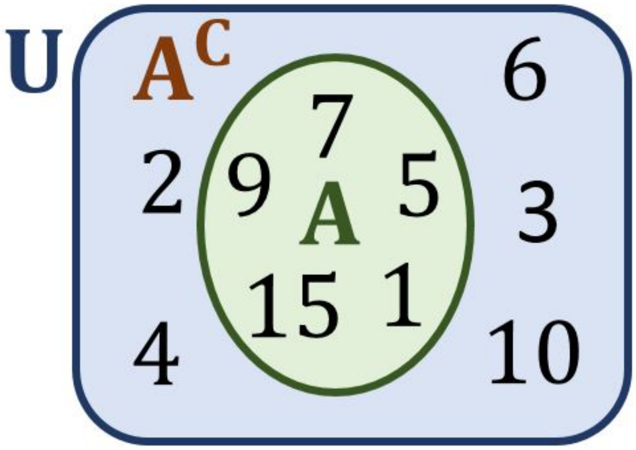


Figura 1.11: Ilustración de los conjuntos A y U.
Fuente: Creación propia en Paint.

Definición 1.20 *La diferencia simétrica de dos conjuntos A y B es el conjunto $A \triangle B$ cuyos elementos son todos los elementos de A o B, a excepción de los elementos comunes en ambos:*

$$x \in A \triangle B \text{ si y sólo si, o bien } x \in A \text{ o bien } x \in B.$$

Está diferencia simétrica se denota como:

$$A \triangle B = (A - B) \cup (B - A). \textit{Véase Fig. 1.12.}$$

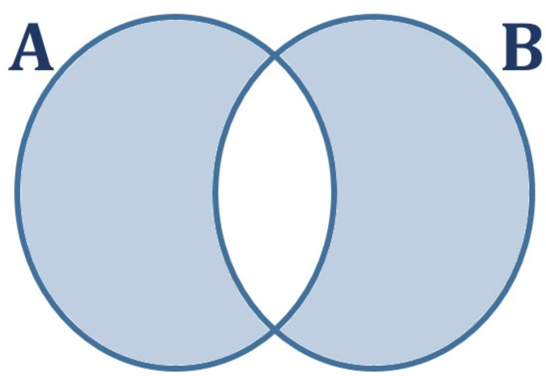


Figura 1.12: Ilustración de $A \triangle B$.
Fuente: Creación propia en Paint.

Teorema 1.4 *Sea U el universo, y sea A y B subconjuntos de U. Entonces se cumple:*

1. $(A^C)^C = A$.
2. $A \cup A^C = U$.
3. $A \cap A^C = \emptyset$.
4. $A - B = A \cap B^C$.
5. $(A \cup B)^C = A^C \cap B^C$.
6. $(A \cap B)^C = A^C \cup B^C$.

Prueba.

1. Se quiere probar que $(A^C)^C = A$.

   Sea $x \in (A^C)^C$.

$$\begin{aligned} x \in (A^C)^C &\Longleftrightarrow x \notin A^C \\ &\Longleftrightarrow x \in A \end{aligned}$$

   Así, $(A^C)^C = A$.

2. Se quiere probar que $A \cup A^C = U$.

   Sea $x \in A \cup A^C$.

$$\begin{aligned} x \in A \cup A^C &\Longleftrightarrow x \in A \vee x \in A^C \\ &\Longleftrightarrow x \in A \vee x \notin A \\ &\Longleftrightarrow x \in U \end{aligned}$$

   Así, $A \cup A^C = U$.

3. Se quiere probar que $A \cap A^C = \emptyset$.

$$\begin{aligned} A \cap A^C &= \{x \mid x \in A \wedge x \in A^C\} \\ &= \{x \mid x \in A \wedge x \notin A\} \\ &= \emptyset \end{aligned}$$

   Por lo que, $A \cap A^C = \emptyset$.

4. Se quiere probar que $A - B = A \cap B^C$.

   Sea $x \in A - B$.

$$\begin{aligned} x \in A - B &\Longleftrightarrow x \in A \wedge x \notin B \\ &\Longleftrightarrow x \in A \wedge x \in B^C \\ &\Longleftrightarrow x \in (A \cap B^C) \end{aligned}$$

   Así, $A - B = A \cap B^C$.

5. Se quiere probar que $(A \cup B)^C = A^C \cap B^C$.

   Sea $x \in (A \cup B)^C$.

$$\begin{aligned} x \in (A \cup B)^C &\Longleftrightarrow x \notin A \cup B \\ &\Longleftrightarrow x \notin A \wedge x \notin B \\ &\Longleftrightarrow x \in A^C \wedge x \in B^C \\ &\Longleftrightarrow x \in A^C \cap B^C \end{aligned}$$

   Así, $(A \cup B)^C = A^C \cap B^C$.

6. Se quiere probar que $(A \cap B)^C = A^C \cup B^C$.

   Sea $x \in (A \cap B)^C$.

$$\begin{aligned} x \in (A \cap B)^C &\Longleftrightarrow x \notin A \cap B \\ &\Longleftrightarrow x \notin A \vee x \notin B \\ &\Longleftrightarrow x \in A^C \vee x \in B^C \\ &\Longleftrightarrow x \in A^C \cup B^C \end{aligned}$$

   Así, $(A \cap B)^C = A^C \cup B^C$.

■

Definición 1.21 *El conjunto potencia de un conjunto X denotado por $\mathbb{P}(X)$ es el conjunto formado por todos los subconjuntos de A.*

Ejemplo 1.18 *Sea $X = \{a, b, c\}$. Encontrar $\mathbb{P}(X)$.*

Solución:

Los subconjuntos de X son: $\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}$. Entonces, el conjunto potencia de X es: $\mathbb{P}(X) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$.

1.5. Álgebra booleana

Definición 1.22 *Un conjunto no vacío de elementos A con dos operaciones binarias $(+)$, $(\cdot)$ se llama álgebra booleana si y sólo si valen los siguientes postulados:*

1. *Las operaciones $(+)$, $(\cdot)$ son conmutativas.*

2. *Existen en A elementos identidad 0 y 1 relativos a las operaciones $(+)$ y $(\cdot)$, respectivamente.*

3. *Cada operación es distributiva con respecto a la otra:*

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

$$a + (b \cdot c) = (a + b) \cdot (a + c)$$

4. *Para cada a en A existe un elemento a' en A, tal que $a + a' = 1$ y $a \cdot a' = 0$*

Denotaremos $a \cdot b$ por ab.

Teorema 1.5 *El álgebra de proposiciones es un álgebra booleana, con las operaciones binarias, $p + q := p \vee q$, $p \cdot q := p \wedge q$.*

Prueba.

Sean las operaciones binarias $p + q := p \vee q$, $p \cdot q := p \wedge q$, por Definición 1.10 se sigue de manera inmediata que las condiciones 1-3 se cumplen. Ahora, para la condición 4 se debe probar que:

$$\forall p \in A, \exists (\neg p) \in A,$$

tal que:

$$p \cdot (\neg p) = c$$

y

$$p \ + \ (\neg p) = t,$$

donde, el 0 de álgebra de proposiciones es c y el 1 es t, esto es cierto por Definición 1.10 inciso 8) y por la parte 9) de la Definición 1.10 las dos igualdades anteriores se cumplen. ■

Ejemplo 1.19 *Si X es un conjunto, entonces el conjunto de partes de X, notado con $\mathbb{P}(X)$, es un álgebra booleana, los elementos distinguidos se definen de la siguiente manera, $0 := \emptyset$, y $1 := X$, y si $A, B \in \mathbb{P}(X)$, entonces $A + B := A \cup B$ y $A \cdot B := A \cap B$. Más aún, el* *complemento de un elemento $A \in \mathbb{P}(X)$ coincide con el habitual complemento conjuntista $X \backslash A$.*

Prueba.

$\forall A, B, C \in \mathbb{P}(X)$ se tienen las siguientes propiedades las cuales son ciertas en teoría de conjuntos.

1.
$$A \cup B = B \cup A,$$
$$A \cap B = B \cap A.$$

2.
$$A \cap X = A,$$
$$A \cup \emptyset = A.$$

3.
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C),$$
$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$

4.
$$A \cap A^c = \emptyset,$$
$$A \cup A^c = X.$$

Luego, X es un álgebra booleana. ■

Definición 1.23 *Sean A un álgebra booleana y $p, q \in A$. Se llama sustracción de p y q a la operación definida de la manera siguiente:*

$$p - q := p \wedge q^{'}.$$

Definición 1.24 *Dados A álgebra booleana y $p, q \in A$. Llamaremos implicación y bicondicional a las operaciones definidas como sigue:*

$$p \Rightarrow q := p^{'} \vee q,$$

$$p \Leftrightarrow q := (p \Rightarrow q) \wedge (q \Rightarrow p).$$

1.6. Anillos booleanos

Definición 1.25 *Un anillo booleano es un séxtuplo $\boldsymbol{A} = (A, +, -, 0, \cdot, 1)$ tal que :*

1. $\forall x, y, z \in A$, $x + (y + z) = (x + y) + z$.
2. $\forall x \in A$, $x + 0 = x$ y $0 + x = x$.
3. $\forall x \in A$, $x + (-x) = 0$ y $(-x) + x = 0$.
4. $\forall x, y \in A$, $x + y = y + x$.
5. $\forall x, y, z \in A$, $x \cdot (y \cdot z) = (x \cdot y) \cdot z$.
6. $\forall x \in A$, $x \cdot 1 = x$ y $1 \cdot x = x$.
7. $\forall x, y, z \in A$,$x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ y $(y + z) \cdot x = (y \cdot x) + (z \cdot x)$.
8. $\forall x \in A$, $x \cdot x = x$.

Observaciones 1.1 *Un anillo booleano es un anillo con unitario en el cual cada elemento es idempotente, es decir $p^2 = p$.*

Ejemplo 1.20 *Un ejemplo trivial de anillo booleano es el anillo de los enteros módulo 2, es decir, $\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$, donde $\overline{0}, \overline{1}$ representan el elemento neutro y la identidad multiplicativa respectivamente.*

Prueba.

Es claro que todos sus elementos son idempotentes, ya que:

$$\overline{0}\cdot\overline{0}=\overline{0\cdot 0}=\overline{0},$$

$$\overline{1}\cdot\overline{1}=\overline{1\cdot 1}=\overline{1}.$$

Por lo tanto, $(\mathbb{Z}_2,+,\cdot)$ es un anillo booleano. ■

Ejemplo 1.21 *Si X es un conjunto cualquiera, entonces $R=\mathbb{P}(X)$ el conjunto de partes de X, (o conjunto potencia), es un anillo booleano, donde $0:=\emptyset$, y $1:=X$, y si $A,B\in R$, entonces $A+B:=A\bigtriangleup B=(A-B)\cup(B-A)$ (La diferencia simétrica), y $A\cdot B:=A\cap B$.*

Prueba.

1. Probemos que $A\bigtriangleup(B\bigtriangleup C)=(A\bigtriangleup B)\bigtriangleup C$

   Sea $A,B,C\in R$,

$$\begin{aligned}
A\bigtriangleup(B\bigtriangleup C)&=(A-(B\bigtriangleup C))\cup((B\bigtriangleup C)-A)\\
&=[A-((B-C)\cup(C-B))]\cup[((B-C)\cup(C-B))-A]\\
&=[A\cap((B\cap C^C)\cup(C\cap B^C))^C]\cup[((B\cap C^C)\cup(C\cap B^C))\cap A^C]\\
&=[A\cap(B^C\cup C)\cap(C^C\cup B)]\cup[((B\cap C^C)\cup(C\cap B^C))\cap A^C]\\
&=(A\cap B^C\cap C^C)\cup(A\cap B\cap C)\cup(A^C\cap B\cap C^C)\cup(A^C\cap B^C\cap C)\\
&=(A\cap B^C\cap C^C)\cup(A^C\cap B\cap C^C)\cup(A^C\cap B^C\cap C)\cup(A\cap B\cap C)\\
&=[((A\cap B^C)\cup(B\cap A^C))\cap C^C]\cup[C\cap((A^C\cup B)\cap(B^C\cup A))]\\
&=[((A-B)\cup(B-A))\cap C^C]\cup[C\cap((A-B)\cup(B-A))^C]\\
&=[((A-B)\cup(B-A))-C]\cup[C-((A-B)\cup(B-A))]\\
&=((A\bigtriangleup B)-C)\cup(C-(A\bigtriangleup B))\\
&=(A\bigtriangleup B)\bigtriangleup C.
\end{aligned}$$

2. Probemos que $A \triangle \emptyset = A$ y $\emptyset \triangle A = A$

   Probaremos únicamente que $A \triangle \emptyset = A$ ya que la otra parte se demuestra de manera análoga.

   Sea $A \in R$ y $x \in A \triangle \emptyset$

$$\begin{aligned} x \in A \triangle \emptyset &\iff x \in (A - \emptyset) \cup (\emptyset - A) \\ &\iff x \in (A \cap \emptyset^C) \cup (\emptyset \cap A^C) \\ &\iff x \in A \cup \emptyset \\ &\iff x \in A. \end{aligned}$$

3. Probemos la existencia del inverso.

   Sea $A \in R$ y sea $A \triangle B = \emptyset$.

$$\begin{aligned} A \triangle B = \emptyset &\implies (A - B) \cup (B - A) = \emptyset \\ &\implies A - B = \emptyset \wedge B - A = \emptyset \\ &\implies A \subset B \wedge B \subset A \\ &\implies B = A. \end{aligned}$$

   Por lo cual, el inverso de A es A entonces $A \triangle A = \emptyset$.

4. Probemos que $A \triangle B = B \triangle A$

   Sea $A, B \in R$ y sea $x \in A \triangle B$.

$$\begin{aligned} x \in A \triangle B &\iff x \in (A - B) \cup (B - A) \\ &\iff x \in (A \cap B^C) \cup (B \cap A^C) \\ &\iff x \in (B \cap A^C) \cup (A \cap B^C) \\ &\iff x \in (B - A) \cup (A - B) \\ &\iff x \in B \triangle A. \end{aligned}$$

5. Probemos que $A \cap (B \cap C) = (A \cap B) \cap C$

   Sea $A, B, C \in R$ y sea $x \in A \cap (B \cap C)$.

$$\begin{aligned} x \in A \cap (B \cap C) &\Longleftrightarrow x \in A \wedge x \in (B \cap C) \\ &\Longleftrightarrow x \in A \wedge x \in B \wedge x \in C \\ &\Longleftrightarrow x \in (A \cap B) \wedge x \in C \\ &\Longleftrightarrow x \in (A \cap B) \cap C. \end{aligned}$$

6. Sea $A \in R$

   Es claro que $A \cap X = A$.

7. Probemos que $A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$

   Sea $A, B, C \in R$

$$\begin{aligned} (A \cap B) \triangle (A \cap C) &= ((A \cap B) - (A \cap C)) \cup ((A \cap C) - (A \cap B)) \\ &= ((A \cap B) \cap (A \cap C)^C) \cup ((A \cap C) \cap (A \cap B)^C) \\ &= ((A \cap B) \cap (A^C \cup C^C)) \cup ((A \cap C) \cap (A^C \cup B^C)) \\ &= (((A \cap B) \cap A^C) \cup ((A \cap B) \cap C^C)) \cup \\ &\quad (((A \cap C) \cap A^C) \cup ((A \cap C) \cap B^C)) \\ &= ((A \cap A^C) \cap B) \cup ((A \cap B) \cap C^C) \cup \\ &\quad (((A \cap A^C) \cap C) \cup ((A \cap C) \cap B^C)) \\ &= (\emptyset \cap B) \cup ((A \cap B) \cap C^C) \cup ((\emptyset \cap C) \cup ((A \cap C) \cap B^C)) \\ &= ((A \cap B) \cap C^C) \cup ((A \cap C) \cap B^C) \\ &= (A \cap (B \cap C^C)) \cup (A \cap (C \cap B^C)) \\ &= A \cap ((B \cap C^C) \cup (C \cap B^C)) \\ &= A \cap ((B - C) \cup (C - B)) \\ &= A \cap (B \triangle C). \end{aligned}$$

8. Sea $A \in R$.

   Se cumple que $A \cap A = A$.

Así, se concluye que R es un anillo booleano. ■

La idempotencia en la definición de anillo booleano tiene gran influencia en su estructura.

Proposición 1.1 *Sea A un anillo booleano:*

1. *A es un anillo conmutativo.*

2. *A tiene característica 2 (i.e. $x + x = 0$, $\forall\ x \in A$)*

Para demostrar esta proposición, necesitaremos el siguiente lema que anunciamos y probamos a continuación.

Lema 1.1 *Sea A un anillo booleano y sea $a, b \in A$, entonces $ab = -ba$*

Prueba.

Por ser A un anillo booleano, para cualquier para de elementos $a, b \in A$, se cumple que $(a + b)^2 = a + b$ y $(ab)^2 = ab$.

Por otra parte, aplicando la propiedad distributiva del producto con respecto de la suma, se obtiene.

$$
\begin{aligned}
(a+b)^2 &= a+b \\
(a+b)(a+b) &= a+b \\
a^2+ab+ba+b^2 &= a+b \\
a+ab+ba+b &= a+b \\
ab+ba &= 0 \\
ab &= -ba.
\end{aligned}
$$

■

Ahora, procedemos a demostrar la proposición, haciendo uso del lema 1.1.

1. A es un anillo conmutativo.

   Prueba.

   Por los axiomas de anillo booleano se tiene que A es un anillo booleano ahora solo falta demostrar la conmutatividad del producto para que A sea un anillo conmutativo. Usando el lema 1.1 se tiene que:

$$\begin{aligned}(ab)^2 &= ab\\(ab)(ab) &= ab\\(-ba)(-ba) &= ab\\(ba)(ba) &= ab\\(ba)^2 &= ab\\ba &= ab.\end{aligned}$$

   Por lo que, $ab = ba$ para todo $a, b \in A$ y así A es un anillo conmutativo. ■

2. A tiene característica 2 (i.e. $x + x = 0$, $\forall\ x \in A$).

   Prueba.

   Dado cualquier $x \in A$, por ser A booleano, se tiene que $(x + x)^2 = x + x$.

   Puesto que

$$(x + x)^2 = (x + x)(x + x) = x^2 + x^2 + x^2 + x^2 = (x + x) + (x + x).$$

   Se tiene

$$(x + x) + (x + x) = (x + x).$$

   Por lo tanto, $x + x$ es idempotente con respecto de la suma y, puesto que $(A, +)$ es un grupo, $x + x = 0$. ■

Definición 1.26 *En cada anillo booleano $(A, +, \cdot)$ podemos introducir operaciones similares a las usadas en teoría de conjuntos, las cuales serán definidas de la siguiente forma:*

$$p \wedge q := p \cdot q, \tag{1.1}$$

$$p \vee q := p + q + (p \cdot q), \tag{1.2}$$

$$p^{'} := 1 + p. \tag{1.3}$$

tales operaciones son llamadas conjunción, disyunción y complementación.

Proposición 1.2 *La suma y el producto de un anillo booleano A pueden ser expresadas en términos de la conjunción, la disyunción y la complementación así como se muestra en las ecuaciones 1.1, 1.2 y 1.3. Dicho en otras palabras, si $p, q \in A$ entonces se cumple que:*

$$p \cdot q = p \wedge q, \tag{1.4}$$

$$p + q = (p \wedge q') \vee (p' \wedge q). \tag{1.5}$$

Prueba.

Primero probamos que $p \cdot q = p \wedge q$, pero tenemos que esto es consecuencia inmediata de la definición 1.26. Ahora, para probar que $p + q = (p \wedge q^{'}) \vee (p^{'} \wedge q)$ es suficiente desarrollar el lado derecho de la misma como sigue:

$$\begin{aligned}
(p \wedge q^{'}) \vee (p^{'} \wedge q) &= (p \cdot q^{'}) \vee (p^{'} \cdot q) \\
&= (p \cdot q^{'}) + (p^{'} \cdot q) + (p \cdot q^{'}) \cdot (p^{'} \cdot q) \\
&= (p \cdot (1 + q)) + ((1 + p) \cdot q) + (p \cdot (1 + q)) \cdot ((1 + p) \cdot q) \\
&= p + (p \cdot q) + q + (p \cdot q) + (p + (p \cdot q)) \cdot (q + (p \cdot q)) \\
&= p + q + 3(p \cdot q) + (p^2 \cdot q) + (p \cdot q^2) + (p \cdot q)^2 \\
&= p + q + 3(p \cdot q) + (p \cdot q) + (p \cdot q) + (p \cdot q) \\
&= p + q + 6(p \cdot q) \\
&= p + q + 3[(p \cdot q) + (p \cdot q)] \\
&= p + q.
\end{aligned}$$

La última igualdad se deduce del hecho de que $(p \cdot q) + (p \cdot q) = 0$ como consecuencia de la parte 2) de la proposición 1.1. ■

Teorema 1.6 *(Teorema de conexión). Cualquier anillo booleano es un álgebra booleana, y viceversa, toda álgebra booleana es un anillo booleano. Más precisamente:*

i) Si $(A, +, \cdot)$ es un anillo booleano, entonces definiendo las operaciones conjunción, disyunción y complementación sobre A a partir de las ecuaciones (1.1), (1.2), (1.3), respectivamente, tenemos que $(A, \wedge, \vee, ')$ es un álgebra booleana.

ii) Si $(A, \wedge, \vee, ')$ es un álgebra booleana, entonces definiendo las operaciones de producto y suma sobre A por medio de las siguientes identidades:

$$p \cdot q := p \wedge q, \tag{1.6}$$

$$p + q := (p \wedge q') \vee (p' \wedge q). \tag{1.7}$$

Con $p, q \in A$, tenemos que $(A, +, \cdot)$ es un anillo booleano.

Prueba.

i) Sea $(A, +, \cdot)$ un anillo booleano. Definamos las operaciones conjunción, disyunción y complementación sobre A a partir de las ecuaciones (1.1), (1.2), (1.3) y mostraremos los axiomas que satisface un álgebra booleana.

   a) Mostraremos que $\vee, \wedge$ son conmutativas.

   Sea $p, q \in A$.

$$\begin{aligned} p \vee q &= p + q + (p \cdot q) & \qquad p \wedge q &= p \cdot q \\ &= q + p + (q \cdot p) & &= q \cdot p \\ &= q \vee p & &= p \wedge p \end{aligned}$$

   Por lo tanto, $\vee, \wedge$ son conmutativas.

b) Mostraremos que existen en A identidades relativas a las operaciones $\vee, \wedge$.

Sea $p \in A$.

$$\begin{aligned} p \vee 1 &= p + 1 + (p \cdot 1) \\ &= p + 1 + p \\ &= 1 + p + p \\ &= 1 \end{aligned} \qquad \begin{aligned} p \wedge 0 &= p \cdot 0 \\ &= 0 \end{aligned}$$

Así, 1 y 0 son las identidades relativas a las operaciones $\vee, \wedge$ respectivamente.

c) Sea $p, q, r \in A$.

Se probará que $p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r)$. Así,

$$\begin{aligned} p \wedge (q \vee r) &= p \cdot (q + r + (q \cdot r)) \\ &= p \cdot q + p \cdot r + p \cdot (q \cdot r) \\ &= p \cdot q + p \cdot r + p^2 \cdot (q \cdot r) \\ &= p \cdot q + p \cdot r + (p \cdot q) \cdot (p \cdot r) \\ &= (p \cdot q) \vee (p \cdot r) \\ &= (p \wedge q) \vee (p \wedge r). \end{aligned}$$

Por lo tanto, $p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r)$.

Ahora, se probará que $p \vee (q \wedge r) = (p \vee q) \wedge (p \vee r)$. Así,

$$\begin{aligned} p \vee (q \wedge r) &= p \vee (q \cdot r) \\ &= p + (q \cdot r) + p \cdot (q \cdot r) \\ &= p + (p \cdot r) + (p \cdot r) + (p \cdot q) + (p \cdot q) + (q \cdot r) + p \cdot (q \cdot r) + \\ &\quad + r \cdot (p \cdot q) + r \cdot (p \cdot q) \\ &= (p + q + (p \cdot q)) \cdot (p + r + (p \cdot r)) \\ &= (p \vee q) \wedge (p \vee r). \end{aligned}$$

Por lo tanto, $p \vee (q \wedge r) = (p \vee q) \wedge (p \vee r)$.

d) Sea $p \in A$.

Probaremos que $\exists p^{'} \in A$ tal que $p \vee p^{'} = 1$ y $p \wedge p^{'} = 0$.

$$\begin{aligned} p \vee p^{'} &= p + p^{'} + (p \cdot p^{'}) \\ &= p + 1 + p + p + p \\ &= 1 + p + p + p + p \\ &= 1 \end{aligned} \qquad\qquad \begin{aligned} p \wedge p^{'} &= p \cdot p^{'} \\ &= p + p \\ &= 0 \end{aligned}$$

Por lo tanto, $\exists p^{'} \in A$ tal que $p \vee p^{'} = 1$ y $p \wedge p^{'} = 0$.

Por lo tanto, $(A, \wedge, \vee, ')$ es un álgebra booleana.

ii) Sea $(A, \wedge, \vee, ')$ un álgebra booleana.

Consideremos el producto y la suma definida sobre A por medio de 1.4 y 1.5 respectivamente. Entonces veamos que A tiene estructura de anillo booleano con estas operaciones.

