Lógica

Universidad Internacional de Valencia

Máster Universitario en Inteligencia Artificial

02MIAR | Matemáticas:
Matemáticas para la Inteligencia Artificial

Profesor:
Víctor M. Campello

universidadviu.com

De:
Planeta Formación y Universidades

Lógica proposicional

Universidad Internacional de Valencia

Definición

Un **enunciado lógico** *o* **proposición lógica** *consiste en una afirmación a la cual se le puede atribuir un* **valor de verdad**, *pudiendo ser este verdadero (1) o falso (0).*

Ejemplos

1. *La proposición "*$2 + 2 = 4$*" tiene valor de verdad* 1.
2. *La proposición "*$4 > 5$*" tiene valor de verdad* 0.
3. *La proposición "todo número par mayor que 2 se puede escribir como la suma de dos números primos" (conjetura de Goldbach) tiene un valor de verdad desconocido.*
4. *La proposición "existe vida inteligente fuera de la Tierra" tiene un valor de verdad desconocido.*
5. *"La mesa de Antonio" no es una proposición lógica.*

Definición

Dados dos enunciados lógicos p y q, se define la **conjunción** *entre p y q a un nuevo enunciado lógico, denotado por $p \wedge q$ y leído como "p y q", cuyo valor de verdad es verdadero siempre y cuando ambos enunciados lo sean simultáneamente.*

La **tabla de verdad** correspondiente es, por tanto:

p	q	$p \cdot q$
1	1	1
1	0	0
0	1	0
0	0	0

El conector $\wedge$ se puede identificar con la operación "$\cdot$", producto.

Definición

Dados dos enunciados lógicos p y q, se define la **disyunción** *entre p y q a un nuevo enunciado lógico, denotado por $p \vee q$ y leído como "p o q", cuyo valor de verdad es verdadero siempre y cuando alguno de los dos enunciados (o ambos) lo sean.*

La tabla de verdad correspondiente es, por tanto:

p	q	$p + q$
1	1	1
1	0	1
0	1	1
0	0	0

El conector $\vee$ se puede identificar con la operación "$+$", suma.

Definición

Dados dos enunciados lógicos p y q, se define la **implicación lógica**, *leída como "p implica q" y denotada por $p \to q$, cuyo valor de verdad está en consonancia con el hecho de que si se da p, entonces necesariamente ha de darse también q, estableciendo de ese modo una relación de causalidad entre ambos enunciados.*

La tabla de verdad correspondiente es, por tanto:

p	q	$p \to q$
1	1	1
1	0	0
0	1	1
0	0	1

Definición

Dados dos enunciados lógicos p y q, se define la **equivalencia**, **bicondicional** *o* **implicación doble**, *leída como "p si y sólo si q" y denotada por $p \leftrightarrow q$, cuyo valor de verdad está en consonancia con el hecho de que si se da p, entonces necesariamente ha de darse también q y viceversa, si se da q, entonces también debe darse p.*

La tabla de verdad correspondiente es, por tanto:

p	q	$p \leftrightarrow q$
1	1	1
1	0	0
0	1	0
0	0	1

Definición

Dado un enunciado lógico p, se define la **negación** *lógica como el resultado de invertir el valor de verdad del enunciado original, denotándose por* $\neg p$ *(y leído como "no p").*

p	$\overline{p}$
1	0
0	1

La negación de un enunciado p, además de $\neg p$, también puede denotarse por $\overline{p}$.

Definición

Una **fórmula lógica** $F(p_1, p_2, \ldots, p_k)$ *consiste en una serie de enunciados lógicos conectados por diferentes conectores lógicos. Según su valor de verdad, puede ser de tres tipos:*

- **Tautológica:** *si* $F(p_1, p_2, \ldots, p_k)$ *tiene valor de verdad* 1 *independientemente de la combinación de valores de verdad de* $p_1, p_2, \ldots, p_k$.
- **Contradictoria:** *si* $F(p_1, p_2, \ldots, p_k)$ *tiene valor de verdad* 0 *independientemente de la combinación de valores de verdad de* $p_1, p_2, \ldots, p_k$.
- **Contingente:** *si* $F(p_1, p_2, \ldots, p_k)$ *tiene valor de verdad* 0 *para ciertas combinaciones de valores de verdad de* $p_1, p_2, \ldots, p_k$, *mientras que vale* 1 *para otras combinaciones.*

Ejemplos

1. $p + \overline{p}$ *es una tautología.*
2. $p \cdot \overline{p}$ *es una contradicción.*
3. $\overline{p}$ *es contingente.*
4. $p \rightarrow p$ *es una tautología.*
5. $p \rightarrow \overline{p}$ *es contingente.*
6. $p \cdot q$ *es contingente.*
7. $p \leftrightarrow \overline{p}$ *es una contradicción.*
8. $(p \cdot q) \rightarrow (p + q)$ *es una tautología.*
9. $(p + q) \rightarrow (p \cdot q)$ *es contingente.*
10. $\overline{p \leftrightarrow p}$ *es una contradicción.*

Lógica proposicional

Definición

Dos fórmulas lógicas son **equivalentes** *si su valor de verdad es coincidente para cualquier combinación de valores de las proposiciones lógicas que la integran.*

Por ejemplo, $p \to q$ es equivalente a $\overline{p} + q$:

p	q	$p \to q$	$\overline{p}$	$\overline{p} + q$
1	1	1	0	1
1	0	0	0	0
0	1	1	1	1
0	0	1	1	1

Ejercicio

Probar que $p \to q$ no es equivalente a su **recíproco**, $q \to p$, *pero sí que es equivalente a su* **contrarrecíproco**, $\overline{q} \to \overline{p}$.

Universidad Internacional de Valencia

Propiedades

- $p \cdot (q \cdot r) = (p \cdot q) \cdot r, \quad p + (q + r) = (p + q) + r.$
- $p \cdot q = q \cdot p, \quad p + q = q + p.$
- $p \cdot (q + r) = (p \cdot q) + (p \cdot r), \quad p + (q \cdot r) = (p + q) \cdot (p + r).$
- $p \cdot \overline{p} = 0, \quad p + \overline{p} = 1.$
- $p \cdot 0 = 0, \quad p + 1 = 1.$
- $p \cdot 1 = p, \quad p + 0 = p.$
- $p \cdot p = p, \quad p + p = p.$
- $p \cdot (p + q) = p, \quad p + (p \cdot q) = p.$
- $\overline{\overline{p}} = p.$
- $\overline{p \cdot q} = \overline{p} + \overline{q}$ *(ley de De Morgan).*
- $\overline{p + q} = \overline{p} \cdot \overline{q}$ *(ley de De Morgan).*

Teoría de conjuntos

Definición

Un **conjunto** *es una colección de objetos físicos o abstractos. Cada uno de estos objetos recibe el nombre de* **elemento**.
Si A es un conjunto, denotamos $a \in A$ a la relación "a es un elemento de A" o, equivalentemente, "a pertenece a A".

Cada conjunto se denota entre llaves separando cada elemento con una coma.

Ejemplos

1. *Conjunto de los planetas del sistema solar:*
   $\{\text{Mercurio}, \text{Venus}, \text{Tierra}, \text{Marte}, \text{Júpiter}, \text{Saturno}, \text{Urano}, \text{Neptuno}, \text{Plutón}\}$.
2. *Conjunto de los números naturales impares:*
   $\{1, 3, 5, 7, 9, 11, \ldots\} = \{2n - 1 \mid n \in \mathbb{N}\}$.

Definición

El **cardinal** *de un conjunto es el número de elementos que posee. Si A es un conjunto, su cardinal se denota por $|A|$.*

En caso de que un conjunto A tenga una infinidad de elementos, denotamos $|A| = \infty$.

Ejemplos

1. *Sea A el conjunto de los planetas del sistema solar. Entonces $|A| = 9$.*
2. *Sea B el conjunto dado por los números naturales impares. Entonces $|B| = \infty$.*

Teoría de conjuntos

- Cada uno de los elementos de un conjunto sólo debe aparecer una única vez.

Ejemplo

El conjunto $\{a, b, c, c, d, a\}$ *no está bien denotado, ya que hay elementos repetidos. Lo correcto sería denotarlo por* $\{a, b, c, d\}$.

- El conjunto formado por cero elementos recibe el nombre de **conjunto vacío** y se denota por $\emptyset$.

Ejemplo

Sea A *el conjunto de satélites de Venus. Entonces* $A = \emptyset$, *ya que Venus no tiene ningún satélite.*

Lógica de predicados

- Algunas afirmaciones lógicas encierran una estructura más compleja.
- La lógica proposicional es limitada en estos casos.
- La **lógica de primer orden** se encarga de analizar enunciados con **predicados**.

