Lógica y Métodos Discretos

LibreIM

Doble Grado de Informática y Matemáticas
Universidad de Granada

libreim.github.io/apuntesDGIIM

Lógica y Métodos Discretos

LibreIM

Doble Grado de Informática y Matemáticas

Universidad de Granada

`libreim.github.io/apuntesDGIIM`

Índice

Parte I.
Teoría

1. Inducción y Recurrencia

1.1. Introducción a los naturales

En el estudio de los números naturales es necesario establecer un punto de partida y a partir de ahí, podremos definir operaciones básicas como la suma, el producto o el orden. Para ello, usaremos de punto de partida los axiomas de Peano y de esta forma llegaremos a todo lo que conocemos sobre los números naturales.

1.2. Axiomática de Peano

Supongamos que existe un conjunto $\mathbb{N}$. Los elementos de este conjunto se llaman números naturales.

Definición 1.1 (Axiomas de Peano). Los axiomas que definen a $\mathbb{N}$ son los siguientes:

- *A1* El cero es un número natural. $0 \in \mathbb{N}$
- *A2* El siguiente de un número natural es un número natural. Si $n \in \mathbb{N} \Rightarrow \sigma(n) \in \mathbb{N}$
- *A3* Cero no es el siguiente de ningún número natural. $\forall n \in \mathbb{N}, \sigma(n) \neq 0$
- *A4* Si los siguientes de dos números naturales son iguales, entonces los números naturales son iguales. $\forall m, n \in \mathbb{N}, \sigma(n) = \sigma(m) \Rightarrow m = n$
- *A5* Si un subconjunto de números naturales tiene el cero y siempre que tiene un número tiene a su siguiente, entonces el subconjunto son todos los números naturales.

Nota. Podemos definir $\sigma(n) = n + 1 \ \forall n \in \mathbb{N}$.

Teorema 1.1. Todo número natural es distinto del siguiente. $\forall n \in \mathbb{N} n \neq \sigma(n)$

Demostración. Sea $A = \{x \in \mathbb{N} : x \neq \sigma(x)\}$:
Como $0 \neq \sigma(0)$, resulta $0 \in A$. Supongamos ahora $n \in A$, es decir, $n \neq \sigma(n)$, luego $\sigma(n) \neq \sigma(\sigma(n))$, por tanto, $\sigma(n) \in A$. Luego $A = \mathbb{N}$. □

Teorema 1.2. Para cada número natural distinto de cero, existe un único número natural del que es su siguiente. $\forall n \in \mathbb{N}(n \neq 0 \Rightarrow \exists! m \in \mathbb{N}$ tal que $x = \sigma(m))$

Demostración. Sea $A = \{x \in \mathbb{N} : x = 0$ o $m \in \mathbb{N}$ tal que $x = \sigma(m)\}$:

Como $0 = 0$, resulta $0 \in A$. Supongamos ahora $n \in A$, es decir, $n = 0$ o $n = \sigma(m)$. En cualquier caso, $\sigma(n) = \sigma(n)$, por tanto $\sigma(n) \in A$. Luego $A = \mathbb{N}$.
La unicidad es consecuencia de $A4$. $\square$

1.3. Aritmética natural

1.3.1. Suma de naturales

> **Teorema 1.3.** Existe una única $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ tal que $\forall m, n \in \mathbb{N}$ verifica:
>
> - $m + 0 = m$
> - $m + \sigma(n) = \sigma(m + n)$

Propiedades 1.1. Para todo $m, n, p \in \mathbb{N}$ se cumple:

1. Todo número natural es 0 o es el siguiente de un número natural.
2. $m + 0 = 0 + m = m$.
3. $m + 1 = 1 + m = \sigma(m)$.
4. $(m + n) + p = m + (n + p)$.
5. $m + n = n + m$.
6. Si $m + p = n + p$, entonces $m = n$.
7. Si $m + n = 0$, entonces $m = n = 0$.

1.3.2. Producto de naturales

> **Teorema 1.4.** Existe una única $\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ tal que $\forall m, n \in \mathbb{N}$ verifica:
>
> - $m \cdot 0 = 0$
> - $m \cdot \sigma(n) = m \cdot n + m$

Propiedades 1.2. Para todo $m, n, p \in \mathbb{N}$ se cumple:

1. $0 \cdot m = m \cdot 0 = 0$.
2. $1 \cdot m = m \cdot 1 = m$.
3. $(m + n) \cdot p = m \cdot p + n \cdot p$.
4. $m \cdot n = n \cdot m$.
5. Si $(m \cdot n) \cdot p = m \cdot (n \cdot p)$.
6. Si $m \cdot n = 0$, entonces $m = 0$ o $n = 0$.