En primer lugar, es claro que A es cerrado bajo las operaciones 1.4 y 1.5, luego probaremos los axiomas que cumple un anillo booleano.

a) Sea $x, y, z \in A$,

$$\begin{aligned} x + (y + z) &= \Big(x \wedge (y+z)^{'}\Big) \vee \Big(x^{'} \wedge (y+z)\Big) \\ &= \Big(x \wedge \Big[\Big(y^{'} \vee z\Big) \wedge \Big(y \vee z^{'}\Big)\Big]\Big) \vee \Big(x^{'} \wedge \Big[\Big(y \wedge z^{'}\Big) \vee \Big(y^{'} \wedge z\Big)\Big]\Big) \\ &= \Big(\Big(x \wedge \Big(y^{'} \vee z\Big)\Big) \wedge \Big(y \vee z^{'}\Big)\Big) \vee \Big(\Big(x^{'} \wedge \Big(y \wedge z^{'}\Big)\Big) \vee \Big(x^{'} \wedge (y^{'} \wedge z)\Big)\Big) \\ &= \Big(\Big[\Big(x \wedge y^{'}\Big) \vee (x \wedge z)\Big] \wedge \Big(y \vee z^{'}\Big)\Big) \vee \Big(\Big(\Big(x^{'} \wedge y\Big) \wedge z^{'}\Big) \vee \Big(\Big(x^{'} \wedge y^{'}\Big) \wedge z\Big)\Big) \end{aligned}$$

$$
\begin{aligned}
&= \left(\left[\left(x \wedge y^{'}\right) \wedge \left(y \vee z^{'}\right)\right] \vee \left[(x \wedge z) \wedge \left(y \vee z^{'}\right)\right]\right) \vee \left(\left[\left(x^{'} \wedge y\right) \wedge z^{'}\right] \vee \left[\left(x^{'} \wedge y^{'}\right) \wedge z\right]\right)\\
&= \left(\left(x \wedge y^{'}\right) \wedge \left(y \vee z^{'}\right) \vee \left(\left(x^{'} \wedge y\right) \wedge z^{'}\right)\right) \vee \left(\left((x \wedge z) \wedge \left(y \vee z^{'}\right)\right) \vee \left((x^{'} \wedge y^{'}) \wedge z\right)\right)\\
&= \left(\left(\left(x \wedge y^{'}\right) \wedge y\right) \vee \left(\left(x \wedge y^{'}\right) \wedge z^{'}\right) \vee \left(\left(x^{'} \wedge y\right) \wedge z^{'}\right)\right) \vee\\
&\quad \left(((x \wedge z) \wedge y) \vee \left((x \wedge z) \wedge z^{'}\right) \vee \left(\left(x^{'} \wedge y^{'}\right) \wedge z\right)\right)\\
&= \left(\left(\left(x \wedge y^{'}\right) \wedge z^{'}\right) \vee \left(\left(x^{'} \wedge y\right) \wedge z^{'}\right)\right) \vee \left(((x \wedge z) \wedge y) \vee \left(\left(x^{'} \wedge y^{'}\right) \wedge z\right)\right)\\
&= \left(\left[\left(x \wedge y^{'}\right) \vee \left(x^{'} \wedge y\right)\right] \wedge z^{'}\right) \vee \left(((x \wedge y) \wedge z) \vee \left(\left(x^{'} \wedge y^{'}\right) \wedge z\right)\right)\\
&= \left(\left[\left(x \wedge y^{'}\right) \vee \left(x^{'} \wedge y\right)\right] \wedge z^{'}\right) \vee \left(\left((x \wedge y) \vee \left(x^{'} \wedge y^{'}\right)\right) \wedge z\right)\\
&= \left(\left[\left(x \wedge y^{'}\right) \vee \left(x^{'} \wedge y\right)\right] \wedge z^{'}\right) \vee \left(\left(\left((x \wedge y) \vee x^{'}\right) \wedge \left((x \wedge y) \vee y^{'}\right)\right) \wedge z\right)\\
&= \left(\left[\left(x \wedge y^{'}\right) \vee \left(x^{'} \wedge y\right)\right] \wedge z^{'}\right) \vee \left(\left(\left[\left(x \vee x^{'}\right) \wedge \left(y \vee x^{'}\right)\right] \wedge\right.\right.\\
&\quad \left.\left.\left[\left(x \vee y^{'}\right) \wedge \left(y \vee y^{'}\right)\right]\right) \wedge z\right)\\
&= \left(\left[\left(x \wedge y^{'}\right) \vee \left(x^{'} \wedge y\right)\right] \wedge z^{'}\right) \vee \left(\left[\left(y \vee x^{'}\right) \wedge \left(x \vee y^{'}\right)\right] \wedge z\right)\\
&= \left(\left[\left(x \wedge y^{'}\right) \vee \left(x^{'} \wedge y\right)\right] \wedge z^{'}\right) \vee \left(\left(\left(x \wedge y^{'}\right) \vee \left(x^{'} \wedge y\right)\right)^{'} \wedge z\right)\\
&= (x + y) + z
\end{aligned}
$$

b) Sea $p \in A$,

$$
\begin{aligned}
p + 0 &= (p \wedge 0^{'}) \vee (p^{'} \wedge 0)\\
&= (p \cdot 1) \vee (p^{'} \cdot 0)\\
&= p \vee 0\\
&= p.
\end{aligned}
$$

c) Sea $p, q \in A$. Queremos probar que $p + (-p) = 0$.
Sea $q = -p$ tal que, $p + q = 0$

$$\begin{aligned} p + q = 0 &\Longrightarrow (p \wedge q^{'}) \vee (p^{'} \wedge q) = 0 \\ &\Longrightarrow p \wedge q^{'} = 0 \ y \ p^{'} \wedge q = 0 \\ &\Longrightarrow q = p. \end{aligned}$$

Comprobando que $p = q$

$$\begin{aligned} p + p &= (p \wedge p^{'}) \vee (p^{'} \wedge p) \\ &= 0 \vee 0 \\ &= 0. \end{aligned}$$

Por lo tanto $p = -p$.

d) Sea $p, q \in A$,

$$\begin{aligned} p + q &= (p \wedge q^{'}) \vee (p^{'} \wedge q) \\ &= (p^{'} \wedge q) \vee (p \wedge q^{'}) \\ &= (q \wedge p^{'}) \vee (q^{'} \wedge p) \\ &= q + p. \end{aligned}$$

e) Sea $p, q, r \in A$,

$$\begin{aligned} p \cdot (q \cdot r) &= p \wedge (q \wedge r) \\ &= (p \wedge q) \wedge r \\ &= (p \cdot q) \cdot r. \end{aligned}$$

f) Sea $p \in A$,

$$\begin{aligned} p \cdot 1 &= (p \wedge 1) \\ &= p. \end{aligned}$$

g) Sea $p, q, r \in A$,

$$\begin{aligned} (p \cdot q) + (p \cdot r) &= \Big[(p \wedge q) \wedge (p \wedge r)^{'}\Big] \vee \Big[(p \wedge q)^{'} \wedge (p \wedge r)\Big] \\ &= \Big[(p \wedge q) \wedge (p^{'} \vee r^{'})\Big] \vee \Big[(p^{'} \vee q^{'}) \wedge (p \wedge r)\Big] \\ &= \Big[((p \wedge q) \wedge p^{'}) \vee ((p \wedge q) \wedge r^{'})\Big] \vee \Big[(p^{'} \wedge (p \wedge r)) \vee (q^{'} \wedge (p \wedge r))\Big] \\ &= \Big[p \wedge (q \wedge r^{'})\Big] \vee \Big[p \wedge (q^{'} \wedge r)\Big] \\ &= p \wedge \Big[(q \wedge r^{'}) \vee (q^{'} \wedge r)\Big] \\ &= p \cdot (q + r). \end{aligned}$$

Por lo tanto, $p \cdot (q + r) = (p \cdot q) + (p \cdot r)$

h) Sea $p \in A$,

$$\begin{aligned} p \cdot p &= p \wedge p \\ &= p. \end{aligned}$$

Por lo tanto, $(A, \wedge, \vee, ')$ es un anillo booleano.

Por lo tanto, toda álgebra booleana es un anillo booleano y viceversa, todo anillo booleano es un álgebra booleana. ■

1.7. Campos de subconjuntos

Formar $P(X)$ no es la única forma natural de hacer un álgebra booleana a partir de un conjunto X no vacío, Una forma más general la presentamos en la siguiente definición.

Definición 1.27 *Sea A una subclase arbitraria no vacía de $P(X)$ que está cerrado bajo unión y complemento, es decir, si P y Q están en A, entonces también lo están $P \cup Q$ y $P^{'}$. Como A contiene al menos un elemento, se sigue que A contiene $\emptyset$ y X. Y por lo tanto A es un álgebra booleana. Cada álgebra booleana obtenida de esta manera se llama campo de conjuntos.*

Normalmente no hay peligro en denotar un campo de conjuntos por el mismo símbolo que la clase de conjuntos que lo componen. Sin embargo, esto no justifica la conclusión de que la intersección, la unión y el complemento de la teoría de conjuntos sean las únicas operaciones posibles que convierten una clase de conjuntos en un álgebra booleana.

Para mostrar que una clase A de subconjuntos de un conjunto X es un campo, basta mostrar que A es no vacío y está cerrado bajo unión y complemento. De echo, si A está cerrado bajo estas dos operaciones, entonces también debe estar cerrado bajo intersección, ya que

$$P \cap Q = (P^{'} \cup Q^{'})^{'}.$$

Para dos subconjuntos cualesquiera P y Q de X. Dualmente, A es un campo siempre que sea no vacío y esté cerrado bajo intersección y complemento.

Un subconjunto P de un conjunto X es cofinito (en X) si su complemento P^C es finito: en otras palabras, P es cofinito si puede obtenerse de X eliminando un número finito de elementos.

Proposición 1.3 *La clase A de todos los subconjuntos de un conjunto X no vacío que son finitos o cofinitos es un campo de subconjuntos de X.*

Prueba.

La unión de dos subconjuntos finitos es finita, mientras que la unión de un subconjunto cofinito con cualquier subconjunto es cofinito; además, el complemento de un subconjunto finito es cofinito, y viceversa. Si el conjunto X es finito, entonces A es simplemente $\mathbb{P}(X)$; si X es infinito; entonces A es un nuevo ejemplo de álgebra booleana y se llama álgebra (o campo) finito-cofinita de X. ■

1.8. Orden

A continuación se enuncian conceptos de relación de orden de forma superficial y serán utilizados posteriormente.

Lema 1.2 *$p \cdot q = p$ si y sólo si $p + q = q$.*

Prueba. "$\Longrightarrow$"
La hipótesis es que $p \cdot q = p$.

$$\begin{aligned} p \cdot q = p &\Longrightarrow p + q = (p \cdot q) + q \\ &\Longrightarrow p + q = q; \text{ usando ley de absorción en la Definición 1.10.} \end{aligned}$$

"$\Longleftarrow$"
La hipótesis es que $p + q = q$.

$$\begin{aligned} p + q = q &\Longrightarrow p \cdot q = p \cdot (p + q) \\ &\Longrightarrow p \cdot q = p; \text{ usando ley de absorción en la Definición 1.10.} \end{aligned}$$

■

Definición 1.28 *Sean A un álgebra booleana y $p, q \in A$. Diremos que p está antes que q si y sólo si $p \cdot q = p$ ó $p + q = q$ y lo denotaremos como $p \leq q$.*

Lema 1.3 *Dada un álgebra booleana A. La relación $\leq$ es un orden parcial sobre A. Además, se satisface que:*

1. $0 \leq p$ *y* $p \leq 1$, $\forall p \in A$.
2. *Si* $p \leq q$ *y* $r \leq s$, *entonces* $p \cdot r \leq q \cdot s$ *y* $p + r \leq q + s$.
3. *Si* $p \leq q$, *entonces* $q' \leq p'$.
4. $p \leq q$ *si y sólo si* $pq' = 0$.

Prueba.

1. Probamos que $0 \leq p$ y $p \leq 1$, $\forall p \in A$.

   a) Sea $p \in A$. Por hipótesis $0 \leq p$.

   $0 \leq p \Longrightarrow 0 \cdot p = 0$ ó $0 + p = p, p \in A;$ usando la Definición 1.28.

   b) Sea $p \in A$. Por hipótesis $p \leq 1$.

   $p \leq 1 \Longrightarrow p \cdot 1 = p$ ó $p + 1 = p', p' \in A;$ usando la Definición 1.28.

2. Probamos que $p \leq q$ si y sólo si $pq' = 0$.

   a) Probamos que si $p \leq q$, entonces $pq' = 0$.

   Se sabe por Definición 1.28 que si $p \leq q$, entonces $p \cdot q = p$, $p + q = q$. Así,

$$\begin{aligned} p \leq q &\Longrightarrow p + q = q \\ &\Longrightarrow (p+q)' = q' \\ &\Longrightarrow p'q' = q' \\ &\Longrightarrow q' = p'q' \\ &\Longrightarrow pq' = p(p'q') \\ &\Longrightarrow pq' = (pp')q' \\ &\Longrightarrow pq' = 0 \cdot q' \\ &\Longrightarrow pq' = 0 \end{aligned}$$

b) Probamos que si $pq^{'} = 0$, entonces $p \leq q$.

Se sabe por Definición 1.28 que si $p \leq q$, entonces $p \cdot q = p$, $p + q = q$.

Así, por hipótesis $pq^{'} = 0$.

$$\begin{aligned}
pq^{'} = 0 &\Longrightarrow pq^{'} = pp^{'}q^{'} \\
&\Longrightarrow pq^{'} + p^{'}q^{'} = pp^{'}q^{'} + p^{'}q^{'} \\
&\Longrightarrow (p + p^{'})q^{'} = (p + 1)p^{'}q^{'} \\
&\Longrightarrow 1 \cdot q^{'} = (1 + p)p^{'}q^{'} \\
&\Longrightarrow q^{'} = p^{'}p^{'}q^{'} \\
&\Longrightarrow q^{'} = p^{'}q^{'} \\
&\Longrightarrow (q^{'})^{'} = (p^{'}q^{'})^{'} \\
&\Longrightarrow q = ((p + q)^{'})^{'} \\
&\Longrightarrow q = p + q \\
&\Longrightarrow p \leq q
\end{aligned}$$

Por lo cual, podemos concluir que $p \leq q$ si y sólo si $pq^{'} = 0$.

3. Probamos que si $p \leq q$, entonces $q^{'} \leq p^{'}$.

Como hipótesis $p \leq q$ y por lo demostrado en el ítem anterior tenemos que $pq^{'} = 0$.

$$\begin{aligned}
pq^{'} = 0 &\Longrightarrow (p^{'})^{'}q^{'} = 0 \\
&\Longrightarrow q^{'}(p^{'})^{'} = 0 \\
&\Longrightarrow q^{'} \leq p^{'}
\end{aligned}$$

Por lo cual, si $p \leq q$, entonces $q^{'} \leq p^{'}$.

4. Probaremos que si $p \leq q$ y $r \leq s$, entonces $p \cdot r \leq q \cdot s$ y $p + r \leq q + s$.

   Usando el inciso 4 se tiene que si $p \leq q$, entonces $pq' = 0$ y si $r \leq s$, entonces $rs' = 0$.

   a) Probamos que $p \cdot r \leq q \cdot s$.

$$
\begin{aligned}
pq' + rs' &= 0 \\
r(pq' + rs') &= r \cdot 0 \\
rpq' + rrs' &= 0 \\
prq' + rs' &= 0 \\
pprq' + prs' &= 0 \\
prq' + prs' &= 0 \\
pr(q' + s') &= 0 \\
pr(qs)' &= 0
\end{aligned}
$$

   Por lo cual, $pr \leq qs$.

   b) Probamos que $p + r \leq q + s$.

$$
\begin{aligned}
pq' + rs' &= 0 \\
pq'(s + s') + rs'(q + q') &= 0 \\
pq's + pq's' + rs'q + rs'q' &= 0 \\
pq's' + rs'q' &= 0 \\
pq's' + rq's' &= 0 \\
(p + r)(q's') &= 0 \\
(p + r)(q + s)' &= 0
\end{aligned}
$$

   Por lo cual, $p + r \leq q + s$.

Así, se puede concluir que si si $p \leq q$ y $r \leq s$, entonces $p \cdot r \leq q \cdot s$ y $p + r \leq q + s$. ■

Lema 1.4 *La relación $\leq$ es un orden parcial. Es decir, es reflexiva ($p \leq p$), antisimétrica (si $p \leq q$ y $q \leq p$, entonces $p = q$) y transitiva (si $p \leq q$ y $q \leq r$, entonces $p \leq r$).*

Prueba.

1. Probamos transitividad. Si $p \leq q$ y $q \leq r$, entonces $p \leq r$.

   Se tiene por Lema 1.3 que:

   $$p \leq q \Longleftrightarrow pq^{'} = 0, \text{ y } q \leq r \Longleftrightarrow qr^{'} = 0.$$

   Se probará que si $pr^{'} = 0$, entonces $p \leq r$. Pues, $p \leq r$ si y sólo si $pr^{'} = 0$. así,

   $$\begin{aligned} pr^{'} &= pr^{'}(q + q^{'}) \\ &= pr^{'}q + pr^{'}q^{'} \\ &= p(0) + r^{'}(0) \\ &= 0 \end{aligned}$$

2. Probamos antisimetría. Si $p \leq q$ y $q \leq p$, entonces $q = p$.

   Se tiene que:

   $$p \leq q \Longleftrightarrow pq^{'} = 0, \text{ y } q \leq p \Longleftrightarrow qp^{'} = 0.$$

   Así,

   $$\begin{array}{cc} pq^{'} = qp^{'} & pq^{'} = qp^{'} \\ (pq^{'})^{'} = (qp^{'})^{'} & (pq^{'})^{'} = (qp^{'})^{'} \\ p^{'} + q = q^{'} + p & p^{'} + q = q^{'} + p \\ p(p^{'} + q) = p(q^{'} + p) & q(p^{'} + q) = q(q^{'} + p) \\ pp^{'} + pq = pq^{'} + pp & qp^{'} + qq = qq^{'} + qp \\ 0 + pq = 0 + p & 0 + q = 0 + qp \\ pq = p & q = qp \\ qp = p & \end{array}$$

Por lo que se puede concluir que si $p \leq q$ y $q \leq p$, entonces $q = p$.

3. Probando que es reflexiva. $p \leq p$. Como $pp' = 0$, entonces $p \leq p$. ■

Definición 1.29 *Un retículo X es un conjunto parcialmente ordenado en el cual cualquier conjunto de al menos dos elementos tiene tanto supremo como ínfimo.*

Dado X un retículo, en analogía con las álgebras booleanas denotaremos por $x \vee y = \sup\{x, y\}$ y $x \wedge y = \text{ínf}\{x, y\}$, para cualesquiera $x, y \in X$.

En cualquier retículo X se tiene que si $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ se satisface, entonces $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$ también se satisface, y viceversa. Un retículo X en el cual ambas leyes distributivas se satisfacen es llamado distributivo.

Definición 1.30 *Un retículo X es llamado complementado si,*

1. *X contiene dos elementos denotados por 0 y 1 tales que $x \in X$, se tiene $0 \leq x$ y $x \leq 1$.*
2. *Para cada $x \in X$, existe al menos un $y \in X$ con $x \wedge y = 0$ y $x \vee y = 1$.*

Observaciones 1.2 *Note que si X es un retículo distributivo y complementado entonces el elemento de la segunda parte de la definición 1.30 es único.*

En efecto, supongamos que para $x \in X$ existen $y_0, y_1 \in X$ tales que $x \wedge y_0 = 0 = x \wedge y_1$ y $x \vee y_0 = 1 = x \vee y_1$. Entonces, como consecuencia de las leyes distributivas tenemos:

$$\begin{aligned}
y_1 &= y_1 \wedge 1 \\
&= y_1 \wedge (x \vee y_0) \\
&= (y_1 \wedge x) \vee (y_1 \wedge y_0) \\
&= (x \wedge y_1) \vee (y_1 \wedge y_0) \\
&= 0 \vee (y_1 \wedge y_0) \\
&= (x \wedge y_0) \vee (y_1 \wedge y_0) \\
&= (x \vee y_1) \wedge y_0 \\
&= 1 \wedge y_0 \\
&= y_0
\end{aligned}$$

Por lo tanto, $y_0 = y_1$.

Teorema 1.7 *Todo retículo complementado y distributivo es un álgebra booleana.*

Prueba.

Sea A un retículo complementado y distributivo. Probamos que A satisface las condiciones de 1.22 con las operaciones:

$$x \vee y := \sup\{x, y\},$$

$$x \wedge y := \text{ínf}\{x, y\}$$

y complementación $(')$ definida en 1.30, de la manera siguiente: dado $x \in A$, existe al menos un elemento $y \in A$ tal que $x \wedge y = 0$ y $x \vee y = 1$, pero por la Observación 1.2 este elemento es único cuando A es distributivo, por lo tanto denotaremos a tal elemento y por x' y lo llamaremos complementario de x.

Es claro que las condiciones de álgebra booleana se cumplen, con lo cual nuestro problema se reduce a verificar la condición 4.

$$\begin{aligned}
(x' \vee y') \wedge (x \wedge y) &= \Big[(x' \vee y') \wedge x\Big] \wedge y \\
&= \Big[(x' \wedge x) \vee (y' \wedge x)\Big] \wedge y \\
&= \Big[0 \vee (y' \wedge x)\Big] \wedge y \\
&= (y' \wedge x) \wedge y \\
&= (x \wedge y') \wedge y \\
&= x \wedge (y' \wedge y) \\
&= x \wedge 0 \\
&= 0
\end{aligned}$$

Análogamente,

$$\begin{aligned}
(x^{'} \vee y^{'}) \vee (x \wedge y) &= \Big[(x^{'} \vee y^{'}) \vee x\Big] \wedge \Big[(x^{'} \vee y^{'}) \vee y\Big] \\
&= \Big[(y^{'} \vee x^{'}) \vee x\Big] \wedge \Big[x^{'} \vee (y^{'} \vee y)\Big] \\
&= \Big[y^{'} \vee (x^{'} \vee x)\Big] \wedge \Big[x^{'} \vee (y^{'} \vee y)\Big] \\
&= (y^{'} \vee 1) \wedge (x^{'} \vee 1) \\
&= 1 \wedge 1 \\
&= 1
\end{aligned}$$

Por tanto, $(x^{'} \vee y^{'}) \wedge (x \wedge y) = 0$ y $(x^{'} \vee y^{'}) \vee (x \wedge y) = 1$. ■

Capítulo 2

Estructuras de Álgebras Booleanas

El presente capítulo está orientado al estudio de las álgebras booleanas y los homomorfismos entre ellas, así como la dualidad de estos conceptos con los anillos booleanos y homomorfismos entre anillos booleanos, en cada sección se presentan definiciones, teoremas, proposiciones y ejemplos.

2.1. Ideales y filtros booleanos

Definición 2.1 *Sea M un subconjunto del álgebra booleana B. Se dice que M es un ideal booleano de B si se satisfacen:*

1. $0 \in M$
2. *Para todo* $a, b \in M$*,* $a \vee b \in M$
3. *Para todo* $a \in M$ *y* $b \in B$*,* $a \wedge b \in M$

Observaciones 2.1 *La condición* 1 *en la definición 2.1 puede ser reemplazada por la condición de que M es distinto de vacío, sin cambiar el concepto de ideal, pues si M no es vacío existe un $a \in M$, luego por la condición* 3 *de la definición 2.1 se tiene que $a \wedge 0 \in M$, pero como B es un álgebra booleana se cumple que $a \wedge 0 = a \cdot 0 = 0$, por tanto $0 \in M$.*

La Definición 2.1 no es la única manera de definir un ideal booleano, esta definición se puede dar a partir de teoría de anillos, así como también usando la noción de orden. Así, se tiene la siguiente proposición.

Proposición 2.1 *Un subconjunto M de una álgebra booleana B es un ideal booleano si y sólo si es un ideal en el anillo booleano.*

Prueba.

"$\Longrightarrow$"
Por hipótesis M es un ideal en el álgebra booleana B y M es un grupo booleano aditivo sobre el álgebra booleana.

1. Probando que M es estable.

   Sean $a \in M$ y $b \in B$.

   $$\begin{aligned} a \in M, b \in B &\Longrightarrow a \cdot b := a \wedge b, \text{ por Definición 2.1 inciso 3 se tiene que } a \wedge b \in M \\ &\Longrightarrow a \cdot b \in M \end{aligned}$$

   Por lo cual, M es estable.

2. Probemos que M es grupo booleano aditivo sobre el anillo booleano B.

   a) Probando que M es cerrado.
   Sea $a, b \in M$ y $a', b' \in B$ por inciso 3 se sabe que $a \wedge b' \in M$ y $a' \wedge b \in M$.
   Luego, por el inciso 2 se tiene que $(a \wedge b') \vee (a' \wedge b) \in M$.
   Por tanto, como $a + b := (a \wedge b') \vee (a' \wedge b) \in M$ se tiene que $a + b \in M$, así se concluye que M es cerrado.

   b) Probando que M es asociativo.
   Sean $a, b, c \in M$ y $a', b', c' \in B$. Como M es cerrado bajo la suma se tiene que

$a \in M$ y $b + c \in M$, entonces $a + (b + c) \in M$. Así,

$$\begin{aligned}
a + (b + c) &= \left[a \wedge \left(\left(b \wedge c^{'}\right) \vee (b^{'} \wedge c)\right)^{'}\right] \vee \left[a^{'} \wedge \left(\left(b \wedge c^{'}\right) \vee \left(b^{'} \wedge c\right)\right)\right] \\
&= \left[a \wedge \left((b^{'} \vee c) \wedge (b \vee c^{'})\right)\right] \vee \left[a^{'} \wedge \left((b \wedge c^{'}) \vee (b^{'} \wedge c)\right)\right] \\
&= \left[(a \wedge (b^{'} \vee c)) \wedge (b \vee c^{'})\right] \vee \left[(a^{'} \wedge (b \wedge c^{'})) \vee (a^{'} \wedge (b^{'} \wedge c))\right] \\
&= \left[\left((a \wedge b^{'}) \vee (a \wedge c)\right) \wedge (b \vee c^{'})\right] \vee \left[((a^{'} \wedge b) \wedge c^{'}) \vee ((a^{'} \wedge b^{'}) \wedge c)\right] \\
&= \left[((a \wedge b^{'}) \wedge (b \vee c^{'})) \vee ((a \wedge c) \wedge (b \vee c^{'}))\right] \vee \\
&\quad \left[((a^{'} \wedge b) \wedge c^{'}) \vee ((a^{'} \wedge b^{'}) \wedge c)\right] \\
&= \left[(a \wedge b^{'}) \wedge (b \vee c^{'}) \vee ((a^{'} \wedge b) \wedge c^{'})\right] \vee \\
&\quad \left[((a \wedge c) \wedge (b \vee c^{'})) \vee ((a^{'} \wedge b^{'}) \wedge c)\right] \\
&= \left[((a \wedge b^{'}) \wedge b) \vee ((a \wedge b^{'}) \wedge c^{'}) \vee ((a^{'} \wedge b) \wedge c^{'})\right] \vee \\
&\quad \left[(((a \wedge c) \wedge b) \vee ((a \wedge c) \wedge c^{'})) \vee ((a^{'} \wedge b^{'}) \wedge c)\right] \\
&= \left[((a \wedge b^{'}) \wedge c^{'}) \vee ((a^{'} \wedge b) \wedge c^{'})\right] \vee \left[((a \wedge c) \wedge b) \vee ((a^{'} \wedge b^{'}) \wedge c)\right]
\end{aligned}$$

Nuevamente, como M es cerrado bajo la suma se tiene que $a + b \in M$ y $c \in M$, entonces $(a + b) + c \in M$. Así,

$$\begin{aligned}
(a + b) + c &= \left[((a \wedge b^{'}) \vee (a^{'} \wedge b)) \wedge c^{'}\right] \vee \left[((a \wedge b^{'}) \vee (a^{'} \wedge b))^{'} \wedge c\right] \\
&= \left[((a \wedge b^{'}) \vee (a^{'} \wedge b)) \wedge c^{'}\right] \vee \left[((a^{'} \vee b) \wedge (b \vee a^{'})) \wedge c\right] \\
&= \left[((a \wedge b^{'}) \vee (a^{'} \wedge b)) \wedge c^{'}\right] \vee \left[((b \vee a^{'}) \wedge (a \vee b^{'})) \wedge c\right] \\
&= \left[((a \wedge b^{'}) \vee (a^{'} \wedge b)) \wedge c^{'}\right] \vee \\
&\quad \left[(((a \vee a^{'}) \wedge (b \vee a^{'})) \wedge ((a \vee b^{'}) \wedge (b \vee b^{'}))) \wedge c\right]
\end{aligned}$$

$$= \left[((a \wedge b^{'}) \vee (a^{'} \wedge b)) \wedge c^{'}\right] \vee \left[(((a \wedge b) \vee a^{'}) \wedge ((a \wedge b) \vee b^{'})) \wedge c\right]$$

$$= \left[((a \wedge b^{'}) \vee (a^{'} \wedge b)) \wedge c^{'}\right] \vee \left[((a \wedge b) \vee (a^{'} \wedge b^{'})) \wedge c\right]$$

$$= \left[((a \wedge b^{'}) \vee (a^{'} \wedge b)) \wedge c^{'}\right] \vee \left[((a \wedge b) \wedge c) \vee ((a^{'} \wedge b^{'}) \wedge c)\right]$$

$$= \left[((a \wedge b^{'}) \wedge c^{'}) \vee ((a^{'} \wedge b) \wedge c^{'})\right] \vee \left[((a \wedge c) \wedge b) \vee ((a^{'} \wedge b^{'}) \wedge c)\right]$$

Por tanto, $(a+b)+c = a+(b+c)$. Así, M es asociativo.

$c)$ Probando que M tiene identidad.

1) Probando que $a + 0 = a$ está en M.

Sea $a, 0 \in M$, la suma la definimos como $a + 0 := (a \wedge 0^{'}) \vee (a^{'} \wedge 0)$.

$$\begin{aligned} a \in M, 0 \in M &\Longrightarrow a + 0 := (a \wedge 0^{'}) \vee (a^{'} \wedge 0) \\ &\Longrightarrow a + 0 = (a \wedge 1) \vee (a^{'} \wedge 0) \\ &\Longrightarrow a + 0 = (a \cdot 1) \vee (a^{'} \cdot 0) \\ &\Longrightarrow a + 0 = a \vee 0 \\ &\Longrightarrow a + 0 = a \end{aligned}$$

2) Probando que $0 + a = a$ está en M.