Ejemplos

- $x < 4$.
- *Para todo entero x, si x es múltiplo de 4 entonces x es par.*
- *Todos los planetas tienen una órbita elíptica.*
- *Existe un entero z tal que $z = z + 1$.*
- *Si $x \in \mathbb{Z}$, entonces $x \in \mathbb{N}$.*

Lógica de predicados

Definición

Un **predicado** $p(x_1, x_2, \ldots, x_n)$ *es una afirmación que hace referencia a una propiedad o una relación entre objetos* $x_1, x_2, \ldots, x_n$*, de forma que al sustituirlos por valores concretos,* $c_1, c_2, \ldots, c_n$*, el resultado de reemplazar dichos objetos por los valores correspondietes es una afirmación lógica,* $p(c_1, c_2, \ldots, c_n)$*, la cual dispone de un valor de verdad, que depende de los valores* c_i*.*

Ejemplos

1. *Sea* $p(x)$ *la afirmación "*x *es un reptil". Entonces, por ejemplo,* $p(\text{serpiente})$ *es verdadera, mientras que* $p(\text{gato})$ *es falsa.*
2. *Tomemos* $p(x, y)$ *la afirmación "*$x + y = 3$*". Entonces, por ejemplo,* $p(1, 2)$ *es verdadera, mientras que* $p(1, 1)$ *no lo es.*

Definición

Si $p(x)$ es un predicado, la afirmación "para todo x, $p(x)$" es una proposición que indica que cualquier valor de $x \in \mathcal{U}$ verifica $p(x)$. El símbolo que denota esta relación es "$\forall$" y recibe el nombre de **cuantificador universal**. *En este caso, la afirmación anterior puede expresarse como $\forall x, p(x)$ o $\forall x \in \mathcal{U}, p(x)$.*

- En la cuantificación universal pueden utilizarse tantas variables como se necesite. Por ejemplo, para expresar "para todo x e y, $p(x, y)$", puede utilizarse indistintamente $\forall x, \forall y, p(x, y)$ o bien $\forall x, y, p(x, y)$.
- Una afirmación universalmente cuantificada es verdadera cuando p se cumple para todos los valores cuantificados.
- En caso contrario (existencia de algún valor o valores que no la cumplan) es falsa.

Ejemplos

Transcribamos formalmente las siguientes afirmaciones:

1. *"El cuadrado de todo número real es mayor o igual que* 0*":*

$$\forall x \in \mathbb{R}, x^2 \geq 0.$$

   Esta afirmación puede expresarse en general de la forma $\forall x, p(x)$*, donde* $\mathcal{U} = \mathbb{R}$ *y* $p(x)$: "$x^2 \geq 0$".

2. *"Todo par de números enteros verifica que su suma es positiva":*

$$\forall x, y \in \mathbb{Z}, x + y > 0.$$

   En este caso, puede expresarse como $\forall x, y, p(x, y)$*, con* $\mathcal{U} = \mathbb{Z}$ *y* $p(x, y)$: $x + y > 0$.

Definición

Si $p(x)$ es un predicado, la afirmación "existe un x tal que $p(x)$" es una proposición que indica la existencia de algún valor de $x \in \mathcal{U}$ verificando $p(x)$. El símbolo que denota esta relación es "$\exists$" y recibe el nombre de **cuantificador existencial**. *En este caso, la afirmación anterior puede expresarse como $\exists x : p(x)$ o $\exists x \in \mathcal{U} : p(x)$.*

- En la cuantificación existencial pueden utilizarse tantas variables como se necesite. Por ejemplo, para expresar "existen x e y tal que $p(x, y)$", puede utilizarse indistintamente $\exists x, \exists y : p(x, y)$ o bien $\exists x, y : p(x, y)$.
- Una afirmación existencialmente cuantificada es verdadera cuando p se cumple para algún valor cuantificado.
- En caso contrario (inexistencia de valores que la cumplan) es falsa.

Ejemplos

Transcribamos formalmente las siguientes afirmaciones:

1. *"Existe un valor real cuyo cuadrado es igual a* -1*":*

$$\exists x \in \mathbb{R} : x^2 = -1.$$

   Esta afirmación puede expresarse en general de la forma $\exists x : p(x)$, *donde* $\mathcal{U} = \mathbb{R}$ *y* $p(x)$: "$x^2 = -1$".

2. *"Existen un par de números enteros tales que su suma es igual a* 10*":*

$$\exists x, y \in \mathbb{Z} : x + y = 10.$$

   En este caso, puede expresarse como $\exists x, y : p(x, y)$, *con* $\mathcal{U} = \mathbb{Z}$ *y* $p(x, y)$: $x + y = 10$.

Nota

Los dos tipos de cuantificadores pueden combinarse de cualquier forma; no obstante, el orden en el que aparecen es **crucial**, *puesto que* **NO** *conmutan.*

Ejemplo

Consideremos las dos afirmaciones siguientes:

1. $\forall x \in \mathbb{N}, \exists y \in \mathbb{N} : y > x$.
   "*Para todo número natural, existe otro natural tal que este último es mayor que el primero*".
2. $\exists y \in \mathbb{N} : \forall x \in \mathbb{N}, y > x$.
   "*Existe un número natural tal que es mayor que el resto de números naturales*".

Lógica de predicados

Definición

Sean A y B dos afirmaciones lógicas. Diremos que A **implica lógicamente** *B, y lo denotaremos por $A \vDash B$, si se cumple que B es verdadera siempre que A lo sea.*

Ejemplo

Sea A la afirmación "$x > 4$" y B la afirmación "$x > 3$".

- *$A \vDash B$, ya que si un valor es mayor que 4 también es mayor que 3.*
- *$B \nvDash A$, puesto que, por ejemplo, tomando $x = 4$, se tiene que B es verdadero ($4 > 3$), pero no A ($4 \not> 4$).*

Definición

Sean A y B dos afirmaciones lógicas. Diremos que A **equivale lógicamente** *a B, y lo denotaremos por $A \equiv B$ se tiene que $A \vDash B$ y viceversa, $B \vDash A$.*

Ejemplos

1. *Sea A la afirmación "$x = y$" y B la afirmación "$x - y = 0$". Entonces $A \equiv B$.*
2. *Sea A la afirmación "$\forall x, p(x)$" y B la afirmación "$\exists x : p(x)$". Entonces $A \not\equiv B$, ya que $B \nvDash A$ (si bien $A \vDash B$).*
3. *Consideremos A "$\forall x, y, x + y > 0$" y B "$\forall x, y, x \cdot y < 0$". Entonces $A \not\equiv B$ ($A \nvDash B$ y $B \nvDash A$).*

Propiedades

Se cumplen las siguientes relaciones:

1. $\forall x, [p(x) \vee q(x)] \Dashv [\forall x, p(x)] \vee [\forall x, q(x)]$.
2. $\exists x : [p(x) \vee q(x)] \equiv [\exists x : p(x)] \vee [\exists x : q(x)]$.
3. $\forall x, [p(x) \wedge q(x)] \equiv [\forall x, p(x)] \wedge [\forall x, q(x)]$.
4. $\exists x : [p(x) \wedge q(x)] \models [\exists x : p(x)] \wedge [\exists x : q(x)]$.

Ejemplos

1. *Consideremos la afirmación "todo número natural es par o bien impar" (verdadera), la cual puede transcribirse como* $\forall x \in \mathbb{N}, [p(x) \vee q(x)]$*, siendo* $p(x)$: *"x es par" y* $q(x)$: *"x es impar".*

   No obstante, la afirmación $[\forall x \in \mathbb{N}, p(x)] \vee [\forall x \in \mathbb{N}, q(x)]$ *se lee como*

   "todo número natural es par, o bien todo número natural es impar"

   (falsa, por ser una disyunción de dos proposiciones falsas).

Lógica de predicados

Ejemplos

2. *Sea* $A = \{1, 2, 3, 4, 5\}$ *y la afirmación "existe algún número en* A *que es múltiplo de* 2 *y* 3 *simultáneamente" (falsa). Ésta puede leerse como* $\exists x \in A : [p(x) \wedge q(x)]$, *donde* $p(x)$: *"*x *es múltiplo de* 2*" y* $q(x)$: *"*x *es múltiplo de* 3*".*

   No obstante, la afirmación $[\exists x \in A : p(x)] \wedge [\exists x \in A : q(x)]$ *se lee como*

   "existe un múltiplo de 2 *en* A *y existe un múltiplo de* 3 *en* A*"*

   (verdadera, por ser una conjunción de dos proposiciones verdaderas).

Teorema

Se cumplen las siguientes **leyes de De Morgan generalizadas***:*

1. $\neg[\forall x, p(x)] \equiv \exists x : \neg p(x)$.
2. $\neg[\exists x : p(x)] \equiv \forall x, \neg p(x)$.
3. $\forall x, p(x) \equiv \neg[\exists x : \neg p(x)]$.
4. $\exists x : p(x) \equiv \neg[\forall x, \neg p(x)]$.

Ejemplos

1. $\forall x, \neg[\exists y : [p(x,y) \to q(x)]]$.

$$\forall x, \neg[\exists y : [\neg p(x,y) \vee q(x)]]$$

$$\forall x, \forall y, \neg[\neg p(x,y) \vee q(x)]$$

$$\forall x, \forall y, [\neg[\neg p(x,y)] \wedge \neg q(x)]$$

$$\forall x, \forall y, [p(x,y) \wedge \neg q(x)]$$

$$\forall x, y, [p(x,y) \wedge \neg q(x)]$$

Ejemplos

2. *Consideremos el enunciado "no es cierto que todo entero sea simultáneamente par y positivo":*

$$\neg[\forall x \in \mathbb{Z}, [p(x) \wedge q(x)]],$$

donde $p(x)$: *"*x *es par", $q(x)$: "*x *es positivo".*

$$\exists x \in \mathbb{Z} : \neg[p(x) \wedge q(x)]$$
$$\exists x \in \mathbb{Z} : \neg p(x) \vee \neg q(x),$$

siendo por tanto el enunciado equivalente "existe algún número entero tal que o bien es impar o bien no es positivo".