1.3.3. Potencias de naturales

> **Teorema 1.5.** Existe una única $\square^{\square} : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ tal que $\forall m, n \in \mathbb{N}$ verifica:
>
> - $m^0 = 1$
> - $m^{\sigma(n)} = m^n \cdot m$

Propiedades 1.3. Para todo $m, n, p \in \mathbb{N}$ se cumple:

1. $0^0 = 1$.

2. $0^n = 0$ para $1 \leq n$.
3. $1^n = 1$.
4. $m^{n+p} = m^n \cdot m^p$.
5. Si $m^{n \cdot p} = (m^n)^p$.

1.3.4. El orden de los naturales

Primero definamos en qué consiste una relación de orden:

Definición 1.2. Sea (A, R) un par ordenado con A un conjunto no vacío y R una relación binaria definida en A, entonces se dice que R es una **relación de orden** si es:

- **Reflexiva**: Todo elemento de A A está relacionado consigo mismo. Es decir, $\forall x \in A,\ xRx$.
- **Antisimétrica**: Si dos elementos de A se relacionan entre sí, entonces ellos son iguales. Es decir, $\forall x, y \in A,\ xRy,\ yRx \ \Rightarrow\ x = y$.
- **Transitiva**: Si un elemento de A está relacionado con otro, y ese otro a su vez se relaciona con un tercero, entonces el primero estará relacionado también con este último. Es decir, $\forall x, y, z \in A,\ xRy, yRz \Rightarrow xRz$.

Definición 1.3 (Orden). Dados $m, n \in \mathbb{N}$ definimos m es menor o igual que n $(m \leq n)$ si $\exists x \in \mathbb{N}$ tal que $m + x = n$. Lo podemos representar como $(\mathbb{N}, \leq)$.

Propiedades 1.4. Para todo $m, n, p \in \mathbb{N}$ se cumple:

1. $m \leq m$.
2. Si $m \leq n$ y $n \leq m$, entonces $m = n$.
3. Si $m \leq n$ y $n \leq p$, entonces $m \leq p$.
4. $m \leq n$ o $n \leq m$.
5. Si $m \leq n$, entonces $\exists! p \in \mathbb{N}$ tal que $m + p = n$ y lo llamamos n menos m $(n - m)$.
6. Si $m \leq n$, entonces $m + p \leq n + p$.
7. Si $m \leq n$, entonces $m \cdot p \leq n \cdot p$.
8. Si $m \cdot p \leq n \cdot p$ y $p \neq 0$, entonces $m \leq n$.
9. Si $m \cdot p = n \cdot p$ y $p \neq 0$, entonces $m = n$.

1.3.5. Divisibilidad en $\mathbb{N}$

Definición 1.4 (Divisibilidad). Dados $m, n \in \mathbb{N}$ definimimos m divide a n $(m|n)$ si $\exists x \in \mathbb{N}$ tal que $m \cdot x = n$.

Propiedades 1.5. Para todo $m, n, p \in \mathbb{N}$ se cumple:

1. $m|m$.

2. Si $m|n$ y $n|m$, entonces $m = n$.
3. Si $m|n$ y $n|p$, entonces $m|p$.
4. Si $m|n$, entonces $\exists! p \in \mathbb{N}$ tal que $m \cdot p = n$ y lo llamamos n partido por m $\left(\frac{n}{m}\right)$.

1.4. Principio de inducción

Teorema 1.6. Las tres propiedades que siguen son equivalentes:

1. **Principio de inducción**. Si $A \subseteq \mathbb{N}$ cumple $0 \in A$ y $(n \in A \Rightarrow n+1 \in A)$, entonces $A = \mathbb{N}$.
2. **Principio del buen orden**. Todo subconjunto no vacío de números naturales tiene mínimo.
3. **Principio de inducción completa**. Si $A \subseteq \mathbb{N}$ cumple $0 \in A$ y si $(\{0, 1, ..., n\} \subseteq A \Rightarrow n+1 \in A)$, entonces $A = \mathbb{N}$.

1.5. Ecuaciones en recurrencia

Definición 1.5. Una **ecuación en recurrencia** es un tipo específico de relación de recurrencia. Una relación de recurrencia es una sucesión $\{a_n\}$ que relaciona a_n con alguno de sus predeesores $a_0, a_1, \dots, a_{n-1}$ para $n \in \mathbb{N}$. Las condiciones iniciales para la sucesión $\{a_n\}$ son valores dados en forma explícita para un número finito de términos de la sucesión.