Sea $a \in M$, la suma la definimos como $0 + a = (0 \wedge a^{'}) \vee (0^{'} \wedge a)$. Así,

$$\begin{aligned} a \in M, 0 \in M &\Longrightarrow 0 + a := (0 \wedge a^{'}) \vee (0^{'} \wedge a) \\ &\Longrightarrow 0 + a = (0 \wedge a^{'}) \vee (1 \wedge a) \\ &\Longrightarrow 0 + a = (0 \cdot a^{'}) \vee (1 \cdot a) \\ &\Longrightarrow 0 + a = 0 \vee a \\ &\Longrightarrow 0 + a = a \end{aligned}$$

Por tanto, 0 es el elemento neutro para la suma en M.

d) Probando que M tiene inverso.

Sea $a \in M$. Se prueba que el inverso aditivo de a es el mismo a.

$$\begin{aligned} a + a &:= (a \wedge a^{'}) \vee (a^{'} \wedge a) \\ &= (a \cdot a^{'}) \vee (a^{'} \cdot a) \\ &= 0 \vee 0 \\ &= 0 \end{aligned}$$

Por tanto, a es el inverso de él mismo en M.

Así, se ha probado que M es un ideal en el anillo booleano B.

"$\Longleftarrow$"
Por hipótesis M es un ideal en el anillo booleano B y se quiere probar que M es un ideal en el álgebra booleana.

1. Probando que $0 \in M$.
   Es claro que $0 \in M$, porque M es un ideal en el anillo booleano B.

2. Probando que M es estable.
   Sea $a \in M$ y $b \in B$.

$$\begin{aligned} a \in M, b \in B &\Longrightarrow a \wedge b := a \cdot b; \text{ pero } a \cdot b \in M \\ &\Longrightarrow a \wedge b \in M \end{aligned}$$

3. Probando que M cumple la condición 2 de ideal.

   Sea $a, b \in M$.

$$\begin{aligned} a, b \in M &\Longrightarrow a \vee b := a + b + ab; \text{ pero } a + b \in M \text{ y } a \cdot b \in M \\ &\Longrightarrow a \vee b := a + b + ab \in M \\ &\Longrightarrow a \vee b \in M \end{aligned}$$

Así, se ha probado que M es un ideal en el álgebra booleana B. ■

Observaciones 2.2 *La condición* 3) *de la Definición 2.1 puede ser reemplazada por: Si* $a \in M$ *y* $b \leq a$, *entonces* $b \in M$.

Prueba.

Para realizar la prueba se hace uso del Lema 1.3, así se tiene que:

$$\begin{aligned} b \leq a &\Longrightarrow ba' = 0 \\ &\Longrightarrow ba + ba' = ba + 0 \\ &\Longrightarrow b(a + a') = ba \\ &\Longrightarrow b(1) = ba \\ &\Longrightarrow b = ba \\ &\Longrightarrow b = ab; \text{ pero } ab \in M \\ &\Longrightarrow b \in M \end{aligned}$$

■

Ejemplo 2.1 *Sean* X *un conjunto no vacío y* $\mathscr{J} = \{A \in \mathbb{P}(X) : A \text{ es infinito numerable}\}$. *La familia* $\mathscr{J}$ *es un ideal en* $\mathbb{P}(X)$.

Prueba.

Se quiere probar que $\mathscr{J}$ es un ideal.

1. Probamos que cumple la primer condición.

   Recordemos que en el álgebra booleana $0 = \emptyset$. Así, $0 = \emptyset \in \mathbb{P}(X)$, entonces $\emptyset$ es numerable, por lo cual se puede concluir que $0 \in \mathscr{J}$.

2. Probamos que cumple la segunda condición.

Sean $A, B \in \mathscr{J}$ donde A y B son numerables, se quiere probar que $A \cup B \in \mathbb{P}(X)$.

Para ello debemos de probar que si existe una función

$$h^{'} : A \cup B \longrightarrow N$$

inyectiva, así $A \cup B \in \mathscr{J}$.

Se sabe que N es numerable, entonces probemos que

$$f : N \times N \longrightarrow N,$$

es inyectiva.

Sea $f : N \times N \longrightarrow N$ definida por $(n, m) \mapsto f(n, m) = 2^m \cdot 3^n$, como se quiere probar que f es inyectiva se tiene que:

Sea $f(n, m) = f(x, y)$ donde $f(n, m) = 2^m \cdot 3^n$ y $f(x, y) = 2^y \cdot 3^x$, entonces $n = x, m = y$.

I) Si $n \neq x$ se tendrían dos casos.

1) Si $n > x$.

$$2^m 3^n = 2^y 3^x \Longrightarrow 2^{y-m} = 3^{n-x}$$

a) Si $y > m$.

$$y > m \Longrightarrow 3^{n-x} = 2^{y-m} (\rightarrow\leftarrow)$$

pues, 3^{n-x} seria par.

b) Si $y < m$.

$$y < m \Longrightarrow 3^{n-x} = 2^{y-m} (\rightarrow\leftarrow)$$

pues, 3^{n-x} sería un racional irreducible.

c) Si $y = m$.

$$y = m \Longrightarrow 3^{n-x} = 1(\rightarrow\leftarrow)$$

pues, $3^{n-x} \neq 1$.

Por lo que, $n \not> x$.

2) Si $n < x$.

$$2^m 3^n = 2^y 3^x \Longrightarrow 2^{m-y} = 3^{x-n}.$$

a) Si $y > m$.

$$y > m \Longrightarrow 2^{m-y} = 3^{x-n}(\rightarrow\leftarrow)$$

pues, 3^{x-n} sería un racional irreducible.

b) Si $y < m$.

$$y < m \Longrightarrow 2^{m-y} = 3^{x-n}(\rightarrow\leftarrow)$$

pues, 3^{x-n} sería par.

c) Si $y = m$.

$$y = m \Longrightarrow 1 = 3^{x-n}(\rightarrow\leftarrow)$$

pues, $3^{x-n} \neq 1$.

Por lo que, $n \not< x$.

Así, se puede concluir que $n = x$ y $m = y$.

II) Si $m \neq y$ se tendrían dos casos.

1) Si $m > y$.

$$2^m 3^n = 2^y 3^x \Longrightarrow 2^{m-y} = 3^{x-n}$$

a) Si $x > n$.

$$x > n \Longrightarrow 2^{m-y} = 3^{x-n}(\rightarrow\leftarrow)$$

pues, 2^{m-y} sería impar.

b) Si $x < n$.

$$x < n \Longrightarrow 2^{m-y} = 3^{x-n}(\rightarrow\leftarrow)$$

pues, 2^{m-y} sería un racional irreducible.

c) Si $x = n$.

$$x = n \Longrightarrow 2^{m-y} = 1(\rightarrow\leftarrow)$$

pues, $2^{m-y} \neq 1$.

Por lo que, $m \not> y$.

2) Si $m < y$.

$$2^m 3^n = 2^y 3^x \Longrightarrow 2^{y-m} = 3^{n-x}.$$

a) Si $x > n$.

$$x > n \Longrightarrow 2^{y-m} = 3^{n-x}(\rightarrow\leftarrow)$$

pues, 2^{y-m} sería un racional irreducible.

b) Si $x < n$.

$$x < n \Longrightarrow 2^{y-m} = 3^{n-x}(\rightarrow\leftarrow)$$

pues, 2^{y-m} sería impar.

c) Si $x = n$.

$$x = n \Longrightarrow 2 = 1(\rightarrow\leftarrow)$$

pues, $2^{y-m} \neq 1$.

Por lo que, $m \not< y$.

Así, se puede concluir que $n = x$ y $m = y$.

Dado que se ha probado que f es inyectiva, podemos concluir que $N \times N$ es numerable.

Sean A, B numerables, se tiene entonces que $A \cup B$ es numerable.

Definamos $\varphi_1 : A \longrightarrow N$ inyectiva definida por $a \mapsto \varphi_1(a)$ y $\varphi_2 : B \longrightarrow N$ inyectiva definida por $b \mapsto \varphi_2(b)$.

Ahora, sea

$$\psi : A \cup B \longrightarrow N \times N,$$

definida por:

$$x \mapsto \psi(x) = \begin{cases} (\varphi_1(x), 1), & \text{si } x \in A \text{ ó } x \in A \cap B \\ (\varphi_2(x), 2), & \text{si } x \in B \text{ y } x \notin A \end{cases}$$

Probamos que ψ es inyectiva.

Sea $x, y \in A \cup B$ tal que $\psi(x) = \psi(y)$.

$$\psi(x) = \begin{cases} (\varphi_1(x), 1), & \text{si } x \in A \text{ ó } x \in A \cap B \\ (\varphi_2(x), 2), & \text{si } x \in B \text{ y } x \notin A \end{cases}$$

$$\psi(y) = \begin{cases} (\varphi_1(y), 1), & \text{si } y \in A \text{ ó } y \in A \cap B \\ (\varphi_2(y), 2), & \text{si } y \in B \text{ y } y \notin A \end{cases}$$

$$\Longrightarrow \begin{cases} (\varphi_1(x), 1) = (\varphi_1(y), 1), & \text{si } x, y \in A \text{ ó } x, y \in A \cap B \\ & \text{ó} \\ (\varphi_2(x), 2) = (\varphi_2(y), 2), & \text{si } x, y \in B \text{ y } x, y \notin A \end{cases}$$

$$\Longrightarrow \begin{cases} \varphi_1(x) = \varphi_1(y), & \text{si } x, y \in A \text{ ó } x, y \in A \cap B \\ & \text{ó} \\ \varphi_2(x) = \varphi_2(y), & \text{si } x, y \in B \text{ y } x, y \notin A \end{cases}$$

$$\Longrightarrow \begin{cases} x = y, & \text{si } x, y \in A \text{ ó } x, y \in A \cap B \\ & \text{ó} \\ x = y, & \text{si } x, y \in B \text{ y } x, y \notin A \end{cases}$$

Así, tenemos que $x = y$. Por lo cual ψ es inyectiva, así hemos probado que $A \cup B$ es numerable.

Por tanto, $A \cup B \in \mathscr{J}$.

3. Probamos que se cumple la tercera condición.

   Sea $A \in \mathbb{P}(X)$, $B \in \mathscr{J}$.

   Si $A \cap B = \emptyset$, $A \cap B$ es numerable, pues $\emptyset$ es numerable. Ahora, si $A \cap B \subset B$, $A \cap B$ es numerable pues B es numerable. Así, concluimos que $A \cap B \in \mathscr{J}$.

Por tanto, se ha probado que $\mathscr{J}$ es un ideal en $\mathbb{P}(X)$. ■

Toda álgebra booleana B contiene un ideal trivial, el conjunto $\{0\}$ (formado justamente por 0). Análogamente, toda álgebra booleana B tiene un ideal impropio, B (él mismo); cualquier otro ideal será llamado **propio**.

Proposición 2.2 *Sea B un álgebra booleana. Un ideal booleano $M \subset B$ es propio, si y sólo si no contiene a* 1 *(si lo contuviese sería el propio B).*

Prueba.

"$\Longrightarrow$"

Supongamos que M es un ideal propio de B y que $1 \in M$.

$$\begin{aligned} p \in B, 1 \in M &\Longrightarrow p \wedge 1 \in M, \text{ por inciso 3 de la Definición 2,1.} \\ &\Longrightarrow p \wedge 1 = p \in M \end{aligned}$$

Así, $M = B$. Lo que contradice el hecho de que M sea un ideal propio de B. Por lo cual, si M es un ideal propio $1 \notin M$.

" $\Longleftarrow$ "

Por hipótesis, se tiene que 1 no está contenido en M.

$$\begin{aligned} 1 \notin M &\Longrightarrow M \text{ no es impropio} \\ &\Longrightarrow M \neq B \\ &\Longrightarrow M \text{ es propio} \end{aligned}$$

■

Definición 2.2 *Sea B un álgebra booleana. El generado por E denotado por $Gen(E)$, es la intersección de todos los ideales en B que contienen a E.*

Teorema 2.1 *Sea B un álgebra booleana y $E \subseteq B$. El $Gen(E)$ es el ideal que consiste de todos los elementos de la forma*

$$(y_1 \wedge x_1) \vee \ldots \vee (y_k \wedge x_k), k \geq 1$$

donde, $x_1, \ldots, x_k \in E$ y $y_1, \ldots, y_k$ son elementos arbitrarios de B.

Prueba. Se quiere probar que el ideal $Gen(E)$ consiste de todos los elementos de la forma $(y_1 \wedge x_1) \vee \ldots \vee (y_k \wedge x_k), k \geq 1$ donde, $x_1, \ldots, x_k \in E$ y $y_1, \ldots, y_k \in B$.

Sea $D = \{x \in B | x = (y_1 \wedge x_1) \vee \ldots \vee (y_k \wedge x_k), k \geq 1, x_i \in E, \text{ y } y_i \in B, i = 1, \ldots, k\}$.

1. Probando que D es un ideal.

   a) Probando que $0 \in D$.

   Sea $0 \in B$.

$$\begin{aligned} 0 \in B &\Longrightarrow 0 = (0 \wedge x_1) \vee (0 \wedge x_2) \vee \ldots \vee (0 \wedge x_k), x_i \in C, i = 1, \ldots, k \\ &\Longrightarrow 0 \in D \end{aligned}$$

b) Probando que si $x, y \in D$, entonces $x \vee y \in D$.

Sean $x, y \in D$, donde $x = (y_1 \wedge x_1) \vee \ldots \vee (y_k \wedge x_k)$ y $y = (z_1 \wedge w_1) \vee \ldots \vee (z_n \wedge w_n)$, con $y_i, z_i \in B$, $x_i, w_i \in E$ con $k, n \geq 1$.

$$\begin{aligned}
x \vee y &= [(y_1 \wedge x_1) \vee \ldots \vee (y_k \wedge x_k)] \vee [(z_1 \wedge w_1) \vee \ldots \vee (z_n \wedge w_n)] \\
&= (y_1 \wedge x_1) \vee \ldots \vee (y_k \wedge x_k) \vee (z_1 \wedge w_1) \vee \ldots \vee (z_n \wedge w_n) \in D; \\
&\quad y_i, z_i \in B, x_i, w_i \in E
\end{aligned}$$

Por lo cual, se puede concluir que $x \vee y \in D$.

c) Probando que si $x \in B$ y $y \in D$, entonces $x \wedge y \in D$.

$$\begin{aligned}
x \wedge y &= x \wedge [(z_1 \wedge w_1) \vee \ldots \vee (z_n \wedge w_n)] \\
&= (x \wedge (z_1 \wedge w_1)) \vee \ldots \vee (x \wedge (z_n \wedge w_n)) \\
&= ((x \wedge z_1) \wedge w_1) \vee \ldots \vee ((x \wedge z_n) \wedge w_n) \in D; \text{ porque } x \wedge z_i \in B, w_i \in E
\end{aligned}$$

Por lo cual, concluimos que $x \wedge y \in D$.

Así, se ha probado que D es ideal.

2. Probamos que $E \subset D$.

$$\begin{aligned}
y \in E &\Longrightarrow y = (1 \wedge y) \vee (0 \wedge y); \text{ donde } 1, 0 \in B. \\
&\Longrightarrow y = (1 \wedge y) \vee (0 \wedge y) \in D \\
&\Longrightarrow y \in D
\end{aligned}$$

Por lo tanto, $E \subset D$.

3. Probamos que D es la intersección de todos los ideales que contienen a E.

   Se quier probar que

$$D = \bigcap_{E \subset I_w} I_w, w \in J$$

   a) Probando que $\bigcap_{E \subset I_w} I_w \subset D, w \in J$.

$$\begin{aligned} E \subset D &\Longrightarrow D = I_w, \text{ para algún } w \in J \\ &\Longrightarrow \bigcap_{E \subset I_w} I_w \subset D \end{aligned}$$

   b) Probando que $D \subset \bigcap_{E \subset I_w} I_w, w \in J$.

   Sea $x \in D$.

$$\begin{aligned} x \in D &\Longrightarrow x = (y_1 \wedge x_1) \vee \ldots \vee (y_k \wedge x_k), \text{ con } x_i \in I_w, \forall w \in J \\ &\Longrightarrow y_i \wedge x_i \in I_w, \forall w \in J, i = 1, \ldots, k \\ &\Longrightarrow y_i \wedge x_i \in \bigcap_{E \subset I_w} I_w, w \in J \end{aligned}$$

Por tanto, se ha probado que:

$$D = \bigcap_{E \subset I_w} I_w, w \in J$$

Pero,

$$Gen(E) = \bigcap_{E \subset I_w} I_w, w \in J$$

Así, $D = Gen(E)$.

Por lo cual se ha probado que el ideal $Gen(E)$ consiste de todos los elementos de la forma $(y_1 \wedge x_1) \vee \ldots \vee (y_k \wedge x_k), k \geq 1$ donde, $x_1, \ldots, x_k \in E$ y $y_1, \ldots, y_k \in B$. ■

Ejemplo 2.2 *Si $E = \{0\}$, entonces $Gen(E) = \{0\}$ es el ideal trivial.*

Teorema 2.2 *Sea B un álgebra booleana y $E \subseteq B$, el ideal $Gen(E)$ consiste de todos los elementos y tal que;*

$$y \leq x_1 \vee \ldots \vee x_k$$

donde, $x_1, \ldots, x_k$ son elementos arbitrarios de E.

Prueba.

Sea $C = \{y \in E : y \leq x_1 \vee \ldots \vee x_k, k \geq 1 \text{ con } x_i \in E\}$.

1. Probando que C es un ideal.

   a) Probando que $0 \in C$.

   $0 \leq x \vee x \vee x \in C, x \in C$ Por lo cual, $0 \in C$.

   b) Probando que se cumple la condición 2 de ideal.

   Sea $y \leq x_1 \vee \ldots \vee x_k$ y $z \leq x_1 \vee \ldots \vee x_n$, con $x_i, x_j \in E, i = 1, \ldots k, j = 1, \ldots n$.

$$\begin{aligned} y \leq x_1 \vee \ldots \vee x_k \text{ y } z \leq x_1 \vee \ldots \vee x_n &\Longrightarrow y \vee z \leq [x_1 \vee \ldots \vee x_k] \vee [x_1 \vee \ldots \vee x_n] \\ &\Longrightarrow y \vee z \leq x_1 \vee \ldots \vee x_k \vee x_1 \vee \ldots \vee x_n \in C \\ &\Longrightarrow y \vee z \in C \end{aligned}$$

   Por tanto, se ha probado que $y \vee z \in C$.

   c) Probando que se cumple la condición 3 de ideal.

   Para probar está condición haremos uso de la Observación 2.2.

   Sea $y \in C, v \in B$.

$$\begin{aligned} y \in C \text{ y } v \leq y &\Longrightarrow y \leq x_1 \vee \ldots \vee x_k \text{ y } v \leq y \\ &\Longrightarrow v \leq y \leq x_1 \vee \ldots \vee x_k \\ &\Longrightarrow v \leq x_1 \vee \ldots \vee x_k \end{aligned}$$

Por tanto, se ha probado que $v \wedge y \in C$

Así, se puede concluir que C es un ideal.

2. Probando que $E \subset C$.

   Sea $x \in E$.

$$\begin{aligned} x \in E &\Longrightarrow x \leq x \vee x \vee x \in C \\ &\Longrightarrow E \subset C \end{aligned}$$

3. Probando que $C = Gen(E)$

   a) Probamos que $C \subset Gen(E)$.

   Sea $y \in C$.

$$\begin{aligned} y \in C &\Longrightarrow y \leq x_1 \vee \ldots \vee x_k; \text{ con } x_i \in E \subset I_w, \forall w \in J \\ &\Longrightarrow (x_1 \vee \ldots \vee x_k) \wedge y \in I_w, \forall w \in J \\ &\Longrightarrow y \in I_w, \forall w \in J \\ &\Longrightarrow y \in \cap_{E \subset I_w} I_w, w \in J \\ &\Longrightarrow y \in Gen(E) \end{aligned}$$

   b) Probar que $Gen(E) \subset C$ es inmediata.

Así, se puede concluir que $C = Gen(E)$. ■

Corolario 2.1 *Sea B un álgebra booleana y $E \subseteq B$, entonces el ideal $Gen(E)$ generado por E es un ideal propio si y sólo si*

$$x_1 \vee \ldots \vee x_k \neq 1$$

para todo $x_1, \ldots, x_k \in E$.

Prueba.

“ $\Longrightarrow$ ”

Supongamos que existe un $x_i \in E, i = 1, \ldots, k$ tal que $1 = x_1 \vee \ldots x_k$.

Haciendo uso del Teorema 2.2 se tiene que si $1 \leq x_1 \vee \ldots x_n$. Así,

$$\begin{aligned} 1 \leq x_1 \vee \ldots x_n &\Longrightarrow 1 \in Gen(E);\ \text{con } x_1, \ldots, x_n \in E \\ &\Longrightarrow Gen(E) \text{ no es propio} \end{aligned}$$

“ $\Longleftarrow$ ”

Supongamos que el $Gen(E)$ no es propio.

$$\begin{aligned} Gen(E) \text{ no es propio } &\Longrightarrow Gen(E) = B \\ &\Longrightarrow 1 \in Gen(B) \\ &\Longrightarrow 1 \leq x_1 \vee \ldots x_n \\ &\Longrightarrow (x_1 \vee \ldots x_n) \wedge 1 = 1 \\ &\Longrightarrow x_1 \vee \ldots x_n = 1 \end{aligned}$$

■

Teorema 2.3 *Si J es un ideal de un álgebra booleana B, y si $y \in B$, entonces el ideal $Gen(J \cup \{y\})$, generado por J unido con $\{y\}$, consiste de todos los elementos de la forma*

$$(z \wedge y) \vee x$$

donde $z \in B$ y $x \in J$.

Prueba.

Sea $H = \{(z \wedge y) \vee x | z \in B, x \in J\}$, y fijo.

1. Probando que H es un ideal.

   a) Probando que H cumple la condición 1 de ideal.

   $$0 = (0 \wedge y) \vee 0 \in H;\ \text{con } 0 \in B, x \in J, y \text{ fijo.}$$

   así, $0 \in H$.

   b) Probando que H cumple la condición 2 de ideal.

   Sea $(z_1 \wedge y) \vee x_1$, $(z_2 \wedge y) \vee x_2 \in H$.

   $$\begin{aligned}((z_1 \wedge y) \vee x_1) \vee ((z_2 \wedge y) \vee x_2) &= ((z_1 \wedge y) \vee (z_2 \wedge y)) \vee (x_1 \vee x_2) \\ &= ((z_1 \vee z_2) \wedge y) \vee (x_1 \vee x_2) \in H\end{aligned}$$

   Por lo cual, hemos probado que se cumple la condición 2.

   c) Probando que H cumple la condición 3 de ideal.

   Sea $w \in B$ y $(z \wedge y) \vee x \in H$.

   $$\begin{aligned}w \wedge ((z \wedge y) \vee x) &= (w \wedge (z \wedge y)) \vee (w \wedge x) \\ &= ((w \wedge z) \wedge y) \vee (w \wedge x) \in H\end{aligned}$$

   Por lo tanto, se ha probado que se cumple la condición 3.

   Así, se puede concluir que H es un ideal.

2. Probando que $J \cup \{y\} \subset H$.

   a) Probando que $J \subset H$.

   $$\begin{aligned}t \in J &\Longrightarrow t = (0 \wedge y) \vee t \in H \\ &\Longrightarrow t \in H \\ &\Longrightarrow J \subset H\end{aligned}$$

b) Probando que $\{y\} \in H$.

$$\begin{aligned} y = (1 \wedge y) \vee 0 &\Longrightarrow y \in H \\ &\Longrightarrow \{y\} \subset H \end{aligned}$$

Por lo tanto, $J \subset H$.

3. Probando que $H = Gen(J \cup \{y\})$.

a) Probando que $H \subset Gen(J \cup \{y\})$.

Sea $t \in H$.

$$\begin{aligned} t \in H &\Longrightarrow \exists z \in B \text{ y } \exists x \in J \text{ tal que, } t = (z \wedge y) \vee x \\ &\Longrightarrow t = (z \wedge y) \vee (1 \wedge x) \in Gen(J \cup \{y\}) \\ &\Longrightarrow H \subset Gen(J \cup \{y\}) \end{aligned}$$

b) Para probar que $Gen(J \cup \{y\}) \subset H$ es inmediato.

Por lo cual, $H = Gen(J \cup \{y\})$. ■

Corolario 2.2 *Si J es un ideal de un álgebra booleana B, y si $y \in B$ pero $y \notin J$, entonces el ideal $Gen(J \cup \{y\})$ generado por J unido con $\{y\}$ es un ideal propio si y sólo si $x \vee y \neq 1$ para todo $x \in J$, i.e. si y sólo si, para todo x en J, $y' \nleq x$.*

Prueba.

"$\Longrightarrow$"
Razonando por contradicción. Supongamos que existe $x \in J$ talque $x \vee y = 1$.

$$\begin{aligned} x, y \in Gen(J \cup \{y\}) &\Longrightarrow 1 = x \vee y \in Gen(J \cup \{y\}) \\ &\Longrightarrow 1 \in Gen(J \cup \{y\}) \\ &\Longrightarrow Gen(J \cup \{y\}) \text{ no es propio} \end{aligned}$$

" $\Longleftarrow$ "

Razonando por contradicción, y haciendo uso del Teorema 2.2.

Sea $Gen(J \cup \{y\}) = \{z \in B | z \leq x_1 \vee, \ldots, x_n \vee y, x_i \in J \text{ y } y \in \{y\}\}$.

$$\begin{aligned} Gen(J \cup \{y\}) = \{z \in B | z \leq x_1 \vee, \ldots, x_n \vee y, x_i \in J \text{ y } y \in \{y\}\} &\Longrightarrow 1 \leq (x_1 \vee, \ldots, x_n) \vee y \\ &\Longrightarrow 1 \leq x \vee y \end{aligned}$$

Así, como $Gen(J \cup \{y\})$ es ideal, por la Observación 2.2 se tiene que si $1 \leq x \vee y$, entonces:

$$1 \wedge (x \vee y) = 1$$

$$1 = x \vee y$$

■

Definición 2.3 *Un ideal M de un álgebra booleana B se dice que es maximal si y sólo si, M es un ideal propio y no existe un ideal propio J de B tal que $M \subset J$.*

Teorema 2.4 *Dado un ideal propio M de un álgebra booleana B. M es maximal si y sólo si, para cada y en B, se tiene que $y \in M$ o $y' \in M$.*

Prueba.

" $\Longrightarrow$ "

1. Suponiendo que $y \notin M$.

$$\begin{aligned} M \text{ maximal } &\Longrightarrow M \neq B \\ &\Longrightarrow \exists y \in B | y \notin M \\ &\Longrightarrow I = Gen(M \cup \{y\}) \text{ es un ideal en } B, \text{ con } M \subset I \\ &\Longrightarrow I = B \end{aligned}$$

$$\begin{aligned} &\Longrightarrow I \text{ no es propio} \\ &\Longrightarrow \exists x \in M | y^{'} \leq x \\ &\Longrightarrow y^{'}x = y^{'} \in M \\ &\Longrightarrow y^{'} \in M \end{aligned}$$

2. Suponiendo que $y \in M$ donde M es propio.

   Supongamos que $y^{'} \in M$.

$$y^{'} \in M \Longrightarrow y \vee y^{'} = 1 \in M$$

   Pero, esto sería una contradicción dado que M es propio y por la definición de propio se tiene que $1 \notin M$.

   Por lo cual, se ha probado que si M es propio y maximal, entonces para cada $y \in B$, se tiene que $y \in M$ o $y^{'} \in M$, pero no ambos.

" $\Longleftarrow$ "

Se quiere probar que M es maximal.

Supongamos que M no es maximal, entonces existe un ideal J propio en B tal que $M \subset J$.