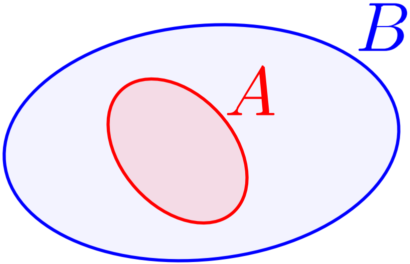
Teoría de conjuntos (parte II)

Definición

Un conjunto A está **incluido** *en otro conjunto B ($A \subseteq B$), o bien que B* **incluye** *A, si todo elemento de A pertenece también a B, es decir:*

$$A \subseteq B \text{ si } \forall x \in A, x \in B.$$

En caso contrario, diremos que $A \not\subseteq B$.



Teoría de conjuntos (parte II)

Ejemplos

1. *Sea* $A = \{a, b, c\}$ *y* $B = \{a, b, c, d\}$. *Entonces* $A \subseteq B$, *ya que todo elemento de* A *está en* B.
   Por otra parte, $B \nsubseteq A$, *ya que por ejemplo* $d \in B$ *pero* $d \notin A$.

2. *Sea* $A = \{1, 3, 4\}$ *y* $B = \{1, 2, 4\}$. *Entonces no se cumple ninguna relación de inclusión.*
   2.1 $A \nsubseteq B$, *ya que* $3 \in A$, *pero* $3 \notin B$.
   2.2 $B \nsubseteq A$, *puesto que* $2 \in B$, *pero* $2 \notin A$.

3. $\emptyset \subseteq A \; \forall A$ *conjunto.*

Teoría de conjuntos (parte II)

Definición

Dos conjuntos A y B son iguales ($A = B$) si todo elemento de A está en B y viceversa. Dicho de otro modo, diremos que $A = B$ si $A \subseteq B$ y $B \subseteq A$. En caso contrario, escribimos $A \neq B$.

Ejemplos

- *$\forall A$ conjunto, $A = A$.*
- *Sean $A = \{a, b, c\}$ y $B = \{b, c, a\}$. Entonces $A = B$, ya que se cumple que $A \subseteq B$ y a la vez $B \subseteq A$.*
- *Sean $A = \{a, b, c\}$ y $B = \{a, b, c, d\}$. Entonces $A \neq B$, ya que $B \nsubseteq A$.*

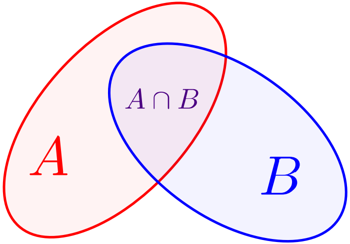
Teoría de conjuntos (parte II)

Definición

La **intersección** *entre dos conjuntos A y B, denotada por $A \cap B$, es un nuevo conjunto formado por los elementos en común de A y B.*

$$A \cap B = \{x \mid x \in A \wedge x \in B\}.$$

Si A y B no tienen ningún elemento en común, entonces $A \cap B = \emptyset$ y se dice que en ese caso A y B son **disjuntos**.



Teoría de conjuntos (parte II)

Ejemplos

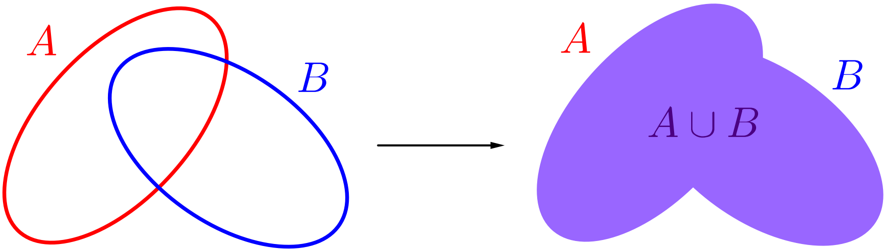
1. *Sean* $A = \{-1, 3, 5, 2, 6, 9\}$ *y* $B = \{-1, 0, 4, 3, 7, 9, 10\}$. *Entonces*
$$A \cap B = \{-1, 3, 9\}.$$
2. *Consideremos ahora* $A = \{a, b, c\}$ *y* $B = \{c, d, e\}$. *En este caso, se tiene*
$$A \cap B = \{c\}.$$
3. *Tomemos* $A = \{a, b, c\}$ *y* $B = \{d, e, f\}$. *Entonces* A *y* B *no tienen elementos comunes, luego* $A \cap B = \emptyset$.
4. *Sean* $A = [-1, 1]$ *y* $B =]0, 2]$. *Entonces* $A \cap B =]0, 1]$.
5. *Si* $A = [0, 1]$ *y* $B = [1, 2]$ *entonces* $A \cap B = \{1\}$.

Teoría de conjuntos (parte II)

Definición

La **unión** *entre dos conjuntos A y B, denotada por $A \cup B$, es un nuevo conjunto formado por todos los elementos de A y B.*

$$A \cup B = \{x \mid x \in A \vee x \in B\}.$$



Teoría de conjuntos (parte II)

Ejemplos

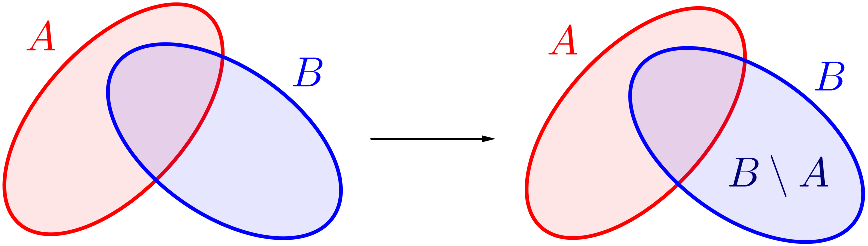
1. *Sean* $A = \{a, b, c, e\}$ *y* $B = \{c, e, f\}$. *Entonces*
$$A \cup B = \{a, b, c, e, f\}.$$
2. *Tomemos ahora* $A = \{1, 3, 5\}$ *y* $B = \{2, 4, 6\}$. *Entonces*
$$A \cup B = \{1, 3, 5, 2, 4, 6\}.$$
3. *Sean* $A = [-1, \sqrt{2}]$ *y* $B =]0, 2]$. *Entonces* $A \cup B = [-1, 2]$.
4. *Si* $A = [0, 2[$ *y* $B = \{2\}$ *entonces* $A \cup B = [0, 2]$.

Teoría de conjuntos (parte II)

Definición

El **complementario** *de un conjunto A sobre otro conjunto B es el conjunto formado por todos los elementos de B que no pertenecen a A y se denota por $B \setminus A$, es decir:*

$$B \setminus A = \{x \mid x \in B \wedge x \notin A\}.$$



Teoría de conjuntos (parte II)

Ejemplos

1. *Sean* $A = \{a, b, c, f\}$ *y* $B = \{b, c, e, f, g, j\}$. *Entonces*
$$B \setminus A = \{e, g, j\}.$$
2. *Tomamos* $A = \{a, b, c\}$ *y* $B = \{d, e, f\}$. *Entonces*
$$B \setminus A = \{d, e, f\} = B.$$
3. *Sean* $A = \{a, b, c, d\}$ *y* $B = \{b, c\}$. *Entonces se tiene:*
$$B \setminus A = \emptyset.$$
4. *Si* $A = [-1, 1]$ *y* $B =]0, 2]$ *entonces* $B \setminus A =]1, 2]$ *y* $A \setminus B = [-1, 0]$.

Teoría de conjuntos (parte II)

Definición

Sean A y B conjuntos. Diremos que B es un **subconjunto** *de A si se cumple $B \subseteq A$.*

Ejemplo

$B = \{a, d, e\}$ *es un subconjunto de* $A = \{a, b, c, d, e, f\}$*, mientras que* $C = \{a, g\}$ *no es un subconjunto de A.*

Definición

Sea A un conjunto. El conjunto de las **partes** *de A es el conjunto formado por todos los subconjuntos de A y se denota por $\mathcal{P}(A)$. En otras palabras:*

$$\mathcal{P}(A) = \{B \mid B \subseteq A\}.$$

Teoría de conjuntos (parte II)

Ejemplos

1. *Sea* $A = \{a, b\}$, *entonces*

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

2. *Sea* $A = \{1, 2, 3\}$, *entonces*

$$\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}.$$

Teorema

Sea A *un conjunto finito, con* $|A| = n$. *Entonces* $|\mathcal{P}(A)| = 2^n$.