Ejemplo 1.1. Número de regiones del plano determinadas por n rectas no paralelas y que por cualquier punto del plano pasan como máximo dos de ellas.
Condiciones iniciales: $a_1 = 2$, $a_2 = 4$, $a_3 = 7$, $a_4 = 11$.

$$a_n = a_{n-1} + n \text{ para } 2 \leq n$$

Ejemplo 1.2. Torres de Hanoi.
Condiciones iniciales: $a_1 = 1$.

$$a_n = 2a_{n-1} + 1 \text{ para } 2 \leq n$$

Ejemplo 1.3. Llamemos a_n al número de listas de longitud n formadas con ceros y unos que no tienen unos consecutivos.
Condiciones iniciales: $a_1 = 2$, $a_2 = 3$.

$$a_n = a_{n-1} + a_{n-2} \text{ para } 3 \leq n$$

Ejemplo 1.4. Sucesión de Fibonacci.
Condiciones iniciales: $F_1 = 0$, $F_2 = 1$.

$$F_n = F_{n-1} + F_{n-2} \text{ para } 3 \leq n$$

1.5.1. Recurrencias homogéneas

Definición 1.6. Sea $x : \mathbb{N} \to \mathbb{R}$ una sucesión. Decimos que dicha sucesión satisface una **relación de recurrencia lineal homogénea con coeficientes constantes** si existe $k \in \mathbb{N}$, $a_1, \ldots$ y $a_k \in \mathbb{R}$ tales que para cualquier $n \geq k$ se verifica que $\sum_{j=0}^{k} a_j \cdot x_{n-j} = a_0 \cdot x_n + a_1 \cdot x_{n-1} + \ldots + a_k \cdot x_{n-k} = 0$, donde $a_0 = 1$. Al número k se le denomina orden de la relación.

Las **condiciones iniciales** son los k términos de la sucesión de la relación de recurrencia que son necesarios para poner en funcionamiento la recurrencia de orden k. Nuestro objetivo es hallar dicha sucesión que satisfaga la relación, siendo esta situación un **problema de recurrencia** y cada una de las sucesiones son las **soluciones del problema de recurrencia**.

Definición 1.7. Dado un problema de recurrencia lineal homogénea con coeficientes constantes $x_n + a_1 x_{n-1} + \ldots + a_k x_{n-k} = 0$. Al polinomio $x^k + a_1 x^{k-1} + \ldots + a_{k-1} x + a_k$ se le conoce como **polinomio característico de la relación**, y a la ecuación $x^k + a_1 x^{k-1} + \ldots + a_{k-1} x + a_k = 0$ la **ecuación característica**.

Proposición 1.1. Si α es una solución de la ecuación característica de un problema de recurrencia, entonces la sucesión $x_n = \alpha^n$ es una solución a dicho problema.

Cabe destacar que si $\alpha_1, \alpha_2, \ldots, \alpha_k$ son raíces del polinomio característico de una relación de recurrencia con $\alpha_i \neq \alpha_j$ $\forall i, j < k$ con $i \neq j$, entonces $x_n = b_1 \alpha_1^n + b_2 \alpha_2^n + \ldots + b_k \alpha_k^n$ es solución de la relación de equivalencia, siendo las condiciones iniciales las que determinan $b_1, b_2, \ldots, b_k$.

Proposición 1.2. Sea $x_n + a_1 x_{n-1} + \ldots + a_k x^{n-k}$ un problema de recurrencia, $p(x)$ su polinomio característico y α una raíz doble de $p(x)$, entonces $x_n = \alpha^n$ es una solución a dicho problema.

Ejemplo 1.5. Raíces simples. $a_n + a_{n-1} - 6a_{n-2} = 0$ para $n \geq 2$
Condiciones iniciales: $a_0 = 1$, $a_1 = 2$.
Hallamos el polinomio característico y factorizamos: $x^2 + x - 6 = (x-2)(x+3)$
Solución general: $s_n = A \cdot 2^n + B \cdot (-3)^n$
Solución particular: la hallamos resolviendo el sistema dado por las condiciones iniciales:

$$\left.\begin{aligned} 1 &= A + B \\ 2 &= 2A - 3B \end{aligned}\right\} \Rightarrow A = -1,\ B = 5 \text{ de donde } a_n = 2^n$$

Ejemplo 1.6. Raíz doble. $a_n - 6a_{n-1} + 9a_{n-2} = 0$ para $n \geq 2$
Condiciones iniciales: $a_0 = 5$, $a_1 = 12$.
Hallamos el polinomio característico y factorizamos: $x^2 - 6x + 9 = (x-3)^2$