Como $M \subset J$, existe $y \in J$ tal que $y \notin M$.

$$\begin{aligned} y \notin M &\Longrightarrow y^{'} \in M; \text{ por hipotesis} \\ &\Longrightarrow y^{'} \in M \subset J \\ &\Longrightarrow y \vee y^{'} = 1; y \vee y^{'} \in J \\ &\Longrightarrow 1 \in J (\longrightarrow\!\longleftarrow) \end{aligned}$$

Por lo cual, se ha probado que M es maximal. ■

Definición 2.4 *Sea B un álgebra booleana. Para $p \in B$, el ideal generado por el conjunto*

$\{p\}$ es llamado ideal principal de B. Lo denotaremos por $\langle p \rangle$.

Ejemplo 2.3 *El ideal trivial es maximal en el álgebra booleana $\{0,1\}$.*

Prueba.

Sea M el ideal trivial, anteriormente se ha mencionado que el ideal trivial esta denotado por $\{0\}$ así; $M = \{0\}$ donde $B = \{0,1\}$.

Se puede observar que $M \neq B$, ahora sea N un ideal de B tal que $M \subset N$.

1. Supongamos que $N \neq M$.

$$\begin{aligned} N \neq M &\Longrightarrow \exists x \in N \text{ tal que } x \notin M \\ &\Longrightarrow x = 1 \\ &\Longrightarrow N = B \end{aligned}$$

2. Supongamos que $N \neq B$.

$$\begin{aligned} N \neq B &\Longrightarrow 1 \notin N \wedge 0 \in N \\ &\Longrightarrow M = N \end{aligned}$$

Por lo cual, se ha probado que el ideal trivial es maximal en el álgebra $\{0,1\}$. ■

Hasta este punto se ha definido en un álgebra booleana B un ideal booleano, ahora se define su dual el cual se denota como $\mathcal{F}$ y se tiene que $\mathcal{F}$ es un subconjunto de B al cual se le llama filtro.

Dado un filtro $\mathcal{F}$ en un álgebra booleana, se define el ideal dual de $\mathcal{F}$ como el conjunto $M_{\mathcal{F}} = \{a \in B | a' \in \mathcal{F}\}$. Análogamente, dado un ideal M en B, se define el filtro dual de M como el conjunto $\mathcal{F}_M = \{a \in B | a' \in M\}$.

Así, el dual de un ideal booleano se define a continuación:

Definición 2.5 *Sea $\mathcal{F}$ un subconjunto del álgebra booleana B. Se dice que $\mathcal{F}$ es un filtro booleano de B si se satisfacen:*

1. $1 \in \mathcal{F}$
2. *Si* $p, q \in \mathcal{F}$, *entonces* $p \wedge q \in \mathcal{F}$
3. *Si* $p \in \mathcal{F}$ *y* $q \in B$, *entonces* $p \vee q \in \mathcal{F}$

Observaciones 2.3 *La condición* 3 *se puede reemplazar por: si* $a \in \mathcal{F}$ *y* $b \geq a$, *entonces* $b \in \mathcal{F}$.

La Definición 2.5 la llevamos a un caso particular del álgebra booleana. Sea X un subconjunto arbitrario; consideremos el álgebra booleana generada por $\mathbb{P}(X)$, donde se denota la suma como unión, el producto como intersección y $(')$ como el complemento.

Definición 2.6 *Un ideal en* $\mathbb{P}(X)$ *es un conjunto* $M \subset \mathbb{P}(X)$ *tal que:*

1. $\emptyset \in \mathcal{F}$
2. $\forall A, B \in M$, $A \cup B \in M$
3. $\forall A \in M$, $\forall B \in \mathbb{P}(X)$, $A \cap B \in M$

Dualizando se tiene la siguiente definición de filtro como dual de un ideal booleano.

Definición 2.7 *Un filtro en* $\mathbb{P}(X)$ *es un conjunto* $\mathcal{F} \subset \mathbb{P}(X)$ *tal que:*

1. $X \in \mathcal{F}$
2. $\forall A, B \in \mathcal{F}$, $A \cap B \in \mathcal{F}$
3. $\forall A \in \mathcal{F}$, $\forall B \in \mathbb{P}(X)$, $A \cup B \in \mathcal{F}$

Definición 2.8 *Si X es un conjunto no vacío, un filtro $\mathcal{F}$ sobre X es una subcolección no vacía de subconjuntos de X tales que:*

1. $\emptyset \notin \mathcal{F}$
2. *$\mathcal{F}$ es cerrado bajo intersecciones finitas.*
3. $(\forall P, Q)(P \in \mathcal{F} \wedge Q \in \mathbb{P}(X) \wedge P \subseteq Q)$, $Q \in \mathcal{F}$.

Probemos que la Definición 2.8 y la Definición 2.7 son equivalentes:

Prueba.

1. Probamos la equivalencia de la propiedad 1.

   Un ideal propio (no trivial) no debe contener a X (X es neutro multiplicativo), porque si lo contiene, el ideal M contendría a $\mathbb{P}(X)$. Por lo cual $X \notin M$ y por dualidad, $\emptyset \notin \mathcal{F}$. Recíprocamente, la condición 3 de 2.8 implica que $X \in \mathcal{F}$ en 2.8.

2. Probamos la equivalencia de la propiedad 3.

   Definición de filtro como dual de un ideal implica definición 2.8.

   Si $P \subseteq Q$, entonces $P \cup Q = Q$ y como $P \cup Q \in \mathcal{F}$ por hipótesis, entonces $Q \in \mathcal{F}$.

   Definición 2.8 implica definición de filtro como dual de un ideal.

   $\forall P \in \mathcal{F} \wedge \forall Q \in \mathbb{P}(X), P \cup Q \in \mathcal{F}$.

   $$P \subset P \cup Q \Longrightarrow P \in \mathcal{F}$$

   Por lo cual, $P \subset Q \in \mathcal{F}$.

Por lo cual se ha probado que la Definición 2.8 y la Definición 2.7 son equivalentes. ■

Ejemplo 2.4 $\{1\}$ *es el filtro trivial.*

Definición 2.9 *Sean F_1 y F_2 dos filtros, diremos que F_1 es mas fino que F_2 si $\mathcal{F} \in F_2$, implica que $\mathcal{F} \in F_1$.*

Los ideales y los filtros no son las únicas subestructuras de una álgebra booleana. De hecho, existe una más natural, la de subálgebra:

Definición 2.10 *Sea A una álgebra booleana y $B \subset A$. Se dice que B es una subálgebra de A si B es no vació y B es cerrado bajo las operaciones. Es decir:*

1. *Si $a, b \in B$, entonces $a \vee b \in B$.*

2. *Si $a, b \in B$, entonces $a \wedge b \in B$.*

3. *Si $a \in B$, entonces $a' \in B$.*

Ejemplo 2.5 *Demuestre que toda subálgebra de una álgebra booleana contiene al conjunto $\{0, 1\}$.*

Prueba.

Sea A un álgebra booleana y sea $B \subset A$ una subálgebra que satisface las condiciones de la Definición 2.10.

Se quiere probar que $\{0, 1\} \subset B$.

Como B es una subálgebra se tiene que si $a \in B$ y $a^{'} \in B$ por inciso 3, entonces $a \vee a^{'} \in B$ por inciso 1 y $a \wedge a^{'} \in B$ por inciso 2. Así,

$$
\begin{aligned}
a \vee a^{'} \in B &\Longrightarrow a \vee a^{'} = 1 \\
&\Longrightarrow 1 \in B
\end{aligned}
\qquad\qquad
\begin{aligned}
a \wedge a^{'} \in B &\Longrightarrow a \wedge a^{'} = 0 \\
&\Longrightarrow 0 \in B
\end{aligned}
$$

Por lo cual, se puede concluir que $\{0, 1\}$ está contenido en toda subálgebra. $\blacksquare$

2.2. Homomorfismos entre álgebras booleanas

Definición 2.11 *Sean A y B álgebras booleanas . Un homomorfismo booleano es una aplicación $f : A \longrightarrow B$ que es compatible con las operaciones de disyunción, conjunción y completamentación de ambas álgebras, es decir, la aplicación $f : A \longrightarrow B$ satisface que:*

1. $f(p \vee q) = f(p) \vee f(q)$,
2. $f(p \wedge q) = f(p) \wedge f(q)$,
3. $f(p') = (f(p))'$.

para cualesquiera $p, q \in A$.

Definición 2.12 *Un homomorfismo booleano $f : A \longrightarrow B$ se dice monomorfismo si $f(p) = f(q)$, implica que $p = q$, es decir, si f es inyectiva. Si f es sobreyectiva, entonces decimos que f es un epimorfismo y si $f$es biyectiva decimos que f es un isomorfismo. Si $B = A$ decimos que f es un endomorfismo y por último, f es un automorfismo si es endomorfismo e isomorfismo a la vez . Si existe un isomorfismo entre A y B entonces A y B son llamadas álgebras booleanas isomorfas. Denotaremos que A y B son isomorfas escribiendo $A \cong B$*

Al igual que en las álgebras booleanas, los elementos distinguidos también juegan un rol importante en los homomorfismos booleanos. Ciertamente, todo homomorfismo booleano preserva elementos distinguidos. En efecto, sea $f : A \longrightarrow B$ un homomorfismo booleano, entonces

$$f(0) = f(p \wedge p^{'}) = f(p) \wedge f(p^{'}) = f(p) \wedge (f(p))^{'} = 0$$

y

$$f(1) = f(p \vee p^{'}) = f(p) \vee f(p^{'}) = f(p) \vee (f(p))^{'} = 1.$$

Lema 2.1 *Sean A y B álgebras booleanas. La aplicación $f : A \longrightarrow B$ tal que para todo $p \in A$, $f(p) = 0$, no es un homomorfismo booleano. En otras palabras, en la teoría de álgebras booleanas no existe un homomorfismo trivial.*

Prueba.

Razonando por contradicción.

Supongamos que la aplicación $f : A \longrightarrow B$ es un homomorfismo booleano, tal que para todo $p \in A$, $f(p) = 0$. Entonces

$$1 = f(p) \vee (f(p))' = f(p \vee p') = 0,$$

con lo cual $1 = 0$, pero esta es una contradicción, pues en un álgebra booleana los elementos distinguidos deben ser diferentes. Por lo tanto, no existe un homomorfismo trivial. ■

Definición 2.13 *Sea $f : A \longrightarrow B$ un homomorfismo booleano. Definimos el $ker(f)$, $Im(f)$ y $Sh(f)$ como los conjuntos*

$$ker(f) := \{p \in A : f(p) = 0\},$$

$$Im(f) := \{f(p) : p \in A\},$$

$$Sh(f) := \{p \in A : f(p) = 1\}.$$

Respectivamente.

Los homomorfismos booleanos también preservan las operaciones de suma, diferencia, producto e implicación, como se muestra en el siguiente resultado.

Teorema 2.5 *Sea $f : A \longrightarrow B$ un homomorfismo booleano, entonces para $p, q \in A$ tenemos*

1. $f(p + q) = f(p) + f(q)$,

2. $f(p \Longrightarrow q) = f(p) \Longrightarrow f(q)$,

3. $f(p - q) = f(p) - f(q)$,

4. $f(p \cdot q) = f(p) \cdot f(q)$.

Prueba.

Probaremos únicamente el inciso 1), la prueba para los demás incisos es análoga.

Sea $p, q \in A$,

$$\begin{aligned} f(p+q) &= f((p \wedge q') \vee (p' \wedge q)) \\ &= f(p \wedge q') \vee f(p' \wedge q) \\ &= (f(p) \wedge f(q')) \vee (f(p') \wedge f(q)) \\ &= (f(p) \wedge (f(q))') \vee ((f(p))' \wedge f(q)) \\ &= f(p) + f(q). \end{aligned}$$

■

Proposición 2.3 *Sea $f : A \longrightarrow B$ un homomorfismo booleano, entonces:*

1. *El kernel de f es un ideal booleano en A.*

2. *f es monomorfismo, si y sólo si, $ker(f) = \{0\}$.*

3. *$f(A)$ es subálgebra booleana de B.*

Prueba.

1. Probaremos que $ker(f)$ es un ideal booleano de A.

   a) Probando que $0 \in ker(f)$.

   Por hipótesis $0 \in A$, luego $f(0) = 0$, entonces $0 \in ker(f)$.

b) Probando la segunda condición de ideal booleano.

Sea $p, q \in ker(f)$.

$p \in ker(f) \Rightarrow f(p) = 0$, $q \in ker(f) \Rightarrow f(q) = 0$, luego

$f(p \vee q) = f(p) \vee f(q) = 0 \vee 0 = 0$.

Por lo tanto si $p, q \in ker(f)$, entonces $p \vee q \in ker(f)$.

c) Probando la tercera condición de ideal booleano.

Sea $p \in ker(f)$ y $q \in A$.

$f(p \wedge q) = f(p) \wedge f(q) = 0 \wedge f(q) = 0$.

Por lo tanto, si $p \in ker(f)$ y $q \in A$, entonces $p \wedge q \in ker(f)$.

Por lo tanto, $ker(f)$ es un ideal booleano.

2. f es monomorfismo, si y sólo si, $ker(f) = \{0\}$.

" $\Longrightarrow$ "
Sea $p \in ker(f)$,

$$\begin{aligned} p \in ker(f) &\Longrightarrow f(p) = 0 \\ &\Longrightarrow f(p) = f(0) \\ &\Longrightarrow p = 0 \\ &\Longrightarrow ker(f) = \{0\}. \end{aligned}$$

Por lo tanto, $ker(f) = \{0\}$.
" $\Longleftarrow$ "
Sea $p, q \in A$ tal que $f(p) = f(q)$. Haciendo uso del teorema 2.5 inciso 3) tenemos:

$$\begin{aligned} f(p) = f(q) &\Longrightarrow f(p - q) = 0 \\ &\Longrightarrow p - q \in ker(f) \\ &\Longrightarrow p - q = 0 \\ &\Longrightarrow p = q. \end{aligned}$$

Por lo tanto, f es monomorfismo.

3. Probaremos que $f(A)$ es subálgebra booleana de B.

   Se tiene que $f(A) = \{b \in B, b = f(a) | a \in A\}$.

   a) Probamos que $f(A)$ no es vacío.

   Sea $0 \in A$.

$$\begin{aligned} 0 \in A &\Longrightarrow f(0) = 0 \\ &\Longrightarrow 0 \in f(A), \text{ por se homomorfismo} \end{aligned}$$

   Así, $f(A) \neq \emptyset$.

   b) Probamos que se cumple la condición 1 de subálgebra.

   Sean $b_1, b_2 \in f(A)$,

$$\begin{aligned} b_1, b_2 \in f(A) &\Longrightarrow \exists a_1, a_2 \in A / f(a_1) = b_1 \ y \ f(a_2) = b_2 \\ &\Longrightarrow b_1 \vee b_2 = f(a_1) \vee f(a_2) \\ &\Longrightarrow b_1 \vee b_2 = f(a_1 \vee a_2), \text{ pero } a_1 \vee a_2 \in A \\ &\Longrightarrow \exists a_1 \vee a_2 \in A / b_1 \vee b_2 = f(a_1 \vee a_2) \in f(A) \\ &\Longrightarrow b_1 \vee b_2 \in f(A). \end{aligned}$$

   c) Probamos que se cumple la condición 2 de subálgebra.

   Sean $b_1, b_2 \in f(A)$,

$$\begin{aligned} b_1, b_2 \in f(A) &\Longrightarrow \exists a_1, a_2 \in A / f(a_1) = b_1 \ y \ f(a_2) = b_2 \\ &\Longrightarrow b_1 \wedge b_2 = f(a_1) \wedge f(a_2) \\ &\Longrightarrow b_1 \wedge b_2 = f(a_1 \wedge a_2), \text{ pero } a_1 \wedge a_2 \in A \\ &\Longrightarrow \exists a_1 \wedge a_2 \in A / b_1 \wedge b_2 = f(a_1 \wedge a_2) \in f(A) \\ &\Longrightarrow b_1 \wedge b_2 \in f(A). \end{aligned}$$

d) Probamos que se cumple la condición 3 de subálgebra.

Sea $b \in f(A)$,

$$\begin{aligned} b \in f(A) &\Longrightarrow \exists a \in A / b = f(a) \\ &\Longrightarrow \neg b = \neg f(a) \\ &\Longrightarrow \neg b = f(\neg a), \neg a \in A \\ &\Longrightarrow \neg b \in f(A). \end{aligned}$$

Por lo cual, podemos concluir que $f(A)$ es subálgebra de B. ■

Procederemos a considerar algunos ejemplos de homomorfismos booleano:

Ejemplo 2.6 *Sea A un álgebra booleana arbitraria y sea $a_0 \neq 0$ un elemento arbitrario de A. Sobre el conjunto B de todos los subelementos de a_0 (esto significa los elementos a con $a \leq a_0$), puede construirse un álgebra booleana como sigue: el 0, la suma y producto en B son los mismos de A, pero el 1 y $a^{'}$ en B se definen como sigue:*

$$1 := a_0 \quad y \quad a^{'} := a_0 - a$$

para $a, a_0 \in A$. El mapeo $f : A \longrightarrow B : a \longmapsto a \cdot a_0$ es un homomorfismo booleano.

Prueba.

1. Sean $x, y \in A$,

$$\begin{aligned} f(x+y) &= (x+y) \cdot a_0 \\ &= (x \cdot a_0) + (y \cdot a_0) \\ &= f(x) + f(y). \end{aligned}$$

   Por lo cual, $f(x+y) = f(x) + f(y)$.

2. Sean $x, y \in A$,

$$
\begin{aligned}
f(x) \cdot f(y) &= (x \cdot a_0) \cdot (y \cdot a_0) \\
&= (x \cdot y) \cdot (a_0 \cdot a_0) \\
&= (x \cdot y) \cdot a_0 \\
&= f(x \cdot y).
\end{aligned}
$$

   Por lo cual, $f(x \cdot y) = f(x) \cdot f(y)$.

3. Sea $x \in A$,

$$
\begin{aligned}
(f(x))^{'} &= (x \cdot a_0)^{'} \\
&= a_0 - x \cdot a_0 \\
&= a_0 - x \\
&= x^{'} \\
&= x^{'} \cdot a_0 \\
&= f(x^{'}).
\end{aligned}
$$

   Por lo cual, $f(x^{'}) = (f(x))^{'}$.

Por lo cual, $f : A \longrightarrow B : a \longrightarrow a \cdot a_0$ es un homomorfismo de álgebras booleanas ■

Ejemplo 2.7 *Sea ϕ un mapeo arbitrario de un conjunto no vacío X en un conjunto Y, y sean A y B campos de subconjuntos de X e Y respectivamente. Sea $f = \phi^{-1}$, o explícitamente, para cada P en B, sea $f(P)$ la imagen inversa de P. En general el conjunto $f(P)$ no pertenecerá al campo A. Si $f(P) \in A$ siempre que $P \in B$, entonces f es un homomorfismo de B en A.*

Prueba.

1. Sean $P, Q \in B$.

Queremos probar que :

$$f(P\cup Q)=f(P)\cup f(Q)$$
$$f(P\cup Q)=\phi^{-1}(P\cup Q)=\phi^{-1}(P)\cup\phi^{-1}(Q)$$

Sea $x\in\phi^{-1}(P\cup Q)$.

$$\begin{aligned}x\in\phi^{-1}(P\cup Q)&\Longleftrightarrow\phi(x)\in P\cup Q\\&\Longleftrightarrow\phi(x)\in P\ o\ \phi(x)\in Q\\&\Longleftrightarrow x\in\phi^{-1}(P)\ o\ x\in\phi^{-1}(Q)\\&\Longleftrightarrow x\in\phi^{-1}(P)\cup\phi^{-1}(Q)\end{aligned}$$

Luego, $f(P\cup Q)=f(P)\cup f(Q)$.

2. Sean $P,Q\in B$.

   Queremos probar que :

$$f(P\cap Q)=f(P)\cap f(Q)$$
$$f(P\cap Q)=\phi^{-1}(P\cap Q)=\phi^{-1}(P)\cap\phi^{-1}(Q)$$

Sea $x\in\phi^{-1}(P\cap Q)$.

$$\begin{aligned}x\in\phi^{-1}(P\cap Q)&\Longleftrightarrow\phi(x)\in P\cap Q\\&\Longleftrightarrow\phi(x)\in P\ y\ \phi(x)\in Q\\&\Longleftrightarrow x\in\phi^{-1}(P)\ y\ x\in\phi^{-1}(Q)\\&\Longleftrightarrow x\in\phi^{-1}(P)\cap\phi^{-1}(Q)\end{aligned}$$

Así, $f(P\cap Q)=f(P)\cap f(Q)$.

3. Sea $P \in B$.

   Queremos probar que :

$$f(P^{'}) = (f(P))^{'}$$
$$f(P^{'}) = \phi^{-1}(P^{'}) = (\phi^{-1}(P))^{'}$$

   Sea $x \in \phi^{-1}(P^{'})$.

$$\begin{aligned} x \in \phi^{-1}(P^{'}) &\Longleftrightarrow \phi(x) \in P^{'} \\ &\Longleftrightarrow \phi(x) \notin P \\ &\Longleftrightarrow x \notin \phi^{-1}(P) \\ &\Longleftrightarrow x \in (\phi^{-1}(P))^{'} \end{aligned}$$

Así, $f(P^{'}) = (f(P))^{'}$. Por lo tanto, $f : B \longrightarrow A$ es un homomorfismo booleano. ■

Llamaremos al homomorfismo descrito en estos ejemplos, homomorfismo inducido por a_0 y ϕ respectivamente.

Ejemplo 2.8 *Para cualquier álgebra booleana A existe un único homomorfismo booleano*

$$f : \mathbb{Z}_2 \longrightarrow A : p \longmapsto f(p) = \begin{cases} 1 & si\ p = 1, \\ 0 & si\ p = 0 \end{cases}$$

Prueba.

Sean $p, q \in \mathbb{Z}_2$.

Para la demostración consideraremos los siguientes casos:

Caso 1: $p = 0$ y $q = 0$.

a) $f(0 \vee 0) = f(0) = 0 = 0 \vee 0 = f(0) \vee f(0)$.

b) $f(0 \wedge 0) = f(0) = 0 = 0 \wedge 0 = f(0) \wedge f(0)$.

c) $f(0^{'}) = f(1) = 1 = (f(0))^{'}$.

Caso 2: $p = 1$ y $q = 1$.

a) $f(1 \vee 1) = f(1) = 1 = 1 \vee 1 = f(1) \vee f(1)$.

b) $f(1 \wedge 1) = f(1) = 1 = 1 \wedge 1 = f(1) \wedge f(1)$.

c) $f(1^{'}) = f(0) = 0 = (f(1))^{'}$.

Caso 3: $p = 1$ y $q = 0$.

a) $f(1 \vee 0) = f(1) = 1 = 1 \vee 0 = f(1) \vee f(0)$.

b) $f(1 \wedge 0) = f(0) = 0 = 1 \wedge 0 = f(1) \wedge f(0)$.

c) $f(0^{'}) = f(1) = 1 = (f(0))^{'}$,

$f(1^{'}) = f(0) = 0 = (f(1))^{'}$.

Por último probemos que f es único.

Supongamos que existe g tal que:

$$g : \mathbb{Z}_2 \longrightarrow A : p \longmapsto g(p) = \begin{cases} 1 & \text{si } p = 1, \\ 0 & \text{si } p = 0 \end{cases}$$

Sea $p \in \mathbb{Z}_2$,

Si $p = 0$, entonces $g(0) = 0 = f(0)$, luego $g = f$.

Si $p = 1$. entonces $g(1) = 1 = f(1)$, luego $g = f$.

En todo caso $g = f$, Por lo tanto $f : \mathbb{Z}_2 \longrightarrow A$ es un homomorfismo booleano único. ■

Proposición 2.4 *Sean $f : A \longrightarrow B$ y $g : B \longrightarrow C$ homomorfismos de álgebras booleanas. Entonces $g \circ f$ es un homomorfismo de álgebras booleanas.*

Prueba. Sea $p, q \in A$,

1.

$$\begin{aligned}(g \circ f)(p \vee q) &= g(f(p \vee q)) \\ &= g(f(p) \vee f(q)) \\ &= g(f(p)) \vee g(f(q)) \\ &= (g \circ f)(p) \vee (g \circ f)(q).\end{aligned}$$

2.

$$\begin{aligned}(g \circ f)(p \wedge q) &= g(f(p \wedge q)) \\ &= g(f(p) \wedge f(q)) \\ &= g(f(p)) \wedge g(f(q)) \\ &= (g \circ f)(p) \wedge (g \circ f)(q).\end{aligned}$$

3.

$$\begin{aligned}(g \circ f)(p^{'}) &= g(f(p^{'})) \\ &= g((f(p))^{'}) = (g(f(P)))^{'} \\ &= ((g \circ f)(p))^{'}.\end{aligned}$$

Por lo tanto, $g \circ f$ es un homomorfismo booleano. ∎

Teorema 2.6 *(Primer teorema de homomorfismos booleanos). Todo ideal booleano propio es el kernel de algún epimorfismo booleano.*

Prueba.

Sea B un álgebra booleana, por el teorema de conexión 1.6, B también tiene estructura de anillo booleano. Si $M \subset B$ es un ideal propio de B, entonces el cociente B/M tiene estructura de anillo con las siguientes operaciones, para $\overline{p}, \overline{q} \in B/M$,

$$\overline{p} \oplus \overline{q} := \overline{p+q},$$

$$\overline{p} \odot \overline{q} := \overline{p \cdot q}.$$

Donde $p, q \in B$ y $+, \cdot$ son las operaciones de suma y producto en el anillo booleanos B. Más aún, con las operaciones $(B/M; \oplus; \odot)$, es un anillo con unidad en el que todos sus elementos son idempotentes, es decir, es un anillo booleano.

Definimos la aplicación $\varphi : B \longrightarrow B/M$, dada por $\varphi(p) = \overline{p}$ para cada $p \in B$.

Probemos que φ está bien definida.

Sean $p, q \in B$ tal que $p = q$,

$$\varphi(p) = \overline{p} = \overline{q} = \varphi(q).$$

Por tanto, φ está bien definida.

Probemos si φ es un homomorfismo de anillos

Sea $p, q \in B$,

$$\begin{aligned} \varphi(p+q) &= \overline{p+q} \\ &= \overline{p} \oplus \overline{q} \\ &= \varphi(p) \oplus \varphi(q) \end{aligned} \qquad \begin{aligned} \varphi(p \cdot q) &= \overline{p \cdot q} \\ &= \overline{p} \odot \overline{q} \\ &= \varphi(p) \odot \varphi(q) \end{aligned}$$

Por lo tanto, φ es un homomorfismo de anillos. Probemos si φ es un epimorfismo.

Sea $\overline{p} \in B/M$,

$\overline{p} \in B/M \Longrightarrow \exists p \in B$ tal que $\varphi(p) = \overline{p}$.

Por lo tanto, φ es un epimorfismo

Nuevamente, por el teorema de conexión 1.6, B/M tiene estructura de álgebra booleana.

Finalmente probemos si φ es un homomorfismo booleano.

1. Sea $p, q \in B$,

$$\begin{aligned}\varphi(p \vee q) &= \varphi(p + q + (p \cdot q)) \\ &= \overline{p} \oplus \overline{q} \oplus (\overline{p} \odot \overline{q}) \\ &= \varphi(p) \oplus \varphi(q) \oplus (\varphi(p) \odot \varphi(q)) \\ &= \varphi(p) \vee \varphi(q).\end{aligned}$$

2. Sea $p, q \in B$,

$$\begin{aligned}\varphi(p \wedge q) &= \varphi(p \cdot q) \\ &= \varphi(p) \odot \varphi(q) \\ &= \varphi(p) \wedge \varphi(q).\end{aligned}$$

3. Sea $p, p^{'} \in B$,

$$\begin{aligned}\varphi(p^{'}) &= \varphi(1 + p) \ por \ 1{,}26 \\ &= \overline{1} \oplus \varphi(p) \\ &= (\varphi(p))^{'}.\end{aligned}$$

Por lo tanto φ es un homomorfismo booleano, con lo cual φ es un epimorfismo booleano. Por último, la igualdad $M = ker(\varphi)$ es consecuencia inmediata de la definición de φ. ■

El álgebra booleana B/M es usualmente llamada el cociente de B módulo M.