Teoría de conjuntos (parte II)

Universidad Internacional de Valencia

Definición

Sean A, B dos conjuntos. El **producto cartesiano** *de A y B, denotado por $A \times B$, consta del conjunto de todos los* **pares ordenados**, *donde los elementos de A ocupan la primera posición y los de B la última:*

$$A \times B = \{(a, b) \mid a \in A \wedge b \in B\}.$$

Ejemplo

Sea $A = \{1, 2, 3\}$ y $B = \{\alpha, \beta\}$. Entonces

$$A \times B = \{(1, \alpha), (1, \beta), (2, \alpha), (2, \beta), (3, \alpha), (3, \beta)\}.$$

Teoría de conjuntos (parte II)

Definición

Sean A, B dos conjuntos. Diremos que una regla de la forma $f : A \to B$ es una **aplicación** *o* **función** *si relaciona cada uno de los elementos de A a un* **único** *elemento de B; dicho de otra forma:*

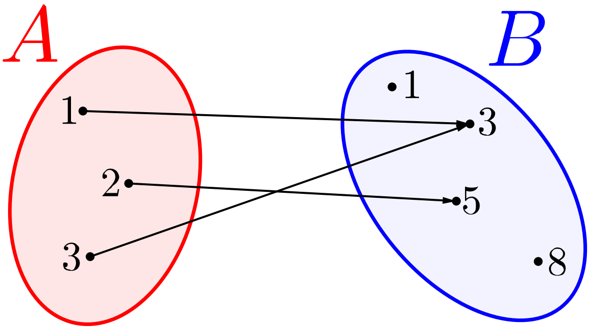
$$\forall a \in A, \exists! b \in B : f(a) = b.$$

- *El conjunto A recibe el nombre de* **dominio** *de f, y se denota por* $\mathrm{Dom}(f)$.
- *El conjunto B se denomina* **codominio** *de f.*
- *El conjunto $f(A)$, dado por $f(A) = \{f(a) \mid a \in A\}$ recibe el nombre de* **recorrido** *o* **imagen** *de f.*
- *Dado $C \subseteq B$, el conjunto $f^{-1}(C) = \{x \in A \mid f(x) \in C\}$ se denota por* **imagen inversa** *o* **preimagen** *de B sobre f.*

Teoría de conjuntos (parte II)

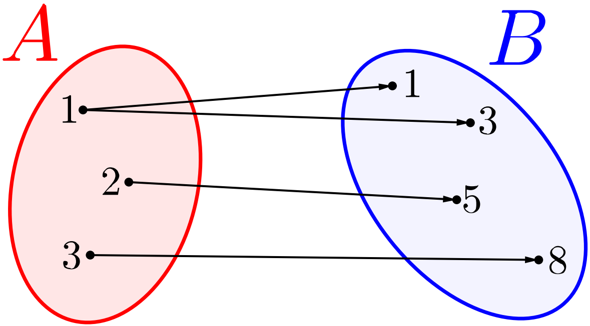
Ejemplos

1. *Sean* $A = \{1, 2, 3\}$ *y* $B = \{1, 3, 5, 8\}$. *Tomamos* $f : A \to B$ *tal que* $f(1) = 3$, $f(2) = 5$ *y* $f(3) = 3$. *Entonces* f *es una aplicación, con* $\mathrm{Dom}(f) = \{1, 2, 3\}$ *e* $\mathrm{Im}(f) = \{3, 5\} \subseteq B$.



Ejemplos

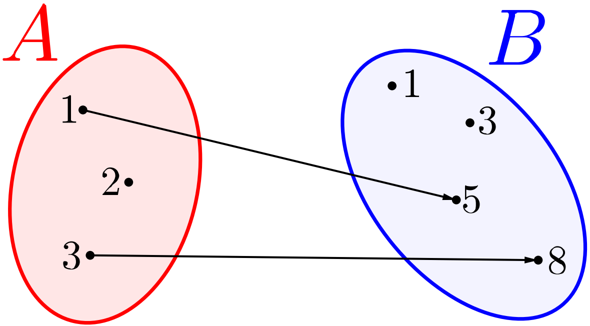
2. *Sean* $A = \{1, 2, 3\}$ *y* $B = \{1, 3, 5, 8\}$. *Sea* $f : A \to B$ *tal que* $f(1) = 1$, $f(1) = 3$, $f(2) = 5$ *y* $f(3) = 8$. *Entonces* f *NO es una aplicación, pues* $1 \in A$ *tiene asignados dos valores de* B*:* 1 *y* 3.



Teoría de conjuntos (parte II)

Ejemplos

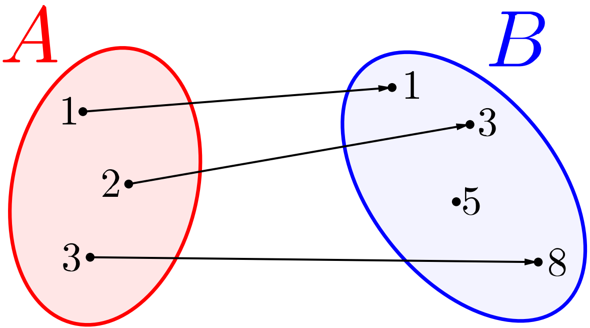
3. *Sean* $A = \{1, 2, 3\}$ *y* $B = \{1, 3, 5, 8\}$. *Tomamos* $f : A \to B$ *tal que* $f(1) = 5$, *y* $f(3) = 8$. *Entonces f* NO *es una aplicación, ya que* $2 \in A$ *no tiene asignado ningún valor.*



Teoría de conjuntos (parte II)

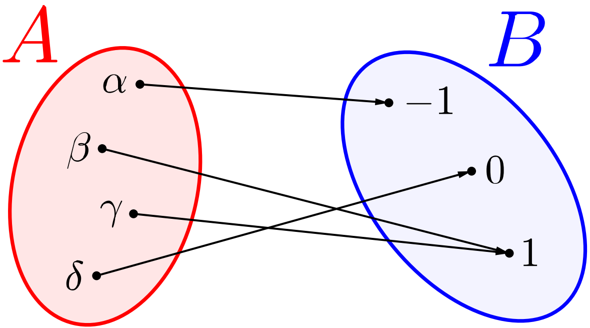
Definición

Sea $f : A \to B$ una aplicación. Diremos que f es **inyectiva** *si $\forall a, b \in A$, $f(a) = f(b) \to a = b$. Dicho de otra forma, f es inyectiva si f siempre lleva elementos distintos de A a elementos distintos de B.*



Definición

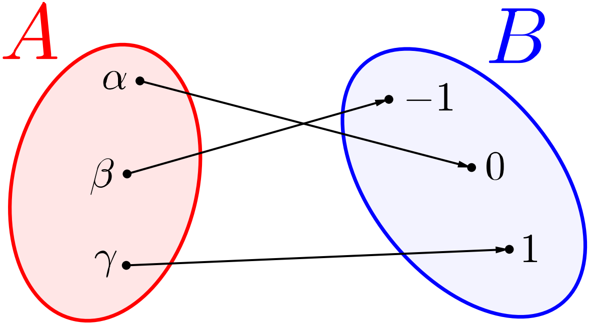
Sea $f : A \to B$ una aplicación. Se dice que f es **sobreyectiva** *o* **suprayectiva** *si $f(A) = B$ o, lo que es lo mismo, $\forall b \in B\ \exists a \in A : f(a) = b$. Es decir, f es sobreyectiva cuando cada elemento de B tiene asociado al menos un elemento de A mediante f.*



Teoría de conjuntos (parte II)

Definición

Sea $f : A \to B$ una aplicación. Se dice que f es **biyectiva** *si f es inyectiva y sobreyectiva simultáneamente. Esta condición se traduce matemáticamente como $\forall b \in B\ \exists! a \in A : f(a) = b$.*



Teoría de conjuntos (parte II)

Ejemplos

1. $f : [-1, 1] \to \mathbb{R}$ *dada por* $f(x) = x^3$. *Es inyectiva.*
2. $f : [-1, 1] \to [0, 1]$ *dada por* $f(x) = x^2$. *Es sobreyectiva.*
3. $f : \mathbb{R} \to \mathbb{R}$ *dada por* $f(x) = x^3$. *Es biyectiva.*

Teorema

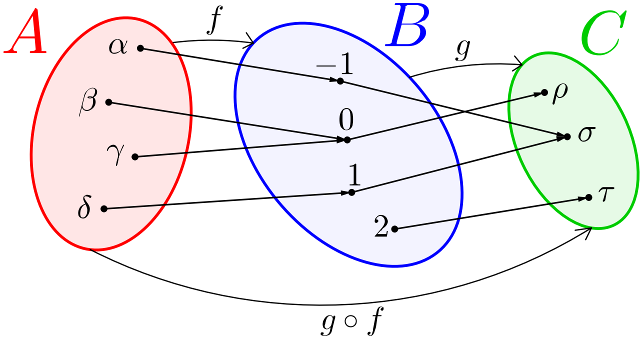
Sean A, B *conjuntos finitos y sea* $f : A \to B$ *una aplicación. Entonces se cumplen las siguientes propiedades:*

1. *Si* f *es inyectiva, entonces* $|A| \leq |B|$.
2. *Si* f *es sobreyectiva, entonces* $|A| \geq |B|$.
3. *Si* f *es biyectiva, entonces* $|A| = |B|$.