Solución general: $s_n = (A \cdot n + B) \cdot 3^n$
Solución particular:

$$\left.\begin{array}{r} 5 = B \\ 12 = (A+B)\cdot 3 \end{array}\right\} \Rightarrow A = -1,\ B = 5 \text{ de donde } a_n = (-n+5)\cdot 3^n$$

Ejemplo 1.7. Raíces complejas simples. $a_n - 2a_{n-1} + 2a_{n-2} = 0$ para $n \geq 2$
Condiciones iniciales: $a_0 = 0$, $a_1 = 1$.
Hallamos el polinomio característico y factorizamos:
$x^2 - 2x + 2 = (x - (1+i))(x - (1-i))$
Solución general: $s_n = A \cdot (1+i)^n + B \cdot (1-i)^n$
Solución particular:

$$\left.\begin{array}{r} 0 = A + B \\ 1 = (1+i)\cdot A - (1-i)\cdot B \end{array}\right\} \Rightarrow A = \frac{-i}{2},\ B = \frac{i}{2} \text{ de donde } a_n = \frac{-i}{2}((1+i)^n - (1-i)^n)$$

Ejemplo 1.8. Raíces polinomio de grado k. $a_n - 5a_{n-1} + 8a_{n-2} - 4a_{n-3} = 0$ para $n \geq 3$
Condiciones iniciales: $a_0 = 0$, $a_1 = 1$, $a_2 = 2$.
Hallamos el polinomio característico y factorizamos: $x^3 - 5x^2 - 2x + 2 = (x - 1)(x-2)^2$
Solución general: $s_n = A + (B \cdot n + C)\cdot 2^n$
Solución particular:

$$\left.\begin{array}{r} 0 = A + C \\ 1 = A + 2B + 2C \\ 2 = A + 8B + 4C \end{array}\right\} \Rightarrow A = -2,\ B = -\frac{1}{2}, C = 2 \text{ de donde } a_n = -2 + (-\frac{1}{2}n + 2)\cdot 2^n$$

1.5.2. Recurrencias no homogéneas

Definición 1.8. Sea $x : \mathbb{N} \to \mathbb{R}$ una sucesión. Decimos que dicha sucesión satisface una **relación de recurrencia lineal con coeficientes constantes** si existe $k \in \mathbb{N}$, $a_1, \ldots, a_k \in \mathbb{R}$ y $f : \mathbb{N} \to \mathbb{R}$ tales que para cualquier $n \geq k$ se verifica que $\sum_{j=0}^{k} a_j \cdot x_{n-j} = a_0 \cdot x_n + a_1 \cdot x_{n-1} + \ldots + a_k \cdot x_{n-k} = f(n)$, donde $a_0 = 1$. Al número k se le denomina orden de la relación.

Proposición 1.3. Sea $x_n + a_1 x_{n-1} + \ldots + a_k x_{n-k} = f(n)$ un problema de recurrencia lineal no homogénea.

- Supongamos que u_n y v_n son soluciones al problema no homogéneo. Entonces la sucesión $u_n - v_n$ es una solución al problema de recurrencia lineal homogéneo asociado.

- Si y_n es una solución al problema no homogéneo, entonces todas las soluciones de dicho problema son de la forma $y_n + h_n$, donde h_n es una solución al problema homogéneo.

Proposición 1.4. Supongamos que x_n es una sucesión que satisface una relación de recurrencia lineal no homogénea $x_n + a_1 x_{n-1} + \ldots + a_k x_{n-k} = f(n)$ donde $f(n)$ es un polinomio de grado r. Entonces x_n satisface una relación de recurrencia lineal homogénea cuyo polinomio característico es $(x^k + a_1 x^{k-1} + \ldots + a_k)(x-1)^{r+1}$.

De manera similar, la siguiente proposición dice así:

Proposición 1.5. Supongamos que x_n es una sucesión que satisface una relación de recurrencia lineal no homogénea $x_n + a_1 x_{n-1} + \ldots + a_k x_{n-k} = b^n f(n)$ donde $f(n)$ es un polinomio de grado r. Entonces x_n satisface una relación de recurrencia lineal homogénea cuyo polinomio característico es $(x^k + a_1 x^{k-1} + \ldots + a_k)(x-b)^{r+1}$.