Lema 2.2 *Cada ideal booleano maximal es el kernel de algún homomorfismo booleano.*

Prueba.

Sea M un ideal booleano maximal, entonces se quiere probar que $M \simeq ker(\varphi)$.

Para realizar la prueba se hace uso del Teorema 2.6.

En el Teorema 2.6 M es un ideal propio, haciendo uso de ello tenemos que como todo ideal booleano propio es el kernel de algún epimorfismo booleano y todo ideal maximal es propio, entonces M es un ideal maximal y un ideal propio.

Ahora, para realizar la prueba usamos la aplicación

$$\varphi : B \longrightarrow B/M,$$

definida por:

$$x \mapsto x + M.$$

1. Probamos que $M \subset ker(\varphi)$.

   Sea $x \in M$.

$$\begin{aligned} x \in M &\Longrightarrow \varphi(x) = x + M = M = 0 \in B/M \\ &\Longrightarrow x \in ker(\varphi) \end{aligned}$$

2. Probamos que $ker(\varphi) \subset M$.

   Sea $x \in ker(\varphi)$.

$$\begin{aligned} x \in ker(\varphi) &\Longrightarrow \varphi(x) = M \\ &\Longrightarrow x + M = M \\ &\Longrightarrow x \in M \end{aligned}$$

■

El álgebra booleana B/M es usualmente llamada el cociente de B módulo M.

Teorema 2.7 *(Segundo teorema fundamental de homomorfismos booleanos). Sean B, B' dos álgebras booleanas y $\varphi : B \longrightarrow B'$un homomorfismo booleano, entonces $\varphi(B) \equiv B/ker(\varphi)$.*

En otras palabras, $\varphi(B)$ es isomorfa al cociente de B módulo $ker(\varphi)$.

Prueba. Debemos encontrar un isomorfismo booleano Ψ, tal que el diagrama sea conmutativo:

$$\begin{tikzcd} B \arrow[r, "f"] \arrow[dr, "\pi"'] & \varphi(B) \\ & B/ker(\varphi) \arrow[u, dashed, "\Psi"'] \end{tikzcd}$$

La aplicación $\Psi : B/ker(\varphi) \longrightarrow \varphi(B)$ se define para cada $\overline{p} \in B/ker(\varphi)$ como $\Psi(\overline{p}) = \varphi(p)$. Por el teorema de conexión 1.6, B, $\varphi(B)$ y $B/ker(\varphi)$ tienen estructura de anillos booleanos, por ello podemos demostrar este teorema a partir de la teoría de anillos. Probemos que, Ψ es un isomorfismo de anillos, para ello probaremos lo siguiente :

1. Está bien definida.
2. Es un homomorfismo de anillos.
3. Es sobreyectiva.
4. Es inyectiva.

1. Probamos que Ψ está bien definida.

   Sean $\overline{p}, \overline{q} \in B/ker(\varphi)$ tal que $\overline{p} = \overline{q}$,

$$\begin{aligned} \overline{p} = \overline{q} &\Rightarrow \overline{p+q} = \overline{0} \\ &\Rightarrow p+q \in ker(\varphi) \\ &\Rightarrow \varphi(p+q) = 0_{B'} \\ &\Rightarrow \varphi(p) + \varphi(q) = 0_{B'} \\ &\Rightarrow \varphi(p) = \varphi(q) \\ &\Rightarrow \Psi(\overline{p}) = \Psi(\overline{q}). \end{aligned}$$

   Por lo tanto, Ψ está bien definida.

2. Probemos que es un homomorfismo de anillos.

   Sean $\overline{p}, \overline{q} \in B/ker(\varphi)$,

   a) $\Psi(\overline{p} \oplus \overline{q}) = \Psi(\overline{p+q}) = \varphi(p+q) = \varphi(p) + \varphi(q) = \Psi(\overline{p}) + \Psi(\overline{q})$,

   b) $\Psi(\overline{p} \odot \overline{q}) = \Psi(\overline{p \cdot q}) = \varphi(p \cdot q) = \varphi(p) \cdot \varphi(q) = \Psi(\overline{p}) \cdot \Psi(\overline{q})$.

   Por lo tanto, Ψ es un homomorfismo de anillos.

3. Probemos que es sobreyectiva.

   Sea $p \in \varphi(B)$,

$$
\begin{aligned}
p \in \varphi(B) &\Rightarrow \exists q \in B \text{ tal que} p = \varphi(q) \\
&\Rightarrow p = \varphi(q) = \Psi(\overline{q}) \\
&\Rightarrow p = \Psi(\overline{q}).
\end{aligned}
$$

   Por lo tanto, Ψ es sobreyectiva.

4. Probemos que es inyectiva.

   Sea $\overline{p}, \overline{q} \in B/ker(\varphi)$ tal que $\Psi(\overline{p}) = \Psi(\overline{q})$,

$$
\begin{aligned}
\Psi(\overline{p}) = \Psi(\overline{q}) &\Longrightarrow \varphi(p) = \varphi(q) \\
&\Longrightarrow \varphi(p) + \varphi(q) = 0_{B'} \\
&\Longrightarrow \varphi(p+q) = 0_{B'} \\
&\Longrightarrow p + q \in ker(\varphi) \\
&\Longrightarrow \overline{p+q} = \overline{0} \\
&\Longrightarrow \overline{p} + \overline{q} = \overline{0} \\
&\Longrightarrow \overline{p} = \overline{q}.
\end{aligned}
$$

   Por lo tanto Ψ es inyectiva, con lo que hemos probado que Ψ es un isomorfismo de anillos. Por último demostraremos que Ψ es un isomorfismo de álgebras booleanas, para ello utilizaremos el teorema de conexión.

Es claro que $B/ker(\varphi)$ y $\varphi(B)$ son anillos booleanos, así por el teorema de conexión ambos tienen estructura de álgebras booleanas, sólo falta probar que Ψ es un homomorfismo booleano.

1. Sea $\overline{p}, \overline{q} \in B/ker(\varphi)$,

$$
\begin{aligned}
\Psi(\overline{p} \vee \overline{q}) &= \Psi(\overline{p} + \overline{q} + (\overline{p} \cdot \overline{q})) \\
&= \Psi(\overline{p+q} + (\overline{p \cdot q})) \\
&= \Psi(\overline{p+q+(p \cdot q)}) \\
&= \varphi(p+q+(p \cdot q)) \\
&= \varphi(p+q) + \varphi(p \cdot q) \\
&= \varphi(p) + \varphi(q) + (\varphi(p) \cdot \varphi(q)) \\
&= \varphi(p) \vee \varphi(q) \\
&= \Psi(\overline{p}) \vee \Psi(\overline{q}).
\end{aligned}
$$

2. Sea $\overline{p}, \overline{q} \in B/ker(\varphi)$,

$$
\begin{aligned}
\Psi(\overline{p} \wedge \overline{q}) &= \Psi(\overline{p} \cdot \overline{q}) \\
&= \Psi(\overline{p \cdot q}) \\
&= \varphi(p \cdot q) \\
&= \varphi(p) \cdot \varphi(q) \\
&= \Psi(\overline{p}) \wedge \Psi(\overline{q}).
\end{aligned}
$$

3. Sea $\overline{p} \in B/ker(\varphi)$,

$$
\begin{aligned}
(\Psi(\overline{p}))' &= (\varphi(p))', \\
&= \varphi(p'), \\
&= \Psi(\overline{p'}) \\
&= \Psi(\overline{p}').
\end{aligned}
$$

Así, Ψ es un isomorfismo booleano

Por lo cual, se puede concluir que $\varphi(B) \equiv B/ker(\varphi)$. ■

Definición 2.14 *Un homomorfismo f es llamado completo en caso de que preserve todo supremo y consecuentemente todo ínfimo. Esto significa que si a_i es una familia de elementos en el dominio de f con supremo a, la familia $f(a_i)$ tiene un supremo y este supremo es igual a $f(a)$.*

2.3. Homomorfismos entre anillos booleanos

Definición 2.15 *Sean A y B dos anillos booleanos. Un homomorfismo de anillos booleanos de A en B es un mapeo $f : A \longrightarrow B$ tal que: $\forall x, y \in A$,*

1. $f(x + y) = f(x) + f(y)$.
2. $f(x \cdot y) = f(x) \cdot f(y)$.
3. $f(-x) = -f(x)$.
4. $f(0) = 0$.
5. $f(1) = 1$.

Observaciones 2.4 *A los homomorfismos de un anillo booleano en sí mismo los denominamos endomorfismos.*

El siguiente resultado es una consecuencia inmediata del teorema 2.5.

Corolario 2.3 *Todo homomorfismo booleano es un homomorfismo entre anillos booleanos, y viceversa, todo homomorfismo entre anillos booleanos es un homomorfismo booleano.Además, todo homomorfismo booleano preserva el orden, es decir,si $p \leq q$, entonces $f(p) \leq f(q)$.*

Prueba. Sea $f : A \longrightarrow B$ un homomorfismo booleano, probaremos que f es un homomorfismo de anillos booleanos. Aplicando el teorema 2.5 tenemos:

1. Sea $p, q \in A$,

$$f(p+q) = f(p) + f(q).$$

2. Sea $p, q \in A$,

$$f(p \cdot q) = f(p) \cdot f(q).$$

3. Sea $p \in A$,

$$\begin{aligned} f(-p) &= f(0-p) \\ &= f(0 \wedge p') \\ &= f(0) \wedge f(p') \\ &= f(0) \wedge (f(p))' \\ &= f(0) - f(p) \\ &= -f(p). \end{aligned}$$

Ahora, supongamos que $f : A \longrightarrow B$ es un homomorfismo de anillos booleanos y probemos que f es un homomorfismo booleano. Nuevamente haremos uso del teorema 2.5.

1. Sea $p, q \in A$,

$$\begin{aligned} f(p \vee q) &= f(p + q + (p \cdot q)) \\ &= f(p + q) + (f(p \cdot q)) \\ &= (f(p) + f(q)) \vee (f(p) \cdot f(q)) \\ &= f(p) \vee f(q). \end{aligned}$$

2. Sea $p, q \in A$,

$$\begin{aligned} f(p \wedge q) &= f(p \cdot q) \\ &= f(p) \cdot f(q) \\ &= f(p) \wedge f(q). \end{aligned}$$

3. Sea $p \in A$,

$$\begin{aligned} f(p^{'}) &= f(1 + p) \\ &= f(1) + f(p) \\ &= 1 + f(p) \\ &= (f(p))^{'}. \end{aligned}$$

Por lo tanto, todo homomorfismo booleano es un homomorfismo entre anillos booleanos, y viceversa, todo homomorfismo entre anillos booleanos es un homomorfismo booleano.

Por último probemos que si $p \leq q$, entonces $f(p) \leq f(q)$.

Sea $p \leq q$,

$$\begin{aligned} p \leq q &\Longrightarrow p \wedge q = p, \\ &\Longrightarrow f(p \wedge q) = f(p), \\ &\Longrightarrow f(p) \wedge f(q) = f(p), \\ &\Longrightarrow f(p) \leq f(q). \end{aligned}$$

Por lo tanto si $p \leq q$, entonces $f(p) \leq f(q)$. ■

2.4. Cociente de anillos booleanos

Sea $\mathcal{F}$ un filtro e I un ideal, definimos las siguientes relaciones de equivalencia:

$x \sim_{\mathcal{F}} y \Longleftrightarrow \exists\ f \in \mathcal{F}$ tal que $x \wedge f = y \wedge f$; y

$x \sim_I y \Longleftrightarrow \exists\ i \in I$ tal que $x \vee i = y \vee i$..

Solo demostraremos que $\sim_I$ es una relación de equivalencia, la demostración para $\sim_{\mathcal{F}}$ es dual.

Sea A un álgebra booleana y $x, y, z \in A$.

1. Reflexiva.

   Sea $i = 0 \in I$ tales que $x \vee i = x \vee i$, entonces $x \sim_I x$.

2. Simétrica.

   Supongamos que $x \sim_I y$.

$$\begin{aligned} x \sim_I y &\Longrightarrow \exists i \in I \text{ tales que } x \vee i = y \vee i \\ &\Longrightarrow y \vee i = x \vee i \\ &\Longrightarrow y \sim_I x. \end{aligned}$$

3. Transitiva.

   Por hipótesis $x \sim_I y$ y $y \sim_I z$.

$$x \sim_I y \Longrightarrow \exists i \in I \text{ tales que } x \vee i = y \vee i \tag{2.1}$$

$$y \sim_I z \Longrightarrow \exists j \in I \text{ tales que } y \vee j = z \vee j \tag{2.2}$$

   De 2.1, tenemos:

$$\begin{aligned}
x \vee i &= y \vee i \\
(x \vee i) \vee j &= (y \vee i) \vee j \\
x \vee (i \vee j) &= (y \vee j) \vee i \\
x \vee (i \vee j) &= (z \vee j) \vee i \\
x \vee (i \vee j) &= z \vee (j \vee i) \\
x \vee k &= z \vee k \text{ donde } \ k = i \vee j \in I.
\end{aligned}$$

Luego, $\exists k \in I$ tales que $x \vee k = z \vee k$, entonces $x \sim_I z$.

Por lo tanto $\sim_I$ es una relación de equivalencia,

Proposición 2.5 *Las relaciones definidas anteriormente son relaciones de equivalencias. Es decir:*

1. *Si $x \sim_{\mathcal{F}} y$ $(x \sim_I y)$, entonces $x' \sim_{\mathcal{F}} y'$ $(x' \sim_I y')$.*

2. *Si $x_1 \sim_{\mathcal{F}} x_2$ y $y_1 \sim_{\mathcal{F}} y_2$ $(x_1 \sim_I x_2$ y $y_1 \sim_I y_2)$, entonces $x_1 \vee y_1 \sim_{\mathcal{F}} x_2 \vee y_2$ $(x_1 \vee y_1 \sim_I x_2 \vee y_2)$.*

3. *Si $x_1 \sim_{\mathcal{F}} x_2$ y $y_1 \sim_{\mathcal{F}} y_2$ $(x_1 \sim_I x_2$ y $y_1 \sim_I y_2)$, entonces $x_1 \wedge y_1 \sim_{\mathcal{F}} x_2 \vee y_2$ $(x_1 \wedge y_1 \sim_I x_2 \vee y_2)$.*

Prueba.

Se demostrará solo para $\sim_{\mathcal{F}}$, el otro caso es dual.

1. Sean $x, y \in A$ tales que $x \sim_{\mathcal{F}} y$

$$\begin{aligned} x \sim_{\mathcal{F}} y &\Longrightarrow \exists f \in \mathcal{F} \text{ tal que } x \wedge f = y \wedge f \\ &\Longrightarrow (x \wedge f)^{'} = (y \wedge f)^{'} \\ &\Longrightarrow x^{'} \vee f^{'} = y^{'} \vee f^{'} \\ &\Longrightarrow (x^{'} \vee f^{'}) \wedge f = (y^{'} \vee f^{'}) \wedge f \\ &\Longrightarrow (x^{'} \wedge f) \vee (f^{'} \wedge f) = (y^{'} \wedge f) \vee (f^{'} \wedge f) \\ &\Longrightarrow x^{'} \wedge f = y^{'} \wedge f \\ &\Longrightarrow \exists f \in \mathcal{F} \text{ tal que } x^{'} \sim_{\mathcal{F}} y^{'}. \end{aligned}$$

2. Sean $x_1, x_2, y_1, y_2 \in A$ tales que $x_1 \sim_{\mathcal{F}} x_2$ y $y_1 \sim_{\mathcal{F}} y_2$. Entonces existen $f_1, f_2 \in \mathcal{F}$ tales que $x_1 \wedge f_1 = x_2 \wedge f_1$ y $y_1 \wedge f_2 = x_2 \wedge f_2$.

   Entonces,

$$\begin{aligned} (x_1 \vee y_1) \wedge (f_1 \wedge f_2) &= (x_1 \wedge (f_1 \wedge f_2)) \vee (y_1 \wedge (f_1 \wedge f_2)) \\ &= ((x_1 \wedge f_1) \wedge f_2) \vee ((y_1 \wedge f_2) \wedge f_1) \\ &= ((x_2 \wedge f_1) \wedge f_2) \vee ((y_2 \wedge f_2) \wedge f_1) \\ &= (x_2 \vee y_2) \wedge (f_1 \wedge f_2). \end{aligned}$$

   Como $\mathcal{F}$ es filtro $f_1 \wedge f_2 \in \mathcal{F}$ por lo que $x_1 \vee y_1 \sim_{\mathcal{F}} x_2 \vee y_2$.

3. Sean $x_1, x_2, y_1, y_2 \in A$ como en el inciso anterior.

   Entonces,

$$\begin{aligned}(x_1 \wedge y_1) \wedge (f_1 \wedge f_2) &= (x_1 \wedge f_1) \wedge (y_1 \wedge f_2)\\ &= ((x_2 \wedge f_1) \wedge (y_2 \wedge f_2)\\ &= (x_2 \wedge y_2) \wedge (f_1 \wedge f_2).\end{aligned}$$

   Por lo que $x_1 \wedge y_1 \sim_{\mathcal{F}} x_2 \wedge y_2$.

■

Si I es un ideal y $\mathcal{F}$ un filtro, es posible construir una álgebra booleana con las relaciones inducidas por ellos. A estas álgebras se les llama álgebras cociente:

Definición 2.16 *Sea I un ideal. Al conjunto $A/I = \{[a]_{\sim I} | a \in A\}$ (recordemos que $[a]_{\sim I} = \{b \in A | b \sim_I a\}$ es la clase de equivalencia de a) se le llama A módulo I y se puede proveer de una estructura de álgebra booleana con las siguientes operaciones:*

1. $[a] \wedge [b] = [a \wedge b]$.
2. $[a] \vee [b] = [a \vee b]$.
3. $[a]' = [a']$.

Si $\mathcal{F}$ es un filtro entonces $A/\mathcal{F}$ es el álgebra booleana de las clases de equivalencia bajo la relación $\sim_{\mathcal{F}}$ con las operaciones heredadas. Tanto A/I como $A/\mathcal{F}$ son álgebras booleanas gracias a la proposición 2.5.

Problema 2.1 *Sea I un ideal y $\mathcal{F}$ un filtro en A. ¿Quién es el 0 y el 1 de A/I y de $A/\mathcal{F}$?.*

Prueba.

Para encontrar el cero de A/I tendremos:

$\forall [a] \in A/I$ $\exists [b]$ tal que $[a] \vee [b] = [a]$

$$\begin{aligned}
[a] \vee [b] = [a] &\Longrightarrow [a \vee b] = [a] \\
&\Longrightarrow a \vee b \sim_I a \\
&\Longrightarrow \exists i \in I \ tales \ que \ (a \vee b) \vee i = a \vee i \\
&\Longrightarrow a \vee (b \vee i) = a \vee i \\
&\Longrightarrow a' \vee a \vee (b \vee i) = a' \vee a \vee i \\
&\Longrightarrow b \vee i = 0 \vee i \\
&\Longrightarrow b \sim_I 0 \\
&\Longrightarrow [b] = [0].
\end{aligned}$$

Para encontrar el 1 de A/I tendremos:

$\forall [a] \in A/I$ $\exists [b]$ tal que $[a] \wedge [b] = [a]$

$$\begin{aligned}
[a] \wedge [b] = [a] &\Longrightarrow [a \wedge b] = [a] \\
&\Longrightarrow a \wedge b \sim_I a \\
&\Longrightarrow \exists i \in I \ tales \ que \ (a \wedge b) \vee i = a \vee i \\
&\Longrightarrow a \wedge (b \vee i) = a \vee i \\
&\Longrightarrow a' \vee a \wedge (b \vee i) = a' \vee a \vee i \\
&\Longrightarrow b \vee i = 1 \vee i \\
&\Longrightarrow b \sim_I 1 \\
&\Longrightarrow [b] = [1].
\end{aligned}$$

Luego, el 1 de A/I es [1]. Siguiendo un proceso de manera análoga, llegamos a que el 0 y 1 de $A/\mathcal{F}$ son [0] y $\mathcal{F}$ respectivamente. ■

Existen homomorfismos naturales de A en A/I y $A/\mathcal{F}$ llamados proyecciones

$$p_I : A \longrightarrow A/I,$$

$$p_{\mathcal{F}} : A \longrightarrow A/\mathcal{F}$$

y cumplen que $p(a) = [a]$, $\forall a \in A$.

Prueba.

Probaremos únicamente que p_I es un homomorfismo booleano, la prueba para $p_{\mathcal{F}}$ es dual.

1. Probemos que p_I está bien definida

   Sean $a, b \in A$ tal que $a = b$, y probaremos que $[a] = [b]$

   Sea $x \in [a]$

$$\begin{aligned} x \in [a] &\Longleftrightarrow x \sim_I a \\ &\Longleftrightarrow \exists i \in I \ \textit{tales que } x \vee i = a \vee i \\ &\Longleftrightarrow x \vee i = b \vee i \\ &\Longleftrightarrow x \sim_I b \\ &\Longleftrightarrow x \in [b]. \end{aligned}$$

   Por lo tanto $[a] = [b]$ así $p_I(a) = p_I(b)$

2. Probamos si p_I es homomorfismo booleano.

   $a)$ Sean $a, b \in A$

$$\begin{aligned} p_I(a \vee b) &= [a \vee b] \\ &= [a] \vee [b] \\ &= p_I(a) \vee p_I(b). \end{aligned}$$

b) Sean $a, b \in A$

$$\begin{aligned} p_I(a \wedge b) &= [a \wedge b] \\ &= [a] \wedge [b] \\ &= p_I(a) \wedge p_I(b). \end{aligned}$$

c) Sea $a \in A$

$p_I(a^{'}) = [a^{'}] = [a]^{'} = (p_I(a))^{'}$

Por lo tanto, p_I es un homomorfismo booleano. ■

Lema 2.3 *Sea I un ideal en A, y $\mathcal{F}$ un filtro,. Entonces $ker(p_I) = I$ y $Sh(p_{\mathcal{F}}) = \mathcal{F}$.*

Prueba.

Demostraremos sólo el caso de los ideales. La demostración para los filtros es dual.

Sea $a \in ker(p_I)$.

$$\begin{aligned} a \in ker(p_I) &\Longrightarrow p_I(a) = [0], \\ &\Longrightarrow [a] = [0], \\ &\Longrightarrow a \sim_I 0, \\ &\Longrightarrow \exists i \in I \text{ tales que } a \vee i = 0 \vee i = i \in I, \\ &\Longrightarrow a \vee i \in I, \\ &\Longrightarrow a \in I. \end{aligned}$$

Luego, $ker(p_I) \subset I$. Además, $\forall i \in I$ $[i] = [0]$. Por lo tanto, $Ker(p_I) = I$. ■

Las álgebras cociente se comportan de una manera bastante interesante como lo evidencia el siguiente teorema.

Teorema 2.8 *Sea I un ideal en A. Entonces A/I cumple la siguiente propiedad (universal):*

si $f : A \longrightarrow B$ es un homomorfismo booleano tal que $I \subseteq ker(f)$, entonces existe un único homomorfismo $h : A/I \longrightarrow B$ tal que $f = h \circ p_I$. O en otras palabras, que hace conmutar el siguiente diagrama.

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "p_I"'] & B \\ A/I \arrow[ur, dashed, "\exists ! h"'] & \end{tikzcd}$$

Prueba.

Sea I un ideal y $f : A \longrightarrow B$ un homomorfismo booleano tal que $I \subseteq ker(f)$. Definamos $h : A/I \longrightarrow B$ como sigue: $h([a]) = f(a)$. Tenemos que verificar tres cosas:

1. Que la función h está bien definida,
2. Que h es un homomorfismo booleano único y que ,
3. Hace conmutar el diagrama.

1. Sean $[a], [b] \in A/I$ tales que $[a] = [b]$

$$\begin{aligned} [a] = [b] &\Longrightarrow a \sim_I b \\ &\Longrightarrow \exists i \in I \text{ tal que } a \vee i = b \vee i, \end{aligned}$$

Luego, se tiene que:

$$\begin{aligned} h([a]) &= f(a) \\ &= f(a) \vee 0 \\ &= f(a) \vee f(i) \\ &= f(a \vee i) \end{aligned}$$

$$\begin{aligned} &= f(b \vee i) \\ &= f(b) \vee f(i) \\ &= f(b) \vee 0 \\ &= f(b) \\ &= h([b]). \end{aligned}$$

Por lo que h está bien definida.

2. Que h sea un homomorfismo es consecuencia de que f es homomorfismo y de como indujimos las operaciones en A/I.

3. Es claro que $f = h \circ p_I$. Por último probemos que h es único.

   Sea $h^{'} : A/I \longrightarrow B$ un homomorfismo tales que $f = h^{'} \circ p_I$.

   Entonces, $h([a]) = h(p_I(a)) = f(a) = h^{'}(p_I(a)) = h^{'}([a])$, por lo que $h^{'} = h$.

Por lo tanto, se puede concluir que existe un único homomorfismo $h : A/I \longrightarrow B$ tal que $f = h \circ p_I$. ■

Teorema 2.9 *Sea $f : A \longrightarrow B$ un homomorfismo booleano. Entonces $A/ker(f) \simeq Im(f)$.*

Prueba. Sea $I = ker(f)$ por el teorema anterior existe un homomorfismo $h : A/I \longrightarrow B$ tal que $f = h \circ p_I$. Veamos que h es un isomorfismo con la imagen, anteriormente probamos que h está bien definida sólo probaremos que h es monomorfismo y epimorfismo.

Probando que h es monomorfismo.

Sean $[a], [b] \in A/I$ tales que $h([a]) = h([b])$

$$\begin{aligned} h([a]) = h([b]) &\Longrightarrow f(a) = f(b) \\ &\Longrightarrow f(a-b) = 0 \\ &\Longrightarrow a - b \in ker(f) = I \\ &\Longrightarrow a \sim_I b \\ &\Longrightarrow [a] = [b]. \end{aligned}$$

Por lo tanto h es monomorfismo.

Es claro que $Im(h) = Im(f)$ por lo tanto es $h : A/I \longrightarrow Im(h)$ monomorfismo y epimorfismo por lo tanto isomorfismo. Por lo que $A/I \simeq Im(f)$. ■

Corolario 2.4 *Sea $f : A \longrightarrow B$ un epimorfismo booleano. Entonces $A/ker(f) \simeq B$.*

Prueba. Como f es epimorfismo, entonces $Im(f) = B$. Luego, por el teorema 2.9 se sabe que:

$$A/ker(f) \simeq Im(f),$$

de donde se obtiene que:

$$A/ker(f) \simeq B.$$

■

Capítulo 3

Aplicaciones del Álgebra Booleana

El presente capítulo esta dirigido al estudio de aplicaciones del álgebra booleana. Una de ellas son las compuertas lógicas, las cuales son de gran utilidad en el diseño de los circuitos lógicos. La otra es el código genético y $\mathbb{Z}_2^6$ donde se describe brevemente un modelo del código genético en términos de álgebra booleana y $\mathbb{Z}_2^6$.

3.1. Compuertas Lógicas

Una compuerta es un circuito electrónico que trabaja con dos estados $''0''$ y $''1''$, el estado 1 tiene un valor de $5V$ (5 voltios) como máximo y el estado 0 tiene un valor de $0V$ (0 voltios) como mínimo, una compuerta lógica está compuesta por dos o más entradas y una salida, que tiene la capacidad de tomar decisiones. La decisión tomada por una compuerta es situar su salida en 0 ó en 1, depende del estado de sus entradas y de la función lógica para la cual ha sido diseñada. Las compuertas lógicas son dispositivos que operan con aquellos estados lógicos que funcionan igual que una calculadora, de un lado se ingresan los datos, ésta realiza una operación, y finalmente, muestra el resultado. Ver figura 3.1.