Teoría de conjuntos (parte II)

Definición

Sean A, B, C conjuntos cualesquiera, $f : A \to B$ y $g : B \to C$ aplicaciones. Entonces puede considerarse la **composición** *de g con f, $g \circ f : A \to C$ definida de la siguiente forma: dado $a \in A$ $(g \circ f)(a) = g(f(a)) \in C$.*



Teoría de conjuntos (parte II)

Ejemplo

Sean

- $f : [0, +\infty[\to \mathbb{R},\ f(x) = \sqrt{x},$
- $g : \mathbb{R} \to [0, +\infty[,\ g(x) = e^x.$

1. $(g \circ f)(x) = g(f(x)) = g(\sqrt{x}) = e^{\sqrt{x}}.$
2. $(f \circ g) = f(g(x)) = f(e^x) = \sqrt{e^x} = e^{x/2}.$

Teorema

Sean A, B, C tres conjuntos cualesquiera y $f : A \to B$, $g : B \to C$ aplicaciones.

1. *Si f, g son inyectivas, entonces $g \circ f$ también lo es.*
2. *Si f, g son sobreyectivas, entonces $g \circ f$ también lo es.*
3. *Si f, g son biyectivas, entonces $g \circ f$ también lo es.*

Teoría de conjuntos (parte II)

Definición

Sea A un conjunto cualquiera. La aplicación **identidad** $\mathrm{Id}_A : A \to A$ *es aquella que viene dada por* $\mathrm{Id}_A(a) = a \; \forall a \in A$.

Teorema

Sean A, B dos conjuntos cualesquiera. Entonces $f : A \to B$ es biyectiva si y sólo si $\exists! g : B \to A$ tal que $g \circ f = \mathrm{Id}_A$ y $f \circ g = \mathrm{Id}_B$. La aplicación (única) g suele denotarse por $g = f^{-1}$ y recibe el nombre de **aplicación inversa**.

Ejemplo

Sean $A = \{\alpha, \beta, \gamma\}$, $B = \{\rho, \sigma, \tau\}$ y $f : A \to B$ dada por $f(\alpha) = \tau$, $f(\beta) = \sigma$ y $f(\gamma) = \rho$. Entonces $f^{-1} : B \to A$ cumple $f^{-1}(\rho) = \gamma$, $f^{-1}(\sigma) = \beta$ y $f^{-1}(\tau) = \alpha$.

Definición

Una **permutación sin repetición** *de un conjunto A de n elementos diferentes consiste en cualquier ordenación que se pueda hacer con éstos, teniendo en cuenta que el orden de secuenciación importa.*
El número de ordenaciones posible viene dado por la expresión

$$P_n = n \cdot (n-1) \cdot (n-2) \cdots 3 \cdot 2 \cdot 1 = n!.$$

Ejemplo

Sea $A = \{a, b, c, d\}$. Queremos cuántas permutaciones pueden realizarse con los elementos de A (por ejemplo, $abcd$, $bdca$ y $dabc$ son tres de ellas). Como $|A| = 4$, se tiene por la expresión anterior, tomando $n = 4$, que $P_4 = 4! = 4 \cdot 3 \cdot 2 \cdot 1 = 24$.

Definición

Dados n elementos de r tipos diferentes, con n_i el número de elementos de tipo i, $1 \leq i \leq r$, una **permutación** *con repetición consiste en una reordenación cualquiera de estos elementos, donde el el total de posibilidades viene dado por*

$$P_n^{n_1, n_2, \ldots, n_r} = \frac{n!}{n_1! \cdot n_2! \cdots n_r!}.$$

Ejemplo

Reordenaciones posibles con las letras de la palabra aabbbc. $r = 3$ elementos diferentes: las letras a, b y c. $n_1 = 2$. $n_2 = 3$. $n_3 = 1$. Por tanto, el resultado es $P_6^{2,3,1} = \frac{6!}{2! \cdot 3! \cdot 1!} = 60$.

Definición

Una **variación sin repetición** *consiste en tomar k elementos dentro de un conjunto de n elementos y contar las posibles elecciones, teniendo en cuenta que no pueden elegirse más de una vez un mismo elemento y que, a diferencia de las combinaciones, el orden de elección importa. El número de posibilidades es, en este caso,*

$$V_{n,k} = n \cdot (n-1) \cdot (n-2) \cdots (n-k+1) = \frac{n!}{(n-k)!}.$$

Ejemplo

Posibles números de dos cifras que pueden formarse con el conjunto de cifras $\{1,2,3,4\}$: $V_{4,2} = \frac{4!}{2!} = 12.$

Definición

Una **variación con repetición** *consiste en tomar k elementos dentro de un conjunto de n elementos y contar las posibles elecciones, teniendo en cuenta que, en este caso, puede elegirse más de una vez un mismo elemento y que el orden de elección importa. El número de posibilidades es, en este caso,*

$$VR_{n,k} = \overbrace{n \cdot n \cdots n}^{k \text{ veces}} = n^k.$$

Ejemplo

Posibles números de dos cifras que pueden formarse con el conjunto de cifras $\{1, 2, 3, 4\}$, *pudiendo utilizarse cada una más de una vez:* $VR_{4,2} = 4^2 = 16$.

Combinatoria

Definición

Una **combinación sin repetición** *consiste en tomar k elementos dentro de un conjunto de n elementos y contar las posibles elecciones, teniendo en cuenta que no se puede elegir más de una vez un mismo elemento y que, además, el orden de elección no importa. En este caso, el número de posibilidades es*

$$C_{n,k} = \binom{n}{k} = \frac{n!}{k! \cdot (n-k)!}.$$

Ejemplo

Posibles grupos de 3 letras dentro del conjunto de 4 letras $\{a, b, c, d\}$:
$C_{4,3} = \binom{4}{3} = \frac{4!}{3! \cdot (4-3)!} = 4.$

Definición

Una **combinación con repetición** *consiste en tomar k elementos dentro de un conjunto de n elementos y contar las posibles elecciones, teniendo en cuenta que, en este caso, puede elegirse más de una vez un mismo elemento y que, de nuevo, el orden de elección no importa. En este caso, el número de posibilidades es*

$$CR_{n,k} = \binom{n+k-1}{k} = \frac{(n+k-1)!}{k! \cdot (n-1)!}.$$

Ejemplo

Posibles grupos de 3 *letras dentro del conjunto de* 4 *letras* $\{a, b, c, d\}$, *admitiendo repetición:* $CR_{4,3} = \binom{4+3-1}{3} = \binom{6}{3} = \frac{6!}{3! \cdot (6-3)!} = 20.$

Funciones booleanas

- Recordemos que $p \to q \equiv \overline{p} + q$.
- $p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$, luego $p \leftrightarrow q \equiv (\overline{p} + q) \cdot (p + \overline{q})$, por lo que simplificando $p \leftrightarrow q \equiv p \cdot q + \overline{p} \cdot \overline{q}$.
- Cualquier fórmula lógica puede expresarse empleando como únicos conectores la conjunción (producto), la disyunción (suma) y la negación (**álgebras de Boole**).

Definición

Una **función booleana** *es una aplicación $f : \mathbb{B}^n \to \mathbb{B}$, donde $\mathbb{B} = \{0, 1\}$ es el* **conjunto binario**. *Se denota $\mathcal{F}_n$ al conjunto formado por todas las funciones booleanas de n variables, es decir:*

$$\mathcal{F}_n = \{f : \mathbb{B}^n \to \mathbb{B} \mid f \text{ aplicación}\}.$$

Funciones booleanas

Ejemplos

1. $f : \mathbb{B} \to \mathbb{B}$, $f(x) = x$.
2. $f : \mathbb{B} \to \mathbb{B}$, $f(x) = \overline{x}$.
3. $f : \mathbb{B}^2 \to \mathbb{B}$, $f(x, y) = x + y$.
4. $f : \mathbb{B}^2 \to \mathbb{B}$, $f(x, y) = x \cdot y$.
5. $f : \mathbb{B}^2 \to \mathbb{B}$, $f(x, y) = \overline{x} + y$.
6. $f : \mathbb{B}^2 \to \mathbb{B}$, $f(x, y) = x \cdot y + \overline{x} \cdot \overline{y}$.
7. $f : \mathbb{B}^3 \to \mathbb{B}$, $f(x, y, z) = \overline{x} \cdot z + y$.

Puertas lógicas

Definición

Una **puerta lógica** *es un operador que transforma uno o dos valores de entrada binarios, x, y, en un valor binario de salida, en función de x, y. Por tanto, una puerta lógica puede verse como elemento de $\mathcal{F}_n$.*

Existen un total de siete puertas lógicas:

- OR
- AND
- XOR
- NOT
- NOR
- NAND
- XNOR

Puertas lógicas

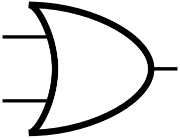
Puerta OR: se trata de la puerta lógica que combina un par de valores $x, y \in \mathbb{B}$ según la tabla de operaciones siguiente:

OR	$y = 0$	$y = 1$
$x = 0$	0	1
$x = 1$	1	1

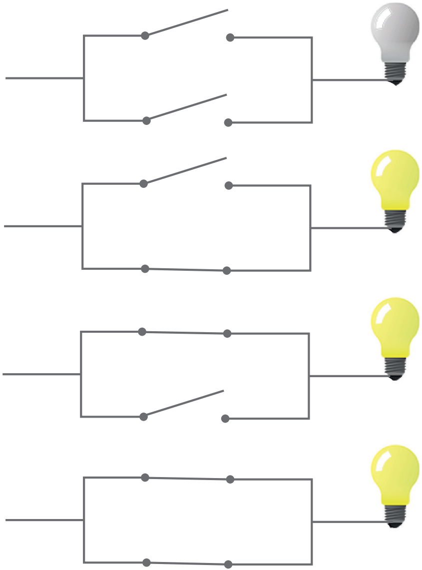
Esta puerta lógica puede interpretarse como la siguiente función booleana de $\mathcal{F}_2$:

$$f : \mathbb{B}^2 \to \mathbb{B}, \quad f(x, y) = x + y.$$

Se representa mediante el siguiente símbolo:



Puertas lógicas



Puertas lógicas

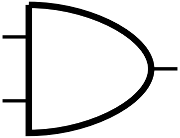
Puerta AND: se trata de la puerta lógica que combina un par de valores $x, y \in \mathbb{B}$ según la tabla de operaciones siguiente:

AND	$y = 0$	$y = 1$
$x = 0$	0	0
$x = 1$	0	1

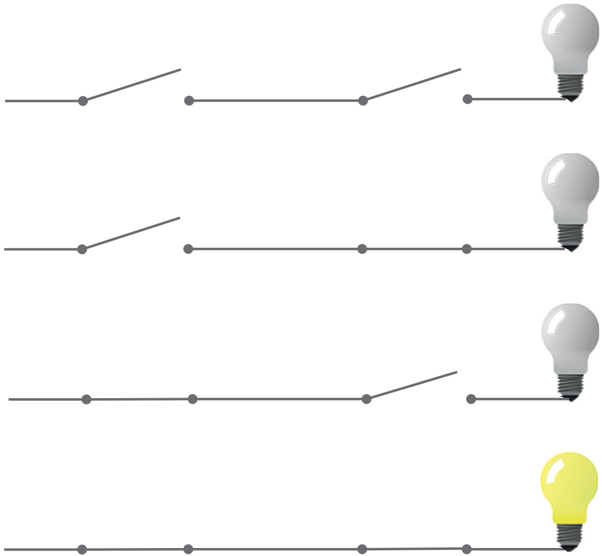
Esta puerta lógica puede interpretarse como la siguiente función booleana de $\mathcal{F}_2$:

$$f : \mathbb{B}^2 \to \mathbb{B}, \quad f(x, y) = x \cdot y.$$

Se representa mediante el siguiente símbolo:



Puertas lógicas



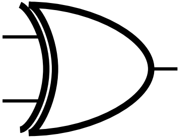
Puerta XOR: se trata de la puerta lógica que combina un par de valores $x, y \in \mathbb{B}$ según la tabla de operaciones siguiente:

XOR	$y = 0$	$y = 1$
$x = 0$	0	1
$x = 1$	1	0

Esta puerta lógica puede interpretarse como la siguiente función booleana de $\mathcal{F}_2$:

$$f : \mathbb{B}^2 \to \mathbb{B}, \quad f(x, y) = (\overline{x} + \overline{y}) \cdot (x + y).$$

Se representa mediante el siguiente símbolo:



Puertas lógicas

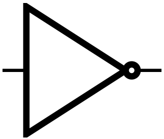
Puerta NOT: se trata de la puerta lógica que invierte el estado de un valor binario $x \in \mathbb{B}$:

NOT	
$x = 0$	1
$x = 1$	0

Esta puerta lógica puede interpretarse como la siguiente función booleana de $\mathcal{F}_1$:

$$f : \mathbb{B} \to \mathbb{B}, \quad f(x) = \overline{x}.$$

Se representa mediante el siguiente símbolo:



Puertas lógicas

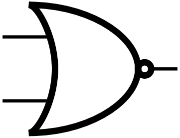
Puerta NOR: se trata de la puerta lógica que combina un par de valores $x, y \in \mathbb{B}$ según la tabla de operaciones siguiente:

NOR	$y = 0$	$y = 1$
$x = 0$	1	0
$x = 1$	0	0

Esta puerta lógica puede interpretarse como la siguiente función booleana de $\mathcal{F}_2$:

$$f : \mathbb{B}^2 \to \mathbb{B}, \quad f(x, y) = \overline{x} \cdot \overline{y}.$$

Se representa mediante el siguiente símbolo:



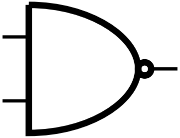
Puerta NAND: se trata de la puerta lógica que combina un par de valores $x, y \in \mathbb{B}$ según la tabla de operaciones siguiente:

NAND	$y = 0$	$y = 1$
$x = 0$	1	1
$x = 1$	1	0

Esta puerta lógica puede interpretarse como la siguiente función booleana de $\mathcal{F}_2$:

$$f : \mathbb{B}^2 \to \mathbb{B}, \quad f(x, y) = \overline{x} + \overline{y}.$$

Se representa mediante el siguiente símbolo:



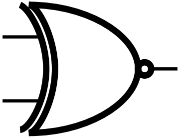
Puerta XNOR: se trata de la puerta lógica que combina un par de valores $x, y \in \mathbb{B}$ según la tabla de operaciones siguiente:

XNOR	$y=0$	$y=1$
$x=0$	1	0
$x=1$	0	1

Esta puerta lógica puede interpretarse como la siguiente función booleana de $\mathcal{F}_2$:

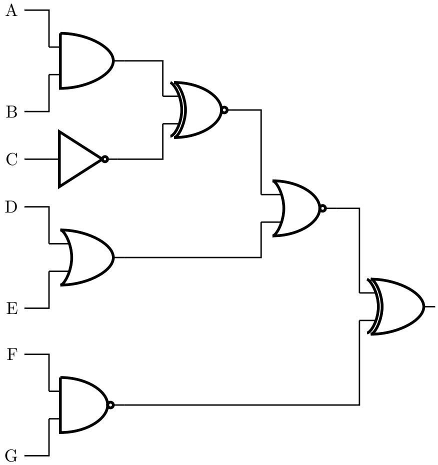
$$f : \mathbb{B}^2 \to \mathbb{B}, \quad f(x,y) = x \cdot y + \overline{x} \cdot \overline{y}.$$

Se representa mediante el siguiente símbolo:



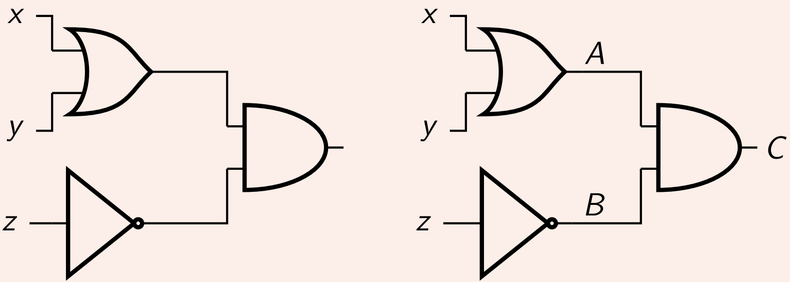
Circuitos lógicos

Las puertas lógicas pueden combinarse entre sí para formar **circuitos lógicos**, los cuales pueden interpretarse como elementos de $\mathcal{F}_n$.



Ejemplo

Consideremos el circuito lógico siguiente:



La función booleana asociada a este circuito es $f \in \mathcal{F}_3$ *dada por*

$$f(x, y, z) = (x + y) \cdot \overline{z}.$$

Teoría de grafos

Definición

Un **grafo** G *es una terna* (V, E, γ), *donde* V *y* E *son conjuntos y* γ *es una aplicación*

$$\gamma : E \to \mathcal{E},$$

donde $\mathcal{E} = \{\{v, v'\} \mid v, v' \in V\}$

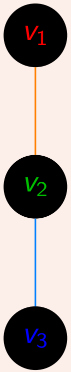
- *Los elementos del conjunto* V *reciben el nombre de* **vértices**.
- *Los elementos del conjunto* E *reciben el nombre de* **lados** *o* **aristas**.
- *La aplicación* γ *se conoce como* **aplicación de incidencia**.
- *Dicha aplicación identifica las aristas con el par correspondiente de vértices que unen.*

Todo grafo tiene su correspondiente representación gráfica, como veremos en los siguientes ejemplos.