Ejemplo 1.9. Torres de Hanoi. $a_n = 2a_{n-1} + 1$ para $n \geq 2$
Condiciones iniciales: $a_1 = 1$.
Término no homogéneo: $1 = b^n p(n) \implies b = 1,\ p(n) = 1,\ gr(p) = 0$
Hallamos el polinomio característico (que tiene las soluciones de la ecuación dada y muchas más) y factorizamos: $x^2 - 3x + 2 = (x-1)(x-2)$
Solución general(ísima) de una homogénea asociada: $g_n = A \cdot 2^n + B$
Extendemos las soluciones iniciales: $a_1 = 1,\ a_2 = 2a_1 + 1 = 2 + 1 = 3$
Solución particular:

$$\left.\begin{aligned} 1 &= 2A + B \\ 3 &= 4A + B \end{aligned}\right\} \Rightarrow A = 1,\ B = -1 \text{ de donde } a_n = 2^n - 1$$

Extendemos las condiciones iniciales para una sucesión arbitraria: $a_1 = a,\ a_2 = 2a_1 + 1 = 2a + 1$
Solución general de la no homogénea:

$$\left.\begin{aligned} a &= 2A + B \\ 2a + 1 &= 4A + B \end{aligned}\right\} \Rightarrow A = \frac{a+1}{2},\ B = -1 \text{ de donde } s_n = \frac{a+1}{2} 2^n - 1$$

Ejemplo 1.10. Regiones del Plano. Las regiones del plano generadas por n rectas no paralelas y cuyas intersecciones no son de más de dos rectas: $a_n = 2a_{n-1} + n$ para $n \geq 1$
Condiciones iniciales: $a_0 = 1$.
Término no homogéneo: $1 = b^n p(n) \implies b = 1,\ p(n) = n,\ gr(p) = 1$
Hallamos el polinomio característico (que tiene las soluciones de la ecuación dada y muchas más) y factorizamos: $x^3 - 3x^2 + 3x - 1 = (x-1)(x-1)^2$
Solución general(ísima) de una homogénea asociada: $g_n = An^2 + Bn + C$
Extendemos las soluciones iniciales: $a_0 = 1,\ a_1 = a_0 + 1 = 2,\ a_2 = a_1 + 2 = 4$
Solución particular:

$$\left.\begin{aligned} 1 &= C \\ 2 &= A+B+C \\ 4 &= 4A+2B+C \end{aligned}\right\} \Rightarrow A=\frac{1}{2},\ B=\frac{1}{2},\ C=1 \text{ de donde } a_n=\frac{n^2+n+2}{2}$$

Extendemos las condiciones iniciales para una sucesión arbitraria: $a_0 = a,\ a_1 = a_1+1 = a+1,\ a_2 = a_1+2 = a+3$
Solución general de la no homogénea:

$$\left.\begin{aligned} a &= C \\ a+1 &= A+B+C \\ a+3 &= 4A+2B+C \end{aligned}\right\} \Rightarrow A=\frac{1}{2},\ B=\frac{1}{2},\ C=a \text{ de donde } s_n=\frac{n^2+n+2a}{2}$$

Otro tipo de ecuaciones en recurrencia no homogéneas más generales con las que vamos a trabajar son $\sum_{j=0}^{k} a_j x_{n-j} = a_0x_n + a_1x_{n-1} + \ldots + a_kx_{n-k} = \sum_{i=1}^{r} b_i^n p_i(n)$, para $k \leq n$, de donde $a_0, a_1, \cdots, a_k$ son constantes con $a_k \neq 0$ *y* $a_{n-k} \neq 0$, b_i otra constante y $p_i(n)$ un polinomio en n de grado r_i.

Ejemplo 1.11. $a_n = 2a_{n-1} + n + 2^n$ para $n \geq 1$
Condiciones iniciales: $a_0 = 0$.
Término no homogéneo: $1 = b^n p(n) \implies b = 1,\ p(n) = n,\ gr(p) = 1$ y $2^n = b^n p(n) \implies b = 2,\ p(n) = 1,\ gr(p) = 0$
Hallamos el polinomio característico (que tiene las soluciones de la ecuación dada y muchas más) y factorizamos: $(x-2)(x-1)^2(x-2)$
Solución general(ísima) de una homogénea asociada: $g_n = (An+B)\cdot 2^n + Cn + D$
Extendemos las soluciones iniciales: $a_0 = 0,\ a_1 = 2a_0 + 1 + 2^1 = 3,\ a_2 = 2a_1 + 2 + 2^2 = 12,\ a_3 = 2a_2 + 3 + 2^3 = 35$
Solución particular:

$$\left.\begin{aligned} 0 &= B+D \\ 3 &= 2A+2B+C+D \\ 12 &= 8A+4B+2C+D \\ 35 &= 24A+8B+3C+D \end{aligned