Figura 3.1: Fases de un circuito.
Fuente:
`http://service.udes.edu.co/modulos/documentos/pedropatino/compuertas.pdf`

Las operaciones boolenas son posibles a través de los operadores binarios negación, suma y multiplicación, es decir, que estos combinan dos o más variables para conformar funciones lógicas.

Una compuerta es un circuito útil para realizar las operaciones anteriormente mencionadas, cada una de las compuertas lógicas se representan mediante un símbolo, y la operación que realiza (operación lógica), le corresponde una tabla llamada tabla de verdad.

Las compuertas son los bloques básicos de cualquier circuito digital, todos los aparatos digitales desde el más simple dispositivo hasta el más sofisticado están formados por compuertas conectadas a una gran variedad de configuraciones.

Las puertas o compuertas lógicas básicas son: La puerta AND, la puerta OR y la puerta NOT. Si a las compuertas anteriores se les niega la salida en el sentido lógico, tenemos la configuración de otras compuertas como NAND, NOR. La puerta XOR es una puerta que se denomina OR EXCLUSIVO.

Existen 8 tipos de compuertas, las cuales se muestran en la Figura 3.2 y se define a continuación:

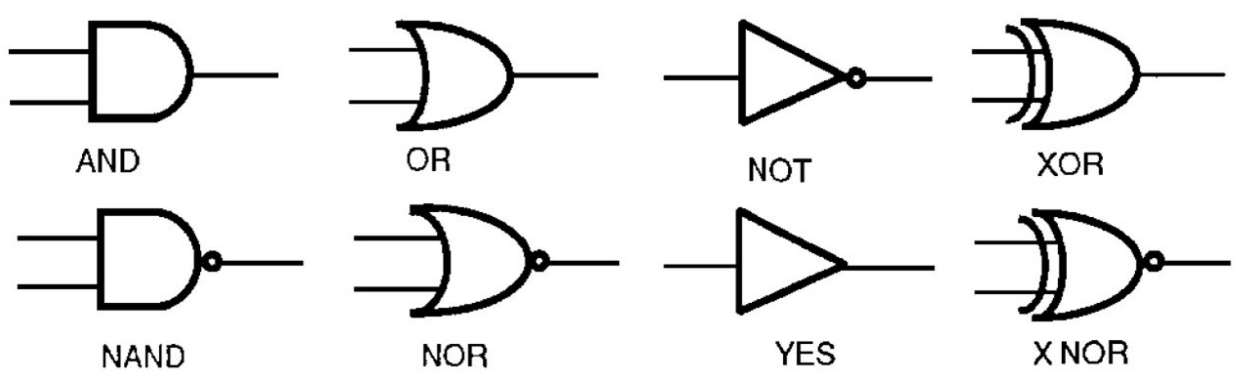


Figura 3.2: Tipos de compuertas lógicas.
Fuente: `https://www.academia.edu/16651436/1184_compuertas_logicas.`

3.1.1. *Compuertas AND de dos entradas*

Una compuerta AND de dos entradas es un dispositivo lógico que entrega una salida **alta** cuando todas sus entradas son **altas** y una salida **baja** cuando hay un **bajo** en cualquiera de sus entradas.

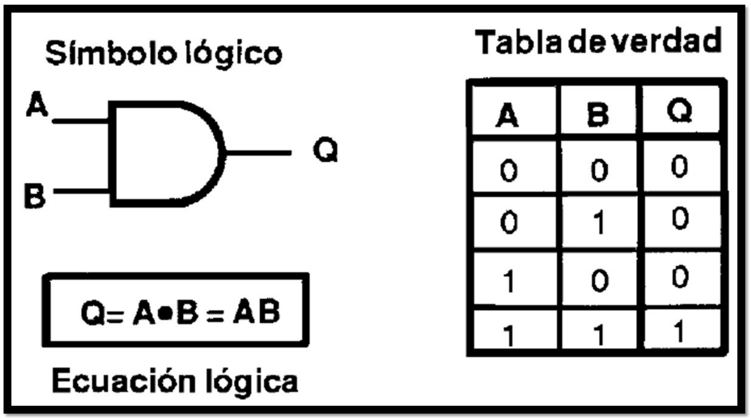


Figura 3.3: Compuerta AND de dos entradas.
Fuente: `https://www.academia.edu/16651436/1184_compuertas_logicas`.

La expresión $Q = A \cdot B$ debe de leerse como Q es igual a A y B, el signo $(\cdot)$ denota la función propia de una compuerta AND y se puede omitir. La función lógica realizada por una compuerta AND se denomina operación AND o **producto lógico**, en la compuerta AND la salida será 1 solo cuando sus 2 entradas estén en 1. La operación de una compuerta AND se representa como el circuito siguiente:

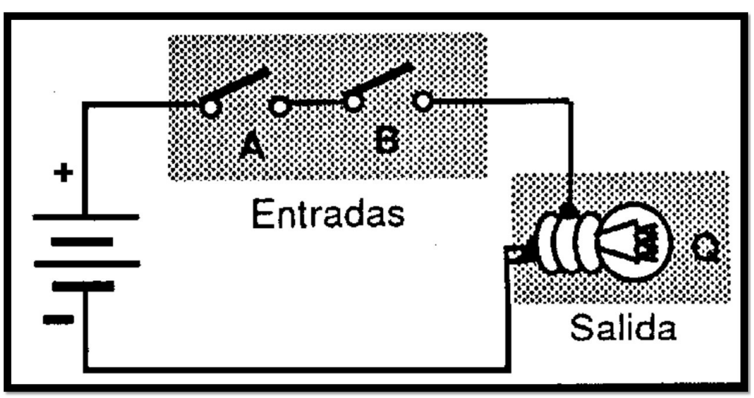
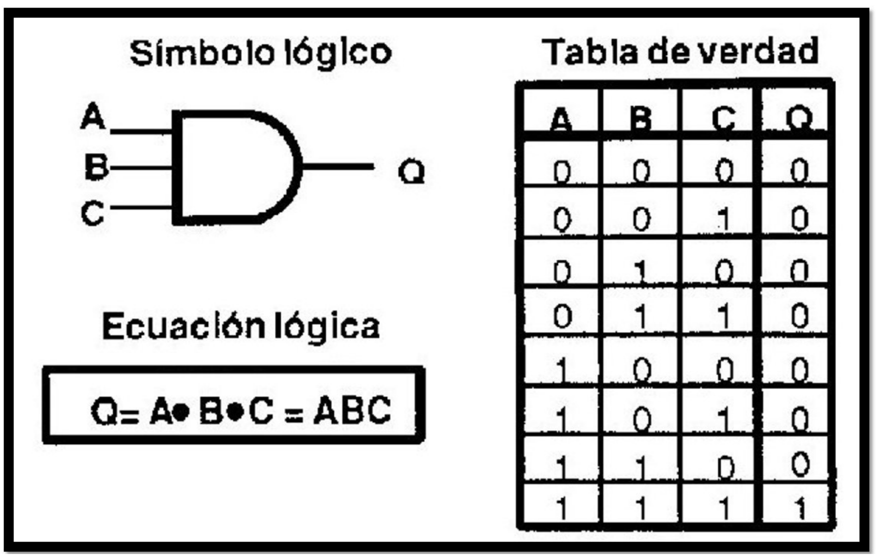


Figura 3.4: Circuito lógico AND de dos entradas.
Fuente: `https://www.academia.edu/16651436/1184_compuertas_logicas`.

Los interruptores A y B representan las entradas de la compuerta y la lámpara Q su salida, puesto que A y B están en serie, la lámpara Q sólo se enciende cuando ambos interruptores están cerrados y permanece apagada mientras cualquiera de los interruptores, o ambos, esté abierto. Un interruptor cerrado se asimila a un nivel **alto** ó 1 lógico y un interruptor abierto a un nivel **bajo** ó 0 lógico.

3.1.2. *Compuertas AND de varias entradas*

En general, una compuerta AND de dos o más entradas entrega un nivel **alto** (ó 1 lógico en su salida) cuando todas sus entradas están en **alto** y un **bajo** (ó 0 lógico) cuando por lo menos una de ellas, o todas, están en **bajo**.



A	B	C	Q
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	0
1	0	0	0
1	0	1	0
1	1	0	0
1	1	1	1

Figura 3.5: Compuerta AND de tres entradas.
Fuente: `https://www.academia.edu/16651436/1184_compuertas_logicas.`

En la figura 3.5 se presenta el símbolo lógico, la ecuación lógica y la tabla de verdad de una compuerta AND de tres entradas la cual nos dice la salida dependiendo de las entradas.

La expresión $Q = A \cdot B \cdot C$ puede leerse como Q es igual a A y B y C, en la compuerta AND de tres entradas la salida será 1 sólo cuando sus 3 entradas estén en 1.

La operación de una compuerta AND de tres entradas se representa como el circuito 3.6, donde los interruptores A, B y C representan las entradas de la compuerta y la lámpara Q

su salida.

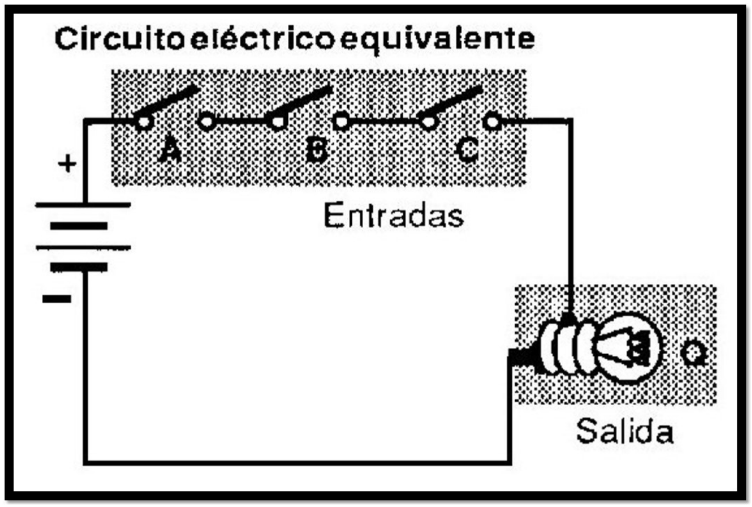


Figura 3.6: Circuito AND de tres entradas.
Fuente: `https://www.academia.edu/16651436/1184_compuertas_logicas.`

3.1.3. *Compuertas OR de dos entradas*

Una compuerta OR de dos entradas es un dispositivo lógico que entrega una salida **baja** cuando todas sus entradas son **bajas**, y una salida **alta** cuando existe por lo menos un **alto** en cualquiera de sus entradas o en las dos al mismo tiempo.

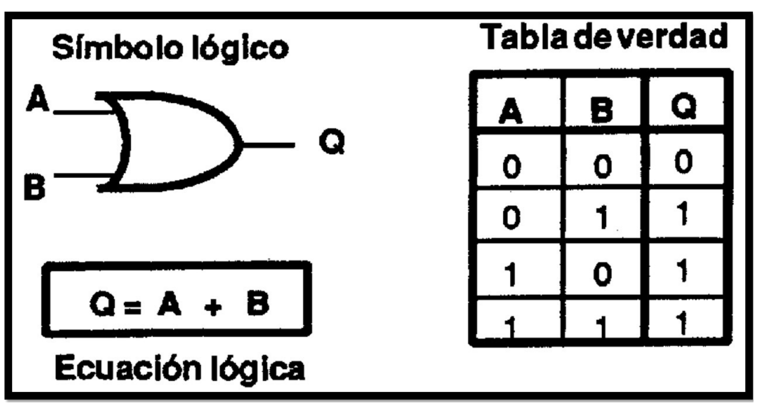


Figura 3.7: Compuerta OR de dos entradas.
Fuente: `https://www.academia.edu/16651436/1184_compuertas_logicas.`

En la figura 3.7 se muestra el símbolo lógico, la ecuación lógica y la tabla de verdad de una compuerta OR de dos entradas, la cual nos dice la salida dependiendo de la combinación de las entradas. La expresión $Q = A + B$ debe leerse como Q es igual a A o B. El signo (+) denota la función propia de una compuerta OR y no se puede omitir, no debe confundirse con el signo ″+″ de la suma aritmética. La función lógica realizada por la compuerta OR se denomina operación OR o **suma lógica**, en la compuerta OR la salida será 1 cuando una o las dos entradas estén en 1.

La operación de una compuerta OR se representa como el circuito siguiente:

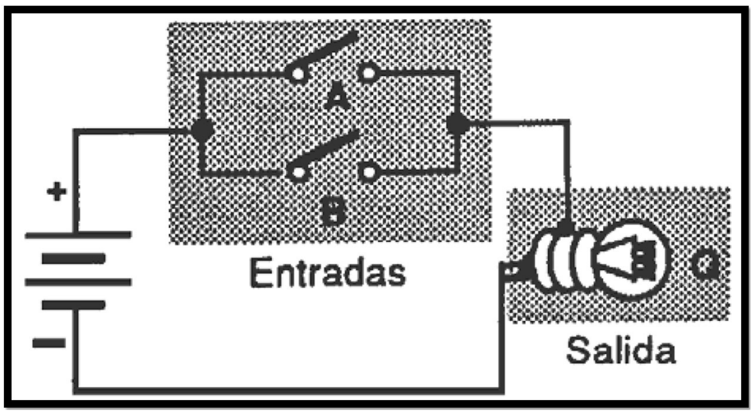


Figura 3.8: Circuito lógico OR de dos entradas.
Fuente: `https://www.academia.edu/16651436/1184_compuertas_logicas.`

Los interruptores A y B representan las entradas de la compuerta y la lámpara Q su salida. Debido a que los interruptores están en paralelo, la lámpara Q sólo se apagará cuando ambos interruptores A y B estén abiertos y permanecerá encendida mientras cualquiera de los interruptores, o ambos, estén cerrados.

3.1.4. *Compuertas OR de varias entradas*

En general, una compuerta OR de dos o más entradas entrega un nivel **bajo** en su salida cuando todas sus entradas están en **bajo** y uno **alto** cuando por lo menos una de ellas, o todas, están en **alto**.

En la figura 3.9 se presenta el símbolo lógico, la ecuación lógica y la tabla de verdad de una compuerta OR de tres entradas la cual nos dice la salida dependiendo de las entradas.

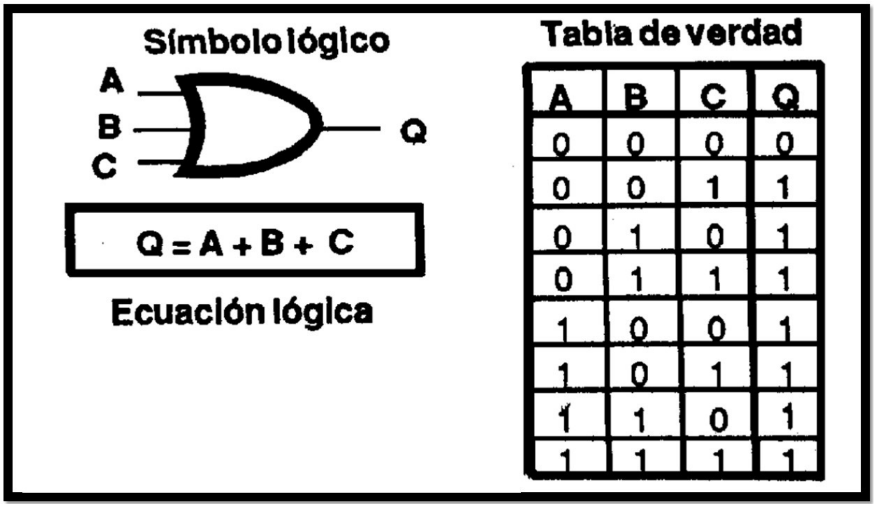


Figura 3.9: Compuerta OR de tres entradas.
Fuente: `https://www.academia.edu/16651436/1184_compuertas_logicas.`

La expresión $Q = A + B + C$ puede leerse como Q es igual a A ó B ó C, en la compuerta OR de tres entradas la salida será 1 cuando una, dos o tres entradas estén en 1. La operación de una compuerta OR de tres entradas se representa como el circuito siguiente:

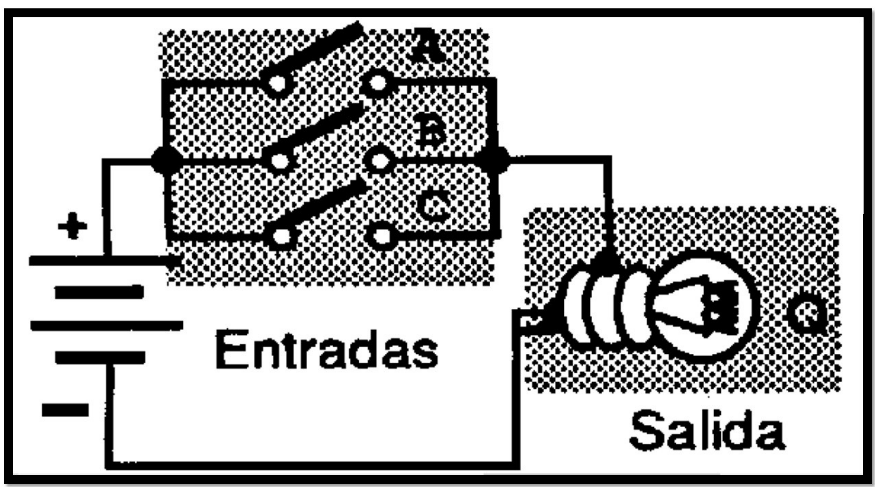


Figura 3.10: Circuito lógico OR de tres entradas.
Fuente: `https://www.academia.edu/16651436/1184_compuertas_logicas.`

En la representación del circuito eléctrico, los interruptores A, B y C representan las entradas de la compuerta y la lámpara Q su salida. La lámpara Q sólo se apaga cuando todos los interruptores estén abiertos; permanece encendida mientras cualquiera de ellos esté cerrado.

3.1.5. *Compuertas NOT o Inversores*

Una compuerta NOT o inversor es un dispositivo lógico con una línea de entrada y una línea de salida que entrega una salida **alta** cuando su entrada es **baja** y una salida **baja** cuando su entrada es **alta**. En otras palabras, un inversor invierte, niega o complementa el nivel lógico de la señal de entrada. Es una de las compuertas más utilizadas.

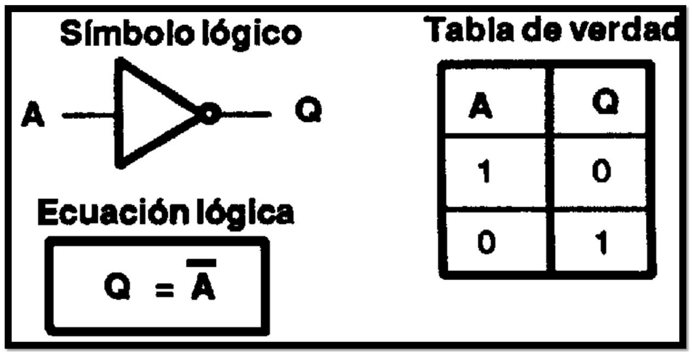


Figura 3.11: Compuerta NOT o Inversor.
Fuente: `https://www.academia.edu/16651436/1184_compuertas_logicas.`

En la figura 3.11 se muestra el símbolo lógico, la ecuación lógica, a tabla de verdad de una compuerta NOT o Inversores, la cual nos dice la salida dependiendo de la combinación de las entradas. La ecuación lógica debe leerse como Q es igual a no A ó Q es igual a A negado. El círculo o burbuja (o) en el símbolo lógico y la barra horizontal ($-$) en la ecuación lógica denotan el proceso de inversión realizado por esta compuerta. La función lógica realizada por un inversor se denomina inversión o **complemento lógico**. No existen inversores de dos o más entradas. La operación de un inversor es análoga a la del circuito mostrado en la figura siguiente:

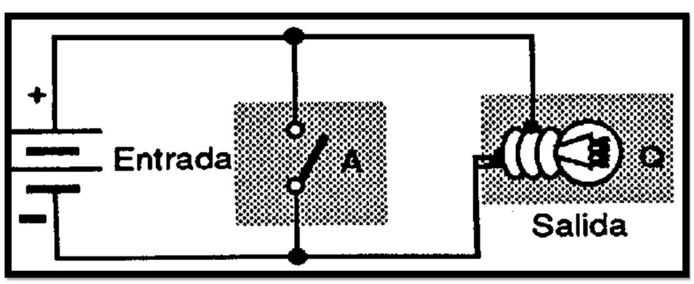


Figura 3.12: Circuito lógico NOT.
Fuente: `https://www.academia.edu/16651436/1184_compuertas_logicas.`

El interruptor A representa la entrada de la compuerta y la lámpara Q su salida, debido a que el interruptor está en paralelo con la lámpara Q, esta última se encenderá cuando el interruptor A se abra y se apagará cuando el interruptor se cierre.

3.1.6. *Compuerta YES*

La compuerta lógica más simple es la compuerta YES. La compuerta YES es un dispositivo lógico con una linea de entrada y una linea de salida que entrega una salida **alta** cuando su entrada es **alta** y una salida **baja** cuando su entrada es **baja**. En otras palabras, en una compuerta YES la salida toma siempre el mismo valor de la entrada.

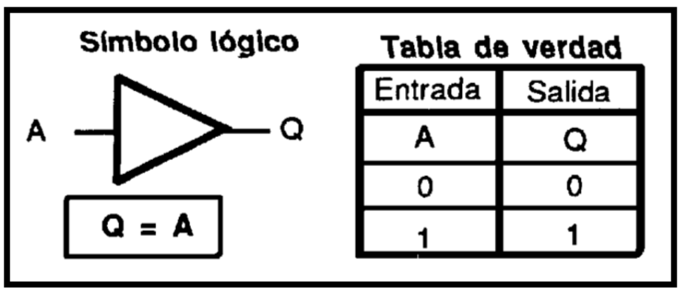


Figura 3.13: Compuerta YES.
Fuente: `https://www.academia.edu/16651436/1184_compuertas_logicas`.

En la figura 3.13 se muestra el símbolo lógico, la ecuación lógica, la tabla de verdad de una compuerta YES, la cual nos dice la salida dependiendo de la combinación de las entradas. La ecuación lógica debe leerse como Q es igual a A.

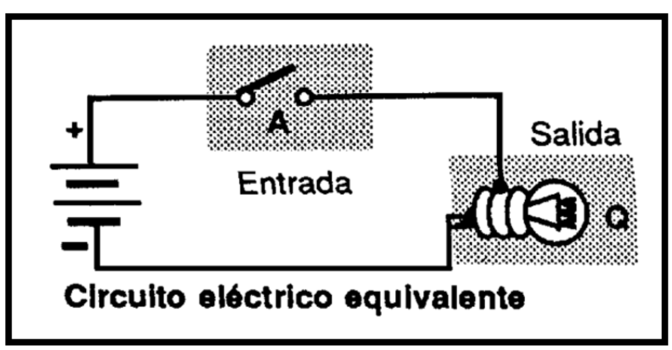


Figura 3.14: Circuito lógico YES.
Fuente: `https://www.academia.edu/16651436/1184_compuertas_logicas`.

En la figura 3.14 se muestra el circuito lógico equivalente de una compuerta YES donde, la lámpara Q se enciende cuando el interruptor A se cierra y se apaga cuando este último se abre.

3.1.7. *Compuertas NAND de dos entradas*

Una compuerta NAND de dos entradas es un dispositivo lógico que opera en forma exactamente contraria a una compuerta AND, entregando una salida **baja** cuando todas sus entradas son **altas** y una salida **alta** mientras exista por lo menos un **bajo** en cualquiera de ellas.

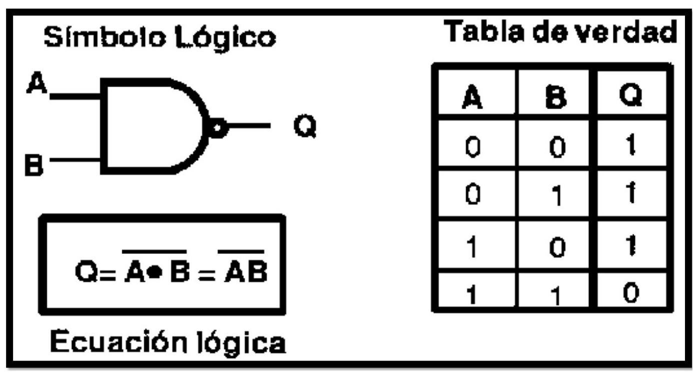


Figura 3.15: Compuerta NAND de dos entradas.
Fuente: `https://www.academia.edu/16651436/1184_compuertas_logicas.`

En la figura 3.15 se muestran el símbolo lógico, la ecuación lógica y la tabla de verdad de una compuerta NAND de dos entradas. La ecuación lógica debe leerse como Q es igual a A y B negado, una compuerta NAND es equivalente a una compuerta AND seguida de un inversor. En la figura 3.16 se puede ver gráficamente esta equivalencia.

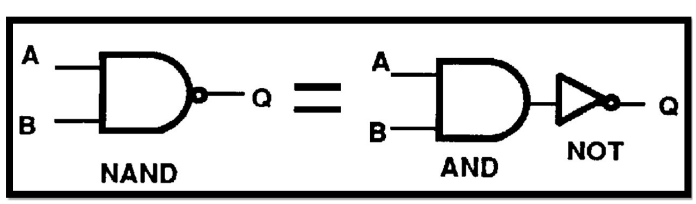


Figura 3.16: Equivalencia de una compuerta NAND y una compuerta AND seguida de un inverso.
Fuente: `https://www.academia.edu/16651436/1184_compuertas_logicas.`

La operación de una compuerta NAND es análoga a la del circuito eléctrico mostrado en siguiente figura:

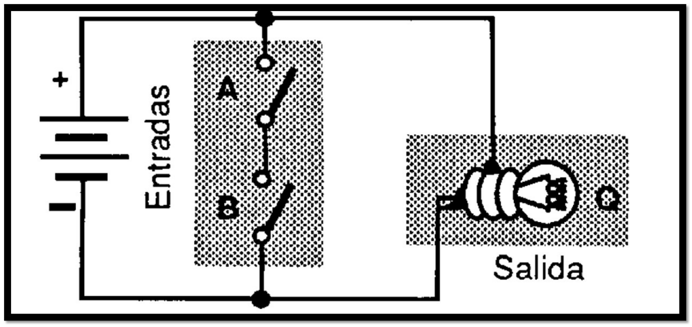
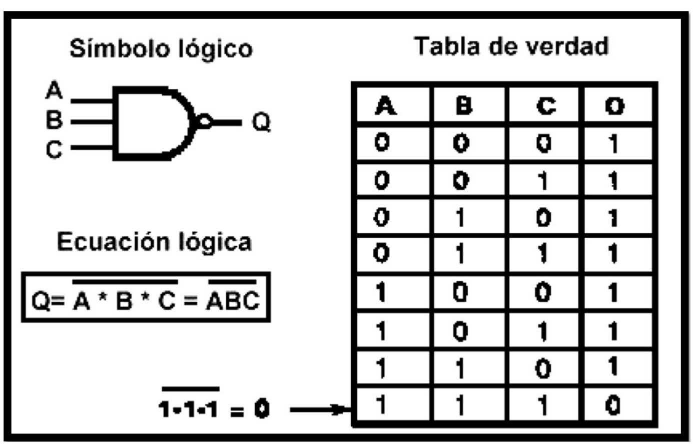


Figura 3.17: Circuito lógico NAND de dos entradas.
Fuente: `https://www.academia.edu/16651436/1184_compuertas_logicas.`

Los interruptores A y B están en serie entre sí y en paralelo con la lámpara Q, esta última sólo se apaga cuando ambos interruptores están cerrados y permanece encendida mientras cualquiera de ellos esté abierto.