Ejemplos

1. *Consideremos el grafo* $G = (V, E, \gamma)$, *con* $V = \{v_1, v_2, v_3\}$, $E = \{e_1, e_2\}$, *siendo* $\gamma : E \to \mathcal{E}$ *dada por:*

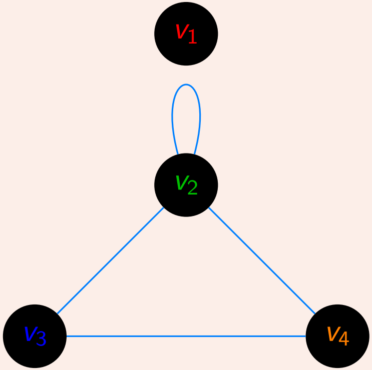
$$\gamma(e_1) = \{v_1, v_2\}$$
$$\gamma(e_2) = \{v_2, v_3\}$$



Ejemplos

2. *Consideremos el grafo* $G = (V, E, \gamma)$*, con* $V = \{v_1, v_2, v_3, v_4\}$*,* $E = \{e_1, e_2, e_3, e_4\}$*, siendo* $\gamma : E \to \mathcal{E}$ *dada por:*

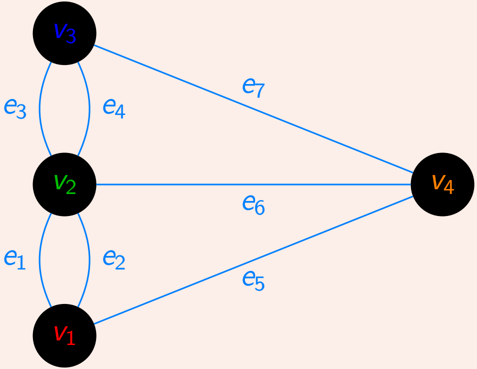
$$\gamma(e_1) = \{v_2, v_2\}$$
$$\gamma(e_2) = \{v_2, v_3\}$$
$$\gamma(e_3) = \{v_3, v_4\}$$
$$\gamma(e_4) = \{v_4, v_2\}$$



Ejemplos

3. *Consideremos el grafo* $G = (V, E, \gamma)$, *con* $V = \{v_1, v_2, v_3, v_4\}$, $E = \{e_1, e_2, e_3, e_4, e_5, e_6, e_7\}$, *siendo* $\gamma : E \to \mathcal{E}$ *dada por:*

$$\gamma(e_1) = \{v_1, v_2\}$$
$$\gamma(e_2) = \{v_1, v_2\}$$
$$\gamma(e_3) = \{v_2, v_3\}$$
$$\gamma(e_4) = \{v_2, v_3\}$$
$$\gamma(e_5) = \{v_1, v_4\}$$
$$\gamma(e_6) = \{v_2, v_4\}$$
$$\gamma(e_7) = \{v_3, v_4\}$$



Grafos dirigidos

Definición

Un **grafo dirigido** G *es una terna* (V, E, γ)*, donde* V *y* E *son conjuntos (de vértices y de aristas o lados, respectivamente) y* γ *es una aplicación de la forma*

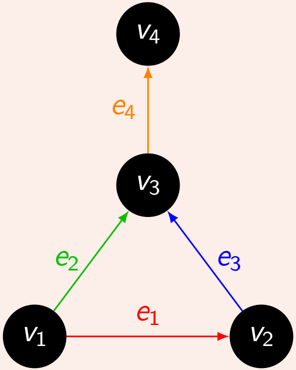
$$\gamma : E \to V \times V.$$

Los grafos dirigidos habitualmente se representan gráficamente dibujando las aristas con una flecha en la dirección válida para recorrerla, siendo la primera componente del par ordenado el punto de partida y la segunda componente el punto de llegada.

Ejemplo

Sea $G = (V, E, \gamma)$ *el grafo dirigido dado por el conjunto de vértices* $V = \{v_1, v_2, v_3, v_4\}$, *el conjunto de aristas* $E = \{e_1, e_2, e_3, e_4\}$ *y* $\gamma : E \to V \times V$ *dada por:*

$$\gamma(e_1) = (v_1, v_2),$$
$$\gamma(e_2) = (v_1, v_3),$$
$$\gamma(e_3) = (v_2, v_3),$$
$$\gamma(e_4) = (v_3, v_4).$$



Grafos simples

Definición

Un **grafo simple** $G = (V, E, \gamma)$ *es un grafo que cumple dos restricciones adicionales:*

1. *No hay aristas diferentes que unan el mismo par de vértices, es decir, si* $e \neq e'$*, entonces* $\gamma(e) \neq \gamma(e')$ *(*γ *es inyectiva).*
2. *No contiene* **bucles** *o* **loops***, es decir, no tiene aristas que unen un vértices consigo mismo; equivalentemente,* $\gamma(e) = \{v_e, v_e'\}$*, con* $v_e \neq v_e'$*,* $\forall e \in E$*.*

Nota

En adelante, y por comodidad, en caso de trabajar con grafos simples, omitiremos la existencia de la aplicación γ *y denotaremos las aristas directamente por el correspondiente conjunto o par ordenado de vértices.*

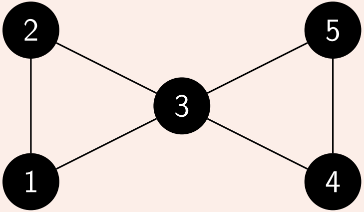
Grafos conexos

Definición

Un grafo G es **conexo** *si para cada par de vértices diferentes existe algún* **camino** *(sucesión de aristas adyacentes) que los une.*

Ejemplos

1. *Sea G un grafo de 5 vértices dado por las aristas* $\{1,2\}, \{1,3\}, \{2,3\}, \{3,4\}, \{3,5\}, \{4,5\}$. *Gráficamente:*

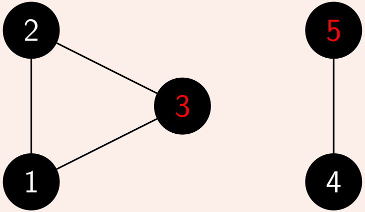


G es conexo.

Grafos conexos

Ejemplos

2. *Sea G un grafo de 5 vértices cuyas aristas son* $\{1,2\},\{1,3\},\{2,3\},\{4,5\}$. *Gráficamente:*



Entonces G no es conexo.

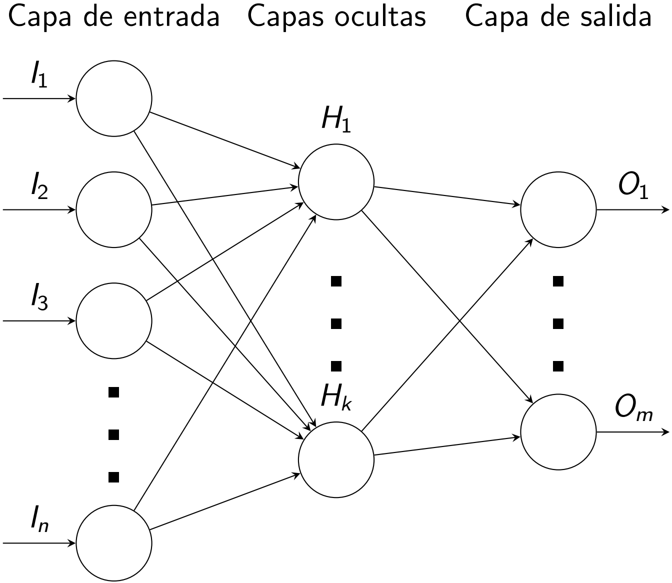
Definición

Una **red neuronal** *es un grafo dirigido* (V, E), *con* $V = \{1, 2, \dots, n\}$ *y* $E \subseteq V \times V$ *con los elementos adicionales siguientes:*

- $\forall i \in V$ *tiene asociada una variable de estado* $a_i \in [0, 1]$.
- $\forall (i, j) \in E$ *tiene asociado un peso* $\omega_{i,j} \in \mathbb{R}$ *(***grafo ponderado***)*.
- $\forall i \in V$ *tiene asociado un* **sesgo** b_i.
- $\forall i \in V$ *le corresponde una* **función de activación** $f_i : \mathbb{R} \to [0, 1]$ *de la forma*

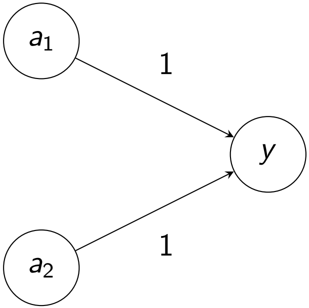
$$f_i\left(\sum_{j=1}^{n} \omega_{j,i} a_j + b_i\right).$$

Redes neuronales



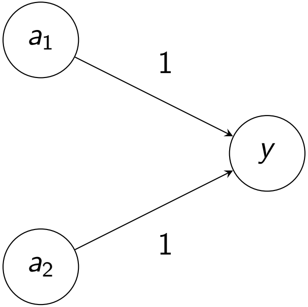
Redes neuronales

Ejemplo 1: neurona AND



$$y = f(a_1 + a_2 - 1.5), \quad f(x) = \begin{cases} 0 & \text{si } x < 0 \\ 1 & \text{si } x \geq 0 \end{cases}$$

Ejemplo 2: neurona OR



$$y = f(a_1 + a_2 - 0.5), \quad f(x) = \begin{cases} 0 & \text{si } x < 0 \\ 1 & \text{si } x \geq 0 \end{cases}$$

Complejidad computacional

La teoría de **complejidad computacional** estudia y clasifica los algoritmos y problemas computacionales en función de su coste y dificultad de resolver.

Algorithm Compute $p = u \cdot v$ for $u, v \in \mathbb{R}^n$

Require: $\text{length}(u) = \text{length}(v)$
Ensure: $p = u \cdot v$

$p \leftarrow u_1 v_1$
for $k \leftarrow 2$ to n **do**
  $p \leftarrow p + u_k v_k$
end for
return p

- **Operaciones:** $n - 1$ sumas, n productos.
- **Total operaciones:** $2n - 1$ operaciones (coste **lineal**).

Complejidad computacional

Algorithm Compute $C = A + B$ for $A, B \in \mathbb{R}^{n \times n}$

Require: $\text{size}(A) = \text{size}(B)$

Ensure: $C = A + B$

```
C ← 0_{n×n}
for i ← 1 to n do
    for j ← 1 to n do
        C_{i,j} ← A_{i,j} + B_{i,j}
    end for
end for
return C
```

- **Operaciones:** n^2 sumas.
- **Total operaciones:** n^2 operaciones (coste **cuadrático**).