3.1.8. *Compuertas NAND de varias entradas*

En general, una compuerta NAND de dos o más entradas entrega un nivel lógico **bajo** en su salida cuando todas sus entradas están en **alto** y un **bajo** cuando por lo menos una de ellas está en **bajo**.



A	B	C	Q
0	0	0	1
0	0	1	1
0	1	0	1
0	1	1	1
1	0	0	1
1	0	1	1
1	1	0	1
1	1	1	0

Figura 3.18: Compuerta NAND de tres entradas.
Fuente: `https://www.academia.edu/16651436/1184_compuertas_logicas.`

En la figura 3.18 se muestra el símbolo lógico, la ecuación lógica, la tabla de verdad.

La ecuación lógica debe leerse como Q es igual a A y B y C negado. La operación de una compuerta NAND de 3 entradas es análoga a la del circuito mostrado en la figura siguiente:

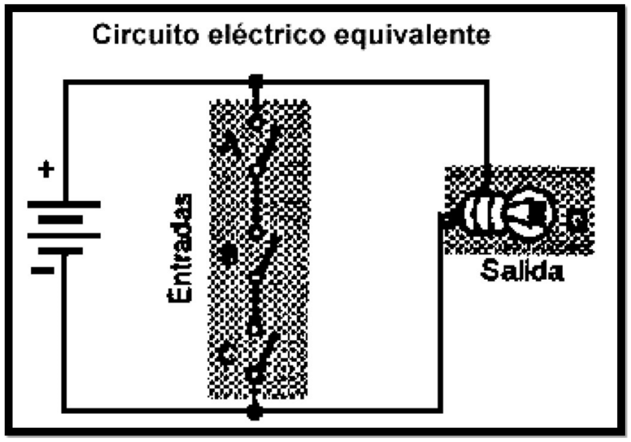


Figura 3.19: Circuito lógico NAND de tres entradas.
Fuente: `https://www.academia.edu/16651436/1184_compuertas_logicas.`

En el circuito eléctrico, los interruptores A, B y C representan las entradas y la lámpara Q la salida de la compuerta. La lámpara sólo se apaga cuando todos los interruptores están cerrados y permanece encendida mientras cualquiera de ellos esté abierto.

3.1.9. *Compuertas NOR de dos entradas*

La compuerta NOR es una combinación de las compuertas OR y NOT, en otras palabras, es la versión inversa de la compuerta OR. Al tener sus entradas en estado inactivo 0 su salida estará en un estado activo 1, pero si alguna de las entradas pasa a un estado binario 1 su salida tendrá un estado inactivo 0.

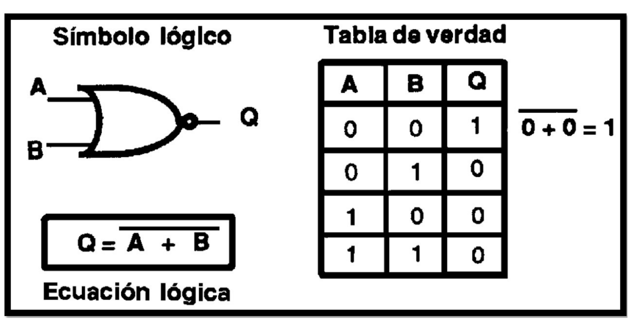


Figura 3.20: Compuerta NOR de dos entradas.
Fuente: `https://www.academia.edu/16651436/1184_compuertas_logicas.`

En la figura 3.20 se muestra el símbolo lógico, la ecuación lógica y la tabla de verdad de una compuerta NOR de dos entradas. La ecuación lógica puede leerse como Q es igual a A o B negado. El signo (+) y la barra (−) en la ecuación lógica y la burbuja en el símbolo OR confirman esta equivalencia. Una compuerta NOR es equivalente a una compuerta OR seguida de un inversor tal como se observa en la figura 3.21.

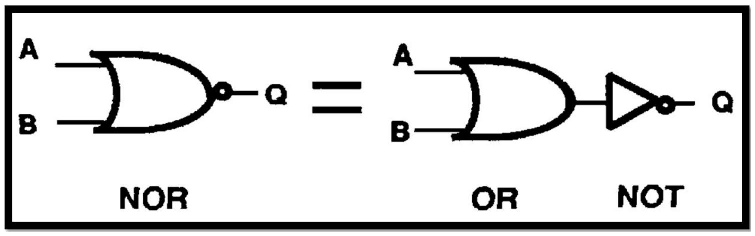


Figura 3.21: Equivalencia de una compuerta NOR y una compuerta OR seguida de un inverso.
Fuente: `https://www.academia.edu/16651436/1184_compuertas_logicas.`

La operación de una compuerta NOR es análoga a la del circuito eléctrico mostrado en la figura 3.22. Donde los interruptores A y B representan las entradas de la compuerta y la lámpara Q su salida. Debido a que los interruptores A y B están en paralelo entre sí y con la lámpara Q, esta última sólo se enciende cuando ambos interruptores están abiertos y permanece apagada mientras cualquiera de ellos, o ambos, esté cerrado.

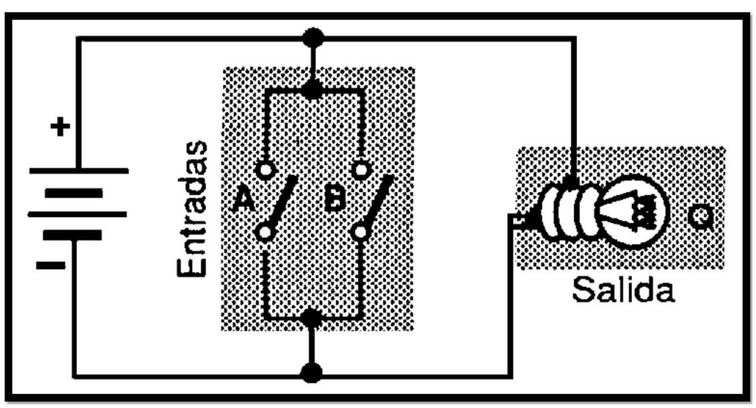
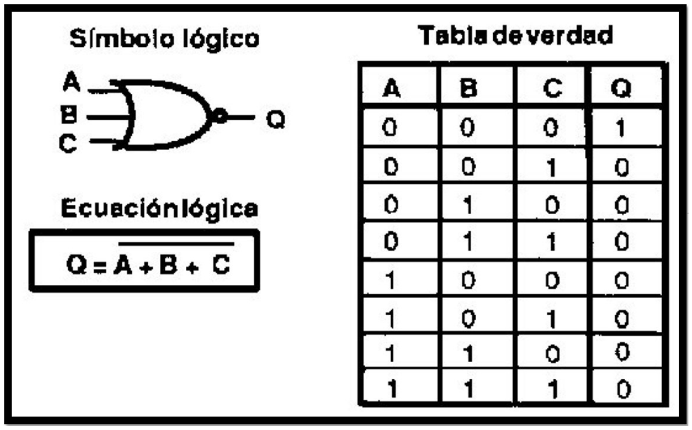


Figura 3.22: Circuito lógico NOR de dos entradas.
Fuente: `https://www.academia.edu/16651436/1184_compuertas_logicas.`

3.1.10. Compuertas NOR de varias entradas

En general, una compuerta NOR de dos ó más entradas entrega un nivel lógico **alto** en su salida cuando todas sus entradas están en **bajo** y un **bajo** cuando por lo menos una de ellas está en **alto**.



A	B	C	Q
0	0	0	1
0	0	1	0
0	1	0	0
0	1	1	0
1	0	0	0
1	0	1	0
1	1	0	0
1	1	1	0

Figura 3.23: Compuerta NOR de tres entradas.
Fuente: `https://www.academia.edu/16651436/1184_compuertas_logicas.`

En la figura 3.23 se muestra el símbolo lógico, la ecuación lógica, la tabla de verdad de una compuerta NOR de tres entradas. La ecuación lógica puede leerse como Q es igual a A o B o C negado. Y su representación eléctrica equivalente de una compuerta NOR de tres entradas se muestra en la siguiente figura:

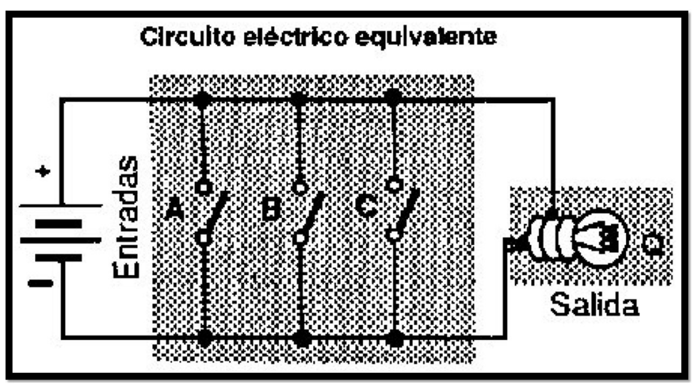


Figura 3.24: Circuito lógico NOR de tres entradas.
Fuente: `https://www.academia.edu/16651436/1184_compuertas_logicas.`

En el circuito eléctrico, los interruptores A, B y C representan las entradas de la compuerta y la lámpara Q su salida. La lámpara Q sólo se enciende cuando todos los interruptores están abiertos y permanece apagada mientras cualquiera de ellos esté cerrado.

3.1.11. Compuertas OR exclusivas o XOR

Una compuerta OR exclusiva o XOR es un dispositivo digital con dos líneas de entrada y una línea de salida que entrega una salida alta cuando una de sus entradas es baja y la otra alta y una salida baja cuando sus entradas son ambas bajas o ambas altas. Es decir, una compuerta XOR informa, mediante un 1 en su salida, cuándo las dos entradas tienen estados lógicos diferentes. Esta característica permite que se utilice como verificador de desigualdad en comparadores y otros circuitos aritméticos.

En la figura 3.25 se muestra el símbolo lógico, la ecuación lógica y la tabla funcional de una compuerta XOR. La ecuación lógica puede leerse como Q es igual a A o B exclusiva.

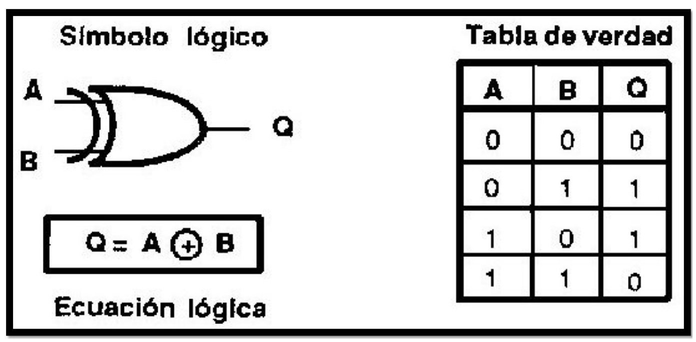


Figura 3.25: Compuerta OR exclusivo o XOR.
Fuente: `https://www.academia.edu/16651436/1184_compuertas_logicas.`

3.1.12. Compuertas NOR exclusivas o XNOR

Una compuerta NOR exclusiva o XNOR opera en forma exactamente opuesta a una compuerta XOR, entregando una salida **baja** cuando una de sus entradas es **baja** y la otra **alta**, y una salida **alta** cuando sus entradas son ambas **altas** o ambas **bajas**. Es decir, una compuerta XNOR indica, mediante un 1 lógico en su salida, cuándo las dos entradas tienen el mismo estado, característica que hace ideal su utilización como verificador de igualdad en comparadores y otros circuitos aritméticos.

En la figura 3.26 se muestra el símbolo lógico y la tabla funcional de una compuerta XNOR. La ecuación lógica puede leerse como Q es igual a A o B exclusiva negada. Para efectos prácticos, una compuerta XNOR es igual a una compuerta XOR seguida de un inversor.

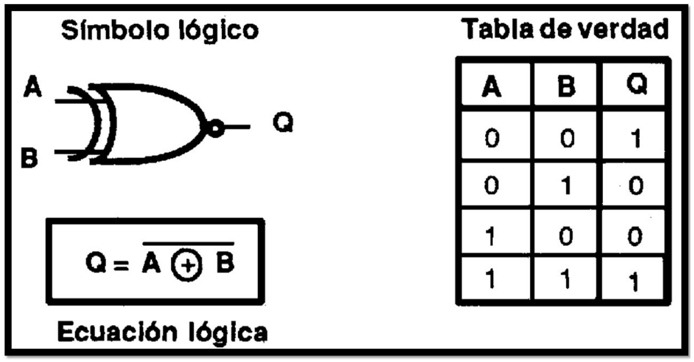


Figura 3.26: Compuerta NOR exclusivo o XNOR.
Fuente: `https://www.academia.edu/16651436/1184_compuertas_logicas`.

3.1.13. *Operaciones booleanas*

Sea X el conjunto de estados de un circuito lógico. El cuaterno $(X, +, \cdot, ^{-})$ forma un álgebra booleana, es decir, se satisfacen las siguientes operaciones booleanas para cualesquiera A, B, C en X:

1. $A + \overline{A} = 1$
2. $A \cdot \overline{A} = 0$
3. $0 + A = A$
4. $1 \cdot A = A$
5. $1 + A = 1$
6. $0 \cdot A = 0$
7. $A + A = A$
8. $A \cdot A = A$
9. $A + B = B + A, A \cdot B = B \cdot A$; Conmutatividad
10. $A + B + C = (A + B) + C = A + (B + C), A \cdot B \cdot C = (A \cdot B) \cdot C = A \cdot (B \cdot C)$; Asociatividad

11. $A + (B \cdot C) = (A + B)(A + C)$, $A \cdot (B + C) = (A \cdot B) + (A \cdot C)$; Distributivo

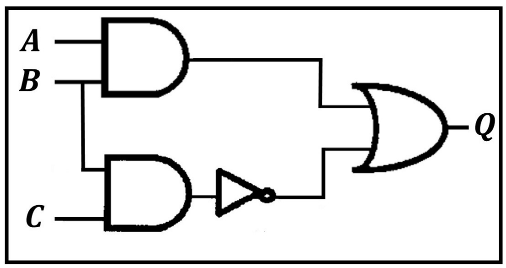
12. $A + (A \cdot B) = A(1 + B) = A, A \cdot (A + B) = (A \cdot A) + (A \cdot B) = A$; Absorción.

13. $\overline{A + B} = \overline{A} \cdot \overline{B}, \overline{A \cdot B} = \overline{A} + \overline{B}$; De Morgan

Estás operaciones nos sirven para simplificar expresiones lógicas.

Ejercicio 3.1 *Escribir la tabla de verdad y la expresión lógica de los siguientes circuitos:*

1.



Solución:

Observando la figura se tienen las entradas A y B así se hará uso de la figura 3.3 y, entonces en el circuito su salida será $A \cdot B$, luego, en la otra figura, se observa que sus entradas son B y C por lo cual, aquí se hará uso de la figura 3.16 y, entonces en el circuito su salida será $\overline{A \cdot B}$. Es así que teniendo estás dos salidas las cuales son ahora las entradas para el siguiente circuito, se tendrán entonces las entradas $A \cdot B$ y $\overline{A \cdot B}$. Luego, haciendo uso de la figura 3.7 su salida será $Q = A \cdot B + \overline{A \cdot B}$. Y se puede observar gráficamente en la siguiente figura:

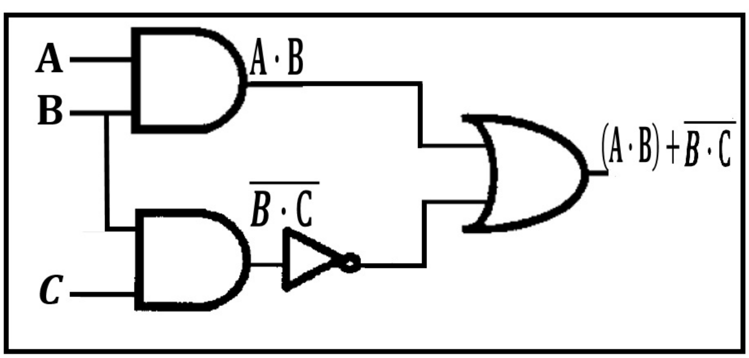


Figura 3.27: Solución del circuito.
Fuente: Creación propia en PowerPoint.

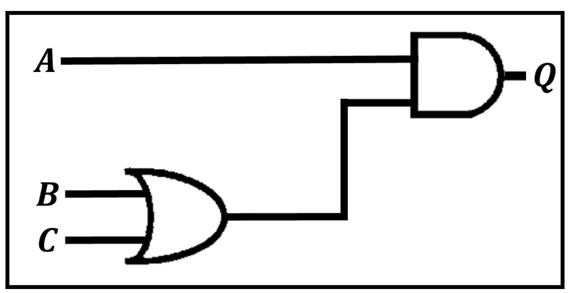
Haciendo uso de las tablas en las figura 3.3, 3.15 y 3.7 se puede obtener la tabla correspondiente al circuito lógico, ya como se observa en la tabla.

Tabla 19

Tabla de verdad correspondiente al circuito lógico.

A	B	C	$A \cdot B$	$\overline{B \cdot C}$	$A \cdot B + \overline{B \cdot C}$
0	0	0	0	1	1
0	0	1	0	1	1
0	1	0	0	1	1
0	1	1	0	0	0
1	0	0	0	1	1
1	0	1	0	1	1
1	1	0	0	1	1
1	1	1	1	0	0

2.



Solución:

Observando la figura se tienen las entradas B y C así se hará uso de la figura 3.7 y entonces en el circuito su salida será $B + C$, ahora para el siguiente circuito se hará uso de la figura 3.3 y entonces su salida será:

$$Q = A \cdot (B + C).$$

Y se puede observar gráficamente en la siguiente figura:

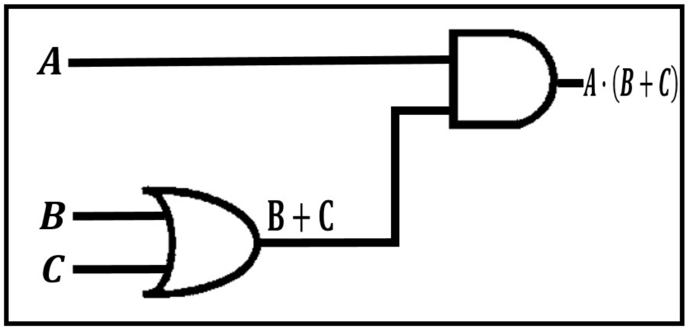


Figura 3.28: Solución del circuito.
Fuente: Creación propia en PowerPoint.

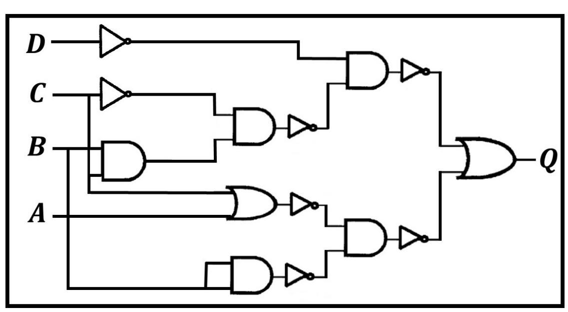
Haciendo uso de las tablas de verdad en las figuras 3.7, 3.3 se puede obtener la tabla correspondiente al circuito lógico, tal como se observa en la tabla.

Tabla 20

Tabla de verdad correspondiente al circuito lógico.

A	B	C	$B + C$	$A \cdot (B + C)$
0	0	0	0	0
0	0	1	1	0
0	1	0	1	0
0	1	1	1	0
1	0	0	0	0
1	0	1	1	1
1	1	0	1	1
1	1	1	1	1

3.



Solución:

Observando la figura se tienen las entradas A, B, C y D. Así,

1. En la primer columna se tiene que:
   a) Para la compuerta NOT se tiene la entrada D y se hace uso de la figura 3.11, entonces en el circuito su salida es $\overline{D}$.
   b) Para la compuerta NOT se tiene la entrada C y se hace uso de la figura 3.11, entonces en el circuito su salida es $\overline{C}$.
   c) Para la compuerta AND se tienen las entradas B, C y se hace uso de la figura 3.3, entonces en el circuito su salida es $B \cdot C$.
2. Para la segunda columna se tiene que:
   a) Para la compuerta NAND se tienen las entradas $\overline{C}$, $B \cdot C$ y se hace uso de la figura 3.15, entonces en el circuito su salida es $\overline{\overline{C} \cdot (B \cdot C)}$.
   b) Para la compuerta NOR se tienen las entradas C, A y se hace uso de la figura 3.20, entonces en el circuito su salida es $\overline{(C + A)}$.
   c) Para la compuerta NAND se tiene la entrada B y se hace uso de la figura 3.15, entonces en el circuito su salida es $\overline{B \cdot B} = \overline{B}$.
3. En la tercer columna se tiene que:
   a) Para la compuerta NAND se tiene las entradas $\overline{D}$, $\overline{C}$, $B \cdot C$ y se hace uso de la figura 3.15, así la salida del circuito será $\overline{\overline{D} \cdot (\overline{\overline{C} \cdot (B \cdot C)})}$.
   b) para la compuerta NAND se tiene las entradas $\overline{(C + A)}$, $\overline{B}$ y se hace uso de la figura 3.15, así la salida del circuito será $\overline{\overline{(C + A)} \cdot \overline{B}}$.
4. Para la cuarta y ultima columna se tiene que las entradas de la compuerta OR son $\overline{\overline{D} \cdot (\overline{\overline{C} \cdot (B \cdot C)})}$ y $\overline{\overline{(C + A)} \cdot \overline{B}}$. Así, haciendo uso de la figura 3.7 su salida será $\overline{\overline{D} \cdot (\overline{\overline{C} \cdot (B \cdot C)})} + \overline{\overline{(C + A)} \cdot \overline{B}}$. Se denotará la salida como:

$$S = \overline{\overline{D} \cdot (\overline{\overline{C} \cdot (B \cdot C)})} + \overline{\overline{(C + A)} \cdot \overline{B}}.$$

Se observa gráficamente en la siguiente figura:

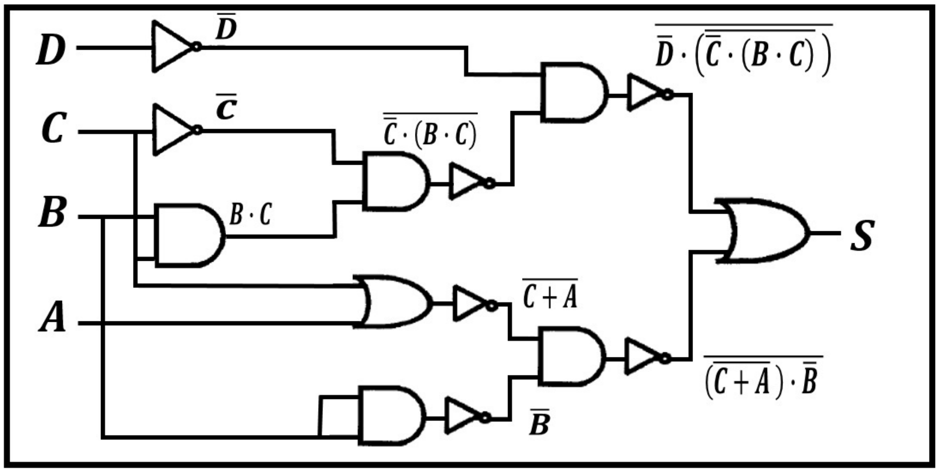


Figura 3.29: Solución del circuito.
Fuente: Creación propia en PowerPoint.

Haciendo uso de las tablas de verdad de AND, NOT, NAND, OR Y NOR se puede construir la tabla de verdad correspondiente al circuito lógico.

Tabla 21

Tabla correspondiente a los posibles valores de las entradas y sus correspondientes negaciones.

A	B	C	D	$\overline{B}$	$\overline{C}$	$\overline{D}$
0	0	0	0	1	1	1
0	0	0	1	1	1	0
0	0	1	0	1	0	1
0	1	0	0	0	1	1
0	0	1	1	1	0	0
0	1	1	0	0	0	1
0	1	0	1	0	1	0
0	1	1	1	0	0	0
1	0	0	0	1	1	1
1	0	1	0	1	0	1
1	0	0	1	1	1	0

1	1	0	0	0	1	1
1	0	1	1	1	0	0
1	1	0	1	0	1	0
1	1	1	0	0	0	1
1	1	1	1	0	0	0

En la siguiente tabla se puede observar la correspondiente tabla de verdad del circuito lógico.

Tabla 22

Tabla del circuito lógico.

$B \cdot C$	$\overline{\overline{C} \cdot (B \cdot C)}$	$\overline{C + A}$	$\overline{\overline{D} \cdot \overline{\overline{C} \cdot (B \cdot C)}}$	$\overline{\overline{C + A} \cdot \overline{B}}$	S
0	1	1	0	0	0
0	1	1	1	0	1
0	1	0	0	1	1
0	1	1	0	1	1
0	1	0	1	1	1
1	1	0	0	1	1
0	1	1	1	1	1
1	1	0	1	1	1
0	1	0	0	1	1
0	1	0	0	1	1
0	1	0	1	1	1
0	1	0	0	1	1
0	1	0	1	1	1
0	1	0	1	1	1
1	1	0	0	1	1
1	1	0	1	1	1

Ejemplo 3.1 *Un avión del aeropuerto internacional de El Salvador emplea un sistema para vigilar las rpm (revoluciones por minuto), presión y temperatura de motores usando censores que operan como sigue:*

1. *Salida del sensor* $R = 0$ *sólo cuando la velocidad es menor que* 4800 *rpm.*
2. *Salida del sensor de* $P = 0$ *sólo cuando la presión es menor que* 220 *psi.*
3. *Salida del sensor* $T = 0$ *solo cuando la temperatura es menor que* $200F$.

La siguiente figura muestra el circuito lógico que controla la luz de advertencia de la cabina para ciertas combinaciones del motor.

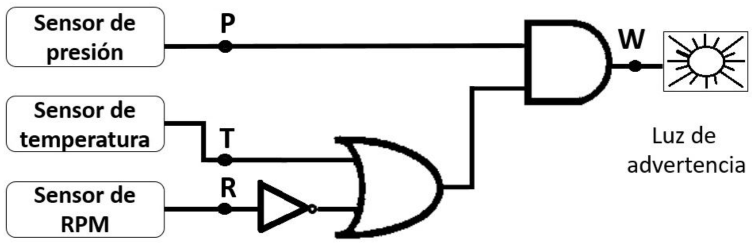


Figura 3.30: Circuito lógico que controla la luz de advertencia de la cabina
Fuente:
`http://service.udes.edu.co/modulos/documentos/pedropatino/compuertas.pdf`

Determinar que condiciones del motor advertirán al piloto.

Solución:

Primero se encuentra la ecuación lógica, haciendo uso de los circuitos logicos NOT, OR y AND.

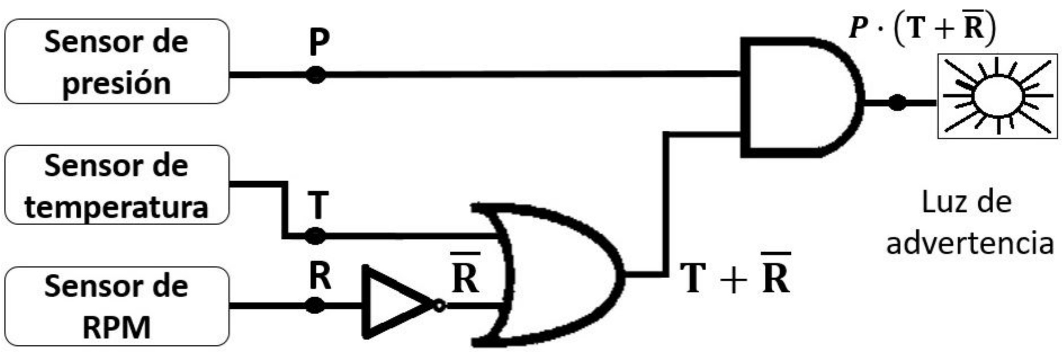


Figura 3.31: Solución del circuito lógico que controla la luz de advertencia de la cabina
Fuente: Creación propia en PowerPoint.

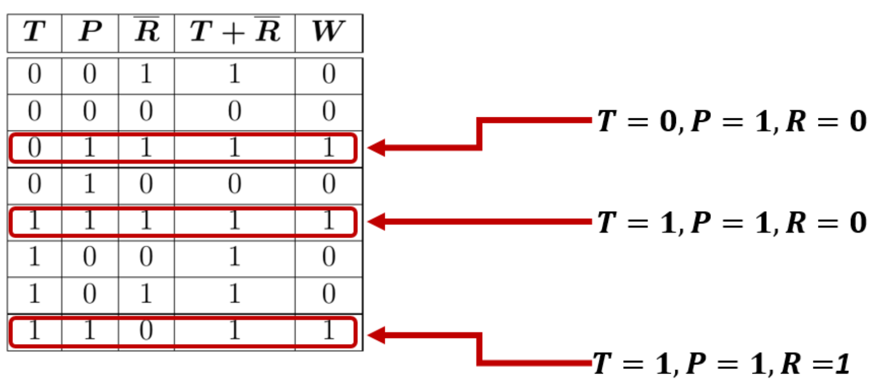
Como se observa en la figura, la salida es $P \cdot (T + \overline{R})$, y se denota por $W = P \cdot (T + \overline{R})$.

Tabla 23

Tabla de verdad correspondiente al circuito lógico.

T	P	$\overline{R}$	$T+\overline{R}$	W
0	0	1	1	0
0	0	0	0	0
0	1	1	1	1
0	1	0	0	0
1	1	1	1	1
1	0	0	1	0
1	0	1	1	0
1	1	0	1	1

Ahora, buscamos en la tabla aquellos valores cuya salida sea 1, pues cuando la salida es 1 es porque se encenderá la luz de advertencia. Véase Fig. 3.32.



T	P	$\overline{R}$	$T+\overline{R}$	W
0	0	1	1	0
0	0	0	0	0
0	1	1	1	1
0	1	0	0	0
1	1	1	1	1
1	0	0	1	0
1	0	1	1	0
1	1	0	1	1

Figura 3.32: Valores de W donde su valor es 1.
Fuente: Creación propia en PowerPoint.

Así, las condiciones cuando el motor advertirá al piloto se presentan en los siguientes casos:

Caso 1: Cuando las condiciones son: $T = 0, P = 1$ y $R = 0$ se tiene que la luz de advertencia se encenderá dado que, $T < 200F$, $P \geq 220psi$ y $R < 4800rpm$.

Caso 2: Cuando las condiciones son: $T = 1$, $P = 1$ y $R = 0$ se tiene que la luz de advertencia se encenderá dado que, $T \geq 200F$, $P \geq 220psi$ y $R < 4800rpm$.

Caso 3: Cuando las condiciones son: $T = 1$, $P = 1$ y $R = 1$ se tiene que la luz de advertencia se encenderá dado que, $T \geq 200F$, $P \geq 220psi$ y $R \geq 4800rpm$.

Ejemplo 3.2 *Supongamos la siguiente situación que deseamos resolver. Debemos identificar las entradas y salidas del sistema para poder obtener un circuito lógico que se ajuste a las especificaciones marcadas.*

Un sistema de aire acondicionado se puede poner en marcha mediante un interruptor (A) *manual. Se encenderá de forma automática, aunque el interruptor está apagado, cuando un termostato* (B) *detecte que la temperatura exterior pasa de* $30C$. *Existe también un detector* (C) *que desconecta el sistema, incluso estando el interruptor encendido, cuando la ventana está abierta.*

Diseñar el sistema electrónico que permite el control del aire acondicionado.

Solución:

Se necesita determinar primero los bloques de entrada y salida.

Entradas:

A: Interruptor manual. 0 = apagado, 1 = encendido.

B: Termostato. 0 si $T < 30C$, 1 si $T > 30C$.

C: Detector. 0 = ventanas cerradas, 1 = ventanas abiertas.

Salida:

S: Será la puesta en marcha o el apagado del sistema de aire acondicionado.

Dado a que ya están determinadas las entradas y la salida, obtenemos su correspondiente tabla de verdad para encontrar los valores de la salida que satisfagan las condiciones dadas para dicho sistema.

Tabla 24

Tabla de verdad del proceso del sistema

A	***B***	***C***	***S***
0	0	0	0
0	0	1	0
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	1
1	1	1	0

El sistema no funcionará ($S = 0$) cuando haya ventanas cerradas ($C = 1$) o cuando el interruptor esté apagado y tampoco haya temperatura alta en el exterior (A y $B = 0$). El resto de los casos la salida será 1.

Así, a continuación se presentan las salidas que cumplen las condiciones especificadas, en otras palabras nos da 1.

A	***B***	***C***	***S***
0	0	0	0
0	0	1	0
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	1
1	1	1	0

Figura 3.33: Selección de los datos donde la salida es 1.
Fuente: Creación propia en PowerPoint.

Teniendo estos valores en la tabla de verdad, se puede obtener la función lógica del sistema, la cual se debe de simplificar.

$$S = \overline{A}B\overline{C} + A\overline{B}\,\overline{C} + AB\overline{C}.$$

Podemos encontrar dos maneras diferentes de simplificar, ambas son correctas:

$$\begin{aligned} S &= \overline{A}B\overline{C} + A\overline{B}\,\overline{C} + AB\overline{C} \\ &= \overline{A}B\overline{C} + AB\overline{C} + A\overline{B}\,\overline{C} \\ &= B\overline{C}\left(A + \overline{A}\right) + A\overline{B}\,\overline{C} \\ &= B\overline{C} + A\overline{B}\,\overline{C} \end{aligned} \qquad \begin{aligned} S &= \overline{A}B\overline{C} + A\overline{B}\,\overline{C} + AB\overline{C} \\ &= \overline{A}B\overline{C} + A\overline{C}(\overline{B} + B) \\ &= \overline{A}B\overline{C} + A\overline{C} \end{aligned}$$

Optamos por la expresión $S = \overline{A}B\overline{C} + A\overline{C}$ y la implementamos mediante puertas lógicas. Así, su correspondiente circuito lógico es:

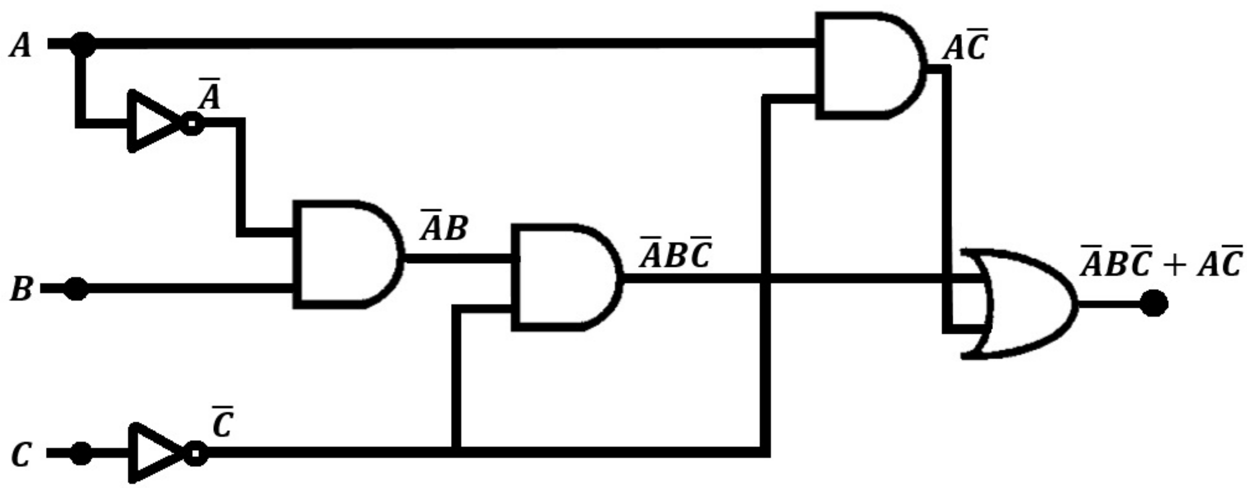


Figura 3.34: Circuito lógico que controla el aire acondicionado.
Fuente: Creación propia en PowerPoint.

3.2. El código genético y $\mathbb{Z}_2^6$

El código genético es el sistema bioquímico que permite establecer las reglas a través de las cuales la secuencia de nucleótidos de un gen es transcrita en la secuencia de codones del ARN mensajero (ARNm) y luego traducida en la secuencia de aminoácidos de la proteína correspondiente. Se le llama código genético al conjunto de las relaciones existentes entre codones y aminoácidos. Ver Figura 3.35.

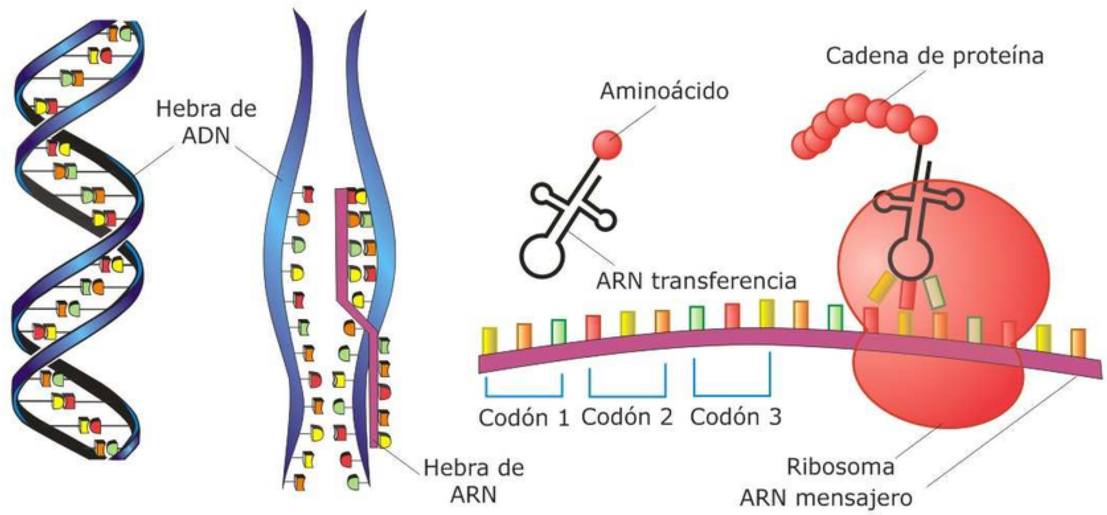


Figura 3.35: Reglas a través de las cuales la secuencia de nucleótidos de un gen es transcrita en la de codones del ARNm y traducida en la secuencia de aminoácidos de una proteína.
Fuente: `https://images.app.goo.gl/FTb2V5Pc6DseHZ2f8`

Nota: El conjunto de codones es una extensión del alfabeto de cuatro letras de la molécula de ADN. Estas letras son las moléculas básicas del ADN: Adenina (A), Guanina (G), Citosina (C) y Timina (T).

Si cada nucleótido determinara un aminoácido, solamente podríamos codificar cuatro aminoácidos diferentes ya que en el ADN solamente hay cuatro nucleótidos distintos (A, G, T y C). Cifra muy inferior a los 20 aminoácidos distintos que existen. El código genético funciona de manera que cada cadena de ADN se lee de tres en tres nucleótidos, de manera que cada grupo de tres nucleótidos determina un aminoácido.

Teniendo en cuenta que existen cuatro nucleótidos diferentes (A, G, T y C), el número de grupos de tres nucleótidos distintos que se pueden obtener son variaciones con repetición de cuatro elementos (los cuatro nucleótidos) tomando de tres en tres son: $VR_{4,3} = 4^3 = 4 \times 4 \times 4 = 64$. Por consiguiente, existe un total de 64 tripletes diferentes, cifra más que suficiente para codificar los 20 aminoácidos distintos. Las bases nitrogenadas se parean en la hélice del ADN de acuerdo a los puentes de hidrógeno: G con C (tres puentes) y A con T (dos puentes). Ver Figura 3.36

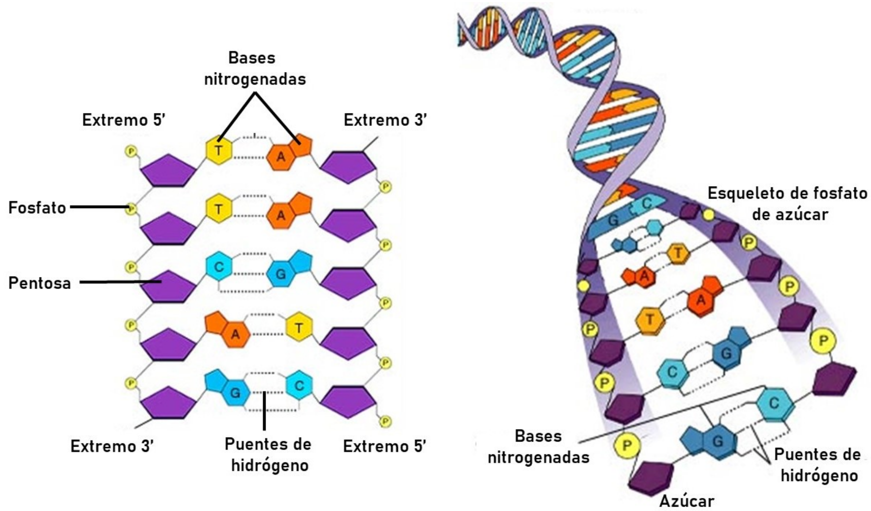


Figura 3.36: Base de nucleótidos del ADN
Fuente: `https://images.app.goo.gl/viMnxUGZXRoZzhc97`

El ARN mensajero es el ácido ribonucleico que contiene la información genética (el código genético) procedente del ADN del núcleo celular a un ribosoma en el citoplasma, es decir, el que determina el orden en que se unirán los aminoácidos y actúa como plantilla o patrón para la síntesis de proteínas, ver Figura 3.35. Similarmente al caso del ADN, las moléculas básicas del ARNm son representadas por las letras A,G,C y U, correspondientes a la Adenina, la Guanina, la Citosina y el Uracilo respectivamente, (se sabe que en el ARNm la Timina es sustituida por el Uracilo). En la Figura 3.37 se presenta las diferencias entre ADN y ARN.

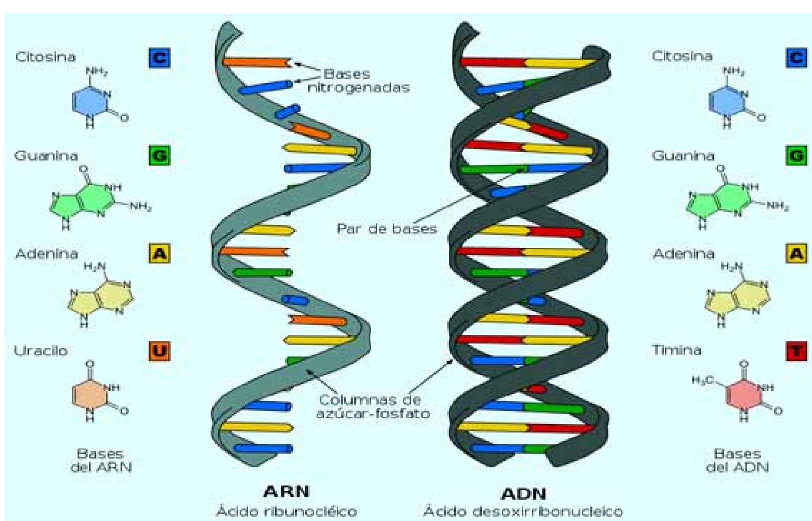


Figura 3.37: ARN mensajero vs. ADN
Fuente: `https://images.app.goo.gl/wMV5Sp12y2GNwMSTA`

En el transcurso de la historia han existido varios intentos para introducir caracterizaciones formales (incluso algebraicas) del código genético, recientemente se ha podido ilustrar una representación de ARNm en términos del álgebra booleana y $\mathbb{Z}_2^6$, dicha caracterización involucra la representación binaria de las cuatro bases nitrogenadas del ARNm y un orden sugerido para ellas.

Sea $X = \{U, C, G, A\}$,el conjunto de las cuatro bases del ARNm (ácido ribonucleico mensajero). Dotaremos al conjunto X de un orden y una estructura booleana de la siguiente manera:

1. Se parte de que cualquier retículo booleano $(B(X), \vee, \wedge)$, construido a partir del conjunto X, definiendo para dos elementos $\alpha, \beta \in X$, $\alpha \leq \beta$ si y sólo si $\alpha' \vee \beta = 1$ o equivalentemente, $\alpha \wedge \beta' = 0$, donde 1 es el elemento máximo del retículo booleano y el 0 el elemento mínimo. Además, si $\alpha \leq \beta$ o $\alpha \geq \beta$ se dice que los elementos α y β son comparables. Dos elementos $\alpha, \beta \in X$. se dicen complementarios si y sólo si $\alpha \vee \beta = 1$ y $\alpha \wedge \beta = 0$.
2. Es conocido también que en cualquier retículo booleano con cuatro elementos todos los elementos son comparables excepto dos de ellos, que son complementarios.
3. El retículo booleano de las cuatro bases nitrogenadas $X = \{U, C, G, A\}$ se construye asumiendo que las bases complementarias en el retículo son también complementarias (apareadas) en la molécula del ADN. Este retículo de cuatro bases debe tener un máximo, un mínimo y dos elementos no comparables.

Sea $X = \{U, C, G, A\}$ el conjunto de las cuatro bases nitrogenadas, a partir de este conjunto construiremos un retículo booleano mediante las siguientes observaciones.

a) Ambos codones, GGG y CCC tienen el mismo número máximo de puentes de hidrógeno. Esta propiedad debe estar reflejada en el retículo de manera que GGG sea complementario a CCC. Además, ambos codifican para cadenas de aminoácidos pequeñas con poca diferencia en la polaridad: Glicina y prolina. Esta propiedad de similaridad determina que estos elementos son comparables.

b) UUU y AAA tienen el mismo número mínimo de puentes de hidrógeno entre ellos, y por tanto, el elemento complementario de UUU en el retículo es AAA. Pero estas tripletas codifican respectivamente para cadenas de aminoácidos con polaridades opuestas extremas (Leucina y Lisina). Consecuentemente esta propiedad opuesta determina que estos elementos no son comparables.

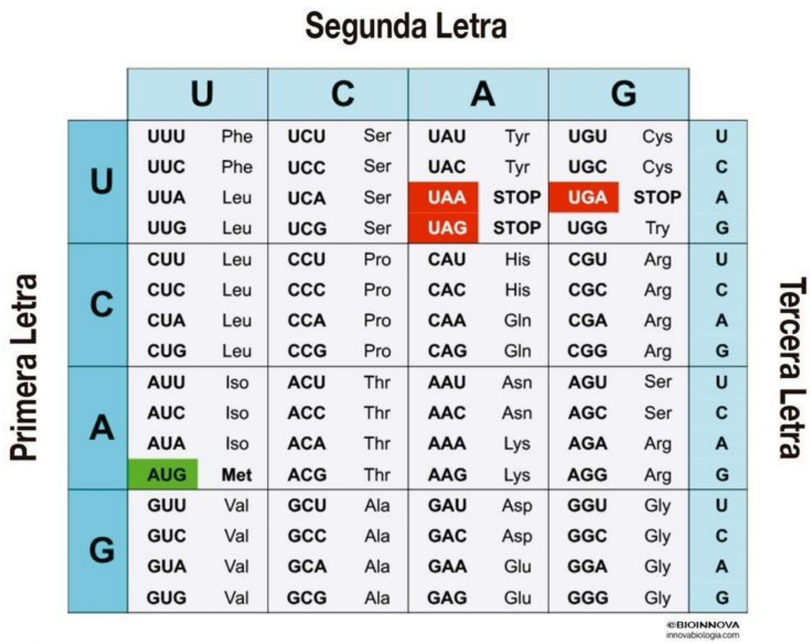
Así, existen solamente dos posibilidades para el retículo de las cuatro bases nitrogenadas. Del literal a) resulta que el mínimo elemento es G y máximo C o al contrario el mínimo es C y el máximo es G, y de b) resulta que U y A no son comparables, y en particular no pueden ser mínimo o máximo si queremos tal significado biológico. Con estas observaciones surgen dos retículos para las bases nitrogenadas llamados convencionalmente retículo primal, $B(X) = \{G, A, U, C\}$ con el orden $G \leq A \leq U \leq C$, y el retículo dual, $\overline{B}(X) = \{C, U, A, G\}$ con el orden $C \leq U \leq A \leq G$. Trabajaremos con el retículo primal. Es importante destacar, que el significado biológico de los retículos primal y dual es el mismo.

Dado que $B(X)$ es un retículo complementado y distributivo, entonces $B(X)$ es un álgebra booleana. Desde un punto de vista algebraico el álgebra booleana $(B(X), \vee, \wedge)$ es isomorfa a $\mathbb{Z}_2^2$. Esto resulta del hecho de que todo par de retículo booleanos con la misma cardinalidad son isomorfos. Por lo tanto, es posible establecer un isomorfismo booleano $\varphi : B(X) \longrightarrow \mathbb{Z}_2^2$ dado por:

$$\varphi(x) := \begin{cases} (\overline{0}, \overline{0}) & \text{si } x = G, \\ (\overline{0}, \overline{1}) & \text{si } x = A, \\ (\overline{1}, \overline{0}) & \text{si } x = U, \\ (\overline{1}, \overline{1}) & \text{si } x = C. \end{cases}$$

Partiremos del conjunto de las cuatro bases nitrogenadas del ARNm para llegar al conjunto de los 64 codones del código genético. La idea es obtener un retículo booleano para los codones del código genético, recordemos que los codones son tripletas formadas por los elementos de X, con $X = \{U, C, G, A\}$ y cada codón codifica al menos un aminoácido, este retículo es inducido por el retículo de las cuatro bases nitrogenadas del ARNm, $B(X)$.

Sea $C(X) = \{GGG, ..., CCC\}$. El retículo de los codones del código genético, con el orden $GGG \leq, ..., \leq CCC$, además, $1 := CCC$ y $0 := GGG$. Al igual que $B(X)$, $C(X)$ es un álgebra booleana ya que es un retículo complementado y distributivo. En la figura 3.38 se muestra los 64 codones del ARNm.



Segunda Letra

Primera Letra	U		C		A		G		Tercera Letra
U	UUU	Phe	UCU	Ser	UAU	Tyr	UGU	Cys	U
	UUC	Phe	UCC	Ser	UAC	Tyr	UGC	Cys	C
	UUA	Leu	UCA	Ser	UAA	STOP	UGA	STOP	A
	UUG	Leu	UCG	Ser	UAG	STOP	UGG	Try	G
C	CUU	Leu	CCU	Pro	CAU	His	CGU	Arg	U
	CUC	Leu	CCC	Pro	CAC	His	CGC	Arg	C
	CUA	Leu	CCA	Pro	CAA	Gln	CGA	Arg	A
	CUG	Leu	CCG	Pro	CAG	Gln	CGG	Arg	G
A	AUU	Iso	ACU	Thr	AAU	Asn	AGU	Ser	U
	AUC	Iso	ACC	Thr	AAC	Asn	AGC	Ser	C
	AUA	Iso	ACA	Thr	AAA	Lys	AGA	Arg	A
	AUG	Met	ACG	Thr	AAG	Lys	AGG	Arg	G
G	GUU	Val	GCU	Ala	GAU	Asp	GGU	Gly	U
	GUC	Val	GCC	Ala	GAC	Asp	GGC	Gly	C
	GUA	Val	GCA	Ala	GAA	Glu	GGA	Gly	A
	GUG	Val	GCG	Ala	GAG	Glu	GGG	Gly	G

©BIOINNOVA
innovabiologia.com

Figura 3.38: Tripletas o codones del ARNm.
Fuente: `https://images.app.goo.gl/ki6oAbQkMKahGkZu7`

Sea $C(X)$ el álgebra booleana inducida para los codones, es decir, el álgebra inducida para los codones a partir de $B(X)$. Usando el hecho de que el producto cartesiano finito de álgebras booleanas es un álgebra booleana, se obtiene que $C(X)$ es isomorfa a $B(X) \times B(X) \times B(X)$. Pero, ya que $B(X) \cong \mathbb{Z}_2^2$, se obtiene que:

$$C(X) \cong B(X) \times B(X) \times B(X) \cong \mathbb{Z}_2^2 \times \mathbb{Z}_2^2 \times \mathbb{Z}_2^2 \cong \mathbb{Z}_2^6.$$

Para definir un isomorfismo booleano $\Psi : C(X) \longrightarrow \mathbb{Z}_2^6$. podemos partir del isomorfismo $\varphi : B(X) \longrightarrow \mathbb{Z}_2^2$ anteriormente definido, procediendo de la forma siguiente: a cada codón Ψ le asigna una 6-tupla correspondiente a un elemento de $\mathbb{Z}_2^2$, la cual se compone precisamente de las imágenes de φ en cada una de las componente del codón.

Así que, por ejemplo:

$$GUC \vee CAG = CCC \longmapsto (0,0,1,0,1,1) \vee (1,1,0,1,0,0) = (1,1,1,1,1,1),$$

$$GUC \wedge CAG = GGG \longmapsto (0,0,1,0,1,1) \wedge (1,1,0,1,0,0) = (0,0,0,0,0,0),$$

$$\sim (GUC) = CAG \longmapsto \sim (0,0,1,0,1,1) = (1,1,0,1,0,0).$$

Así, Ψ se define para cada codón de $C(X)$ como se ilustra en la figura 3.39.

Sea $\Psi : C(X) \longrightarrow \mathbb{Z}_2^6$. dada por:

Figura 3.39: Los 16 codones del ARNm asociados a la Guanina (G) y sus correspondientes imágenes por Ψ.

Fuente: Quintana, Y., & Hernández, S. Estructuras booleanas y el código genético: algunos comentarios.

De igual manera se define para las tres bases restante. El isomorfismo $\Psi : C(X) \longrightarrow \mathbb{Z}_2^6$. permite realizar operaciones lógicas entre nucleótidos y codones, término a término, estas operaciones son precisamente permutaciones de los elementos de $\mathbb{Z}_2^6$. Cada permutación de $\mathbb{Z}_2^6$. representa una mutación en el código genético. De esta conclusión surgen las siguientes preguntas. ¿Acaso cada permutación implica un cambio en el orden en que se unirán los aminoácidos para sintetizar una proteína determinada?, ¿es posible que cada permutación de $\mathbb{Z}_2^6$ altere el correcto plegamiento de las proteínas? Estás preguntas son inquietudes que nos han surgido en el desarrollo de esta aplicación.

Bibliografía

[1] María Mercedes Chacara Montes, Anillos e ideales booleanos en la fundamentación de un modelo no estándar y una aplicación, Universidad de sonora, 1994.

[2] Vidal, J. C. Álgebras booleanas y lógica proposicional. Álgebras de Halmos y lógica de predicados, 2001.

[3] Smith, D., & Eggen, M. Richard St Andre. A Transition to Advanced Mathematics, 2014.

[4] Hasser, N. B., La Salle, J., & Sullivan, J. Análisis Matemático Vol. 1. Editorial Trillas, 2009.

[5] Mendelson, E. Theory and problem of boolean algebra and switching circuits, 1970.

[6] Givant, S., & Halmos, P. Introduction to Boolean algebras. Springer Science & Business Media, 2008.

[7] Edwin Caguate. 1184_ compuertas-logicas. Disponible aquí.

[8] Pedro Patino. Compuertas. Disponible aquí.

[9] Quintana, Y., & Hernandez, S. Estructuras booleanas y el codigo genetico: algunos comentarios. Revista MATUA ISSN: 2389-7422, 2(2), 2015.