Complejidad computacional

Algorithm Compute $C = A \cdot B$ for $A, B \in \mathbb{R}^{n \times n}$

Require: $\text{size}(A) = \text{size}(B)$
Ensure: $C = A \cdot B$

```
C ← 0_{n×n}
for i ← 1 to n do
    for j ← 1 to n do
        for k ← 1 to n do
            C_{i,j} ← C_{i,j} + A_{i,k} B_{k,j}
        end for
    end for
end for
return C
```

- **Operaciones:** n^3 sumas, n^3 productos.
- **Total operaciones:** $2n^3$ operaciones (coste **cúbico**).

Complejidad computacional

Resolución de un sistema de ecuaciones lineal $n \times n$ con matriz de coeficientes triangular inferior:

$$\left.\begin{array}{rcl} a_{1,1}x_1 & = & b_1 \\ a_{2,1}x_1 + a_{2,2}x_2 & = & b_2 \\ \ddots & & \\ a_{n-1,1}x_1 + a_{n-1,2}x_2 + \cdots + a_{n-1,n-1}x_{n-1} & = & b_{n-1} \\ a_{n,1}x_1 + a_{n,2}x_2 + \cdots + a_{n,n-1}x_{n-1} + a_{n,n}x_n & = & b_n \end{array}\right\}$$

Matricialmente: $AX = B$, donde $A \in \mathbb{R}^{n\times n}$, $X \in \mathbb{R}^{n\times 1}$ y $B \in \mathbb{R}^{n\times 1}$:

$$A = \begin{pmatrix} a_{1,1} & 0 & \cdots & 0 & 0 \\ a_{2,1} & a_{2,2} & \ddots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{n-1,1} & a_{n-1,2} & \cdots & a_{n-1,n-1} & 0 \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n-1} & a_{n,n} \end{pmatrix}, \; X = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_{n-1} \\ x_n \end{pmatrix}, \; B = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_{n-1} \\ b_n \end{pmatrix}.$$

Algorithm Solve $AX = B$ for $A \in \mathbb{R}^{n\times n}$, $X, B \in \mathbb{R}^{n\times 1}$

Require: $\det(A) \neq 0$
Ensure: $AX = B$
  for $i \leftarrow 1$ to n **do**
    $X_i \leftarrow B_i$
    for $j \leftarrow 1$ to $i-1$ **do**
      $X_i \leftarrow X_i - A_{i,j}X_j$
    end for
    $X_i \leftarrow \dfrac{X_i}{A_{i,i}}$
  end for
  return X

- **Operaciones:** $(n-1)n/2$ sumas, $(n-1)n/2$ productos, n divisiones.
- **Total operaciones:** n^2 operaciones (coste **cuadrático**).

Complejidad computacional

Definición

Diremos que el coste computacional de un algoritmo es **polinomial** *si el coste en función del tamaño de la entrada, n, es un polinomio.*

Definición

Diremos que el coste computacional de un algoritmo con $c(n)$ operaciones es $\mathcal{O}(n^k)$, $k \in \mathbb{N}$, si

$$\exists \lim_{n \to +\infty} \frac{c(n)}{n^k} = C, \quad C \in]0, +\infty[.$$

Ejemplos

1. *El coste computacional del producto escalar, con $2n - 1$ operaciones, es $\mathcal{O}(n)$:*

$$\lim_{n \to +\infty} \frac{2n - 1}{n} = 2.$$

Universidad Internacional de Valencia

Ejemplos

2. *El coste computacional de la suma de matrices cuadradas, con n^2 operaciones, es $\mathcal{O}(n^2)$:*
$$\lim_{n\to+\infty} \frac{n^2}{n^2} = 1.$$
3. *El coste computacional del producto de matrices cuadradas, con $2n^3$ operaciones, es $\mathcal{O}(n^3)$:*
$$\lim_{n\to+\infty} \frac{2n^3}{n^3} = 2.$$
4. *El coste computacional de la resolución de un sistema triangular, con n^2 operaciones, es $\mathcal{O}(n^2)$:*
$$\lim_{n\to+\infty} \frac{n^2}{n^2} = 2.$$

Algorithm Compute $\det(A)$ for $A \in \mathbb{R}^{n\times n}$

Require: A is a square matrix
Ensure: $d = \det(A)$

$n \leftarrow \dim(A)$
if $n = 1$ **then**
  $d \leftarrow A_{1,1}$
else
  $d \leftarrow 0$
  for $j \leftarrow 1$ to n **do**
    $d \leftarrow d + (-1)^{1+j} A_{1,j} \det(A_{\overline{\{1\}},\overline{\{j\}}})$
  end for
end if
return d

$2 \cdot n!$ operaciones.

- Se tiene que $\forall k \in \mathbb{N}$
$$\lim_{n \to +\infty} \frac{2 \cdot n!}{n^k} = +\infty.$$

- Necesitamos ampliar la noción de $\mathcal{O}$.

Definición

Sea $f : \mathbb{N} \to \mathbb{R}$ y $c(n)$ el número de operaciones requeridas por un algoritmo. Diremos que el coste computacional del algoritmo es $\mathcal{O}\big(f(n)\big)$ si

$$\lim_{n \to +\infty} \frac{c(n)}{f(n)} = C, \quad C \in]0, +\infty[.$$

Ejemplos

1. *El coste computacional del algoritmo que calcula el determinante es* $\mathcal{O}(n!)$*:*

$$\lim_{n\to+\infty} \frac{2\cdot n!}{n!} = 2.$$

2. *El coste computacional de un algoritmo con* $2^n + n^6 - 2n^4 + 3n + 7$ *operaciones es* $\mathcal{O}(2^n)$*:*

$$\lim_{n\to+\infty} \frac{2^n + n^6 - 2n^4 + 3n + 7}{2^n} = 1.$$

3. *Algoritmos de ordenación eficientes:* $\mathcal{O}\big(n\log(n)\big)$.

Problemas de decisión

Definición

Un **problema de decisión** *consiste en un problema cuya respuesta se puede plantear como un "sí" o un "no" en función de sus entradas.*

Ejemplos

1. *Algoritmo que determina si un número dado es par o impar.*
2. *Algoritmo que determina si un número dado es primo o no.*
3. *Algoritmo para determinar si un grafo es o no es conexo.*
4. *Algoritmo que determina si un Sudoku tiene solución o no.*
5. *Algoritmo para determinar si existe un subconjunto de un determinado subconjunto numérico cuyos elementos suman* 0.

Problemas de decisión

Definición

Definimos como **P** *(polynomial time) el conjunto formado por todos los problemas de decisión que pueden resolverse de forma determinista con un coste computacional polinomial.*

Ejemplos

1. *Algoritmo que determina si un número dado es par o impar. Coste computacional:* $\mathcal{O}(1)$.
2. *Algoritmo que determina si una matriz es o no es simétrica. Coste computacional:* $\mathcal{O}(n^2)$.
3. *Algoritmo que determina si se puede encontrar un camino en un grafo simple que recorre todos sus vértices pasando por todas sus aristas una única vez (caminos/ciclos eulerianos). Coste computacional:* $\mathcal{O}(n^2)$.

Problemas de decisión

Definición

Definimos como **NP** *(non-deterministic polynomial time) el conjunto formado por todos los problemas de decisión que pueden resolverse de forma no determinista con un coste computacional polinomial.*

Equivalentemente, **NP** *es el conjunto formado por todos los problemas de decisión cuyas instancias pueden verificarse con un coste computacional polinomial.*

Ejemplos

1. *Sudoku.*
2. *Hallar el subconjunto de un determinado subconjunto numérico cuyos elementos suman* 0*.*
3. *Cualquier problema en* $\mathbf{P}$ *(*$\mathbf{P} \subseteq \mathbf{NP}$*).*

Problemas de decisión

5	3	4	6	7	8	9	1	2
6	7	2	1	9	5	3	4	8
1	9	8	3	4	2	5	6	7
8	5	9	7	6	1	4	2	3
4	2	6	8	5	3	7	9	1
7	1	3	9	2	4	8	5	6
9	6	1	5	3	7	2	8	4
2	8	7	4	1	9	6	3	5
3	4	5	2	8	6	1	7	9

Coste computacional de la verificación: $\mathcal{O}(n^3)$

Problemas de decisión

- Sea A el conjunto dado por

$$A = \{-11, 8, 7, 1, -2, 52, -14, 0, -10, 23\}.$$

- Entonces el subconjunto $B \subseteq A$ dado por

$$B = \{1, -14, -10, 23\}$$

  verifica que la suma de sus elementos es 0.
- Coste computacional de la verificación: $\mathcal{O}(n)$.
- En el caso general, un conjunto A verificando $|A| = n$, posee $|\mathcal{P}(A)| = 2^n$ subconjuntos, luego si se procede por fuerza bruta, en el peor de los casos habría que realizar

$$\sum_{k=1}^{n}(k-1)\binom{n}{k} \text{ sumas} \sim \mathcal{O}(n \cdot 2^n) \text{ operaciones.}$$

PROBLEMA DEL MILLÓN:

$$¿\mathbf{P} = \mathbf{NP}?$$

¡Muchas gracias!

Universidad Internacional de Valencia

Contacto:

victormanuel.campello@campusviu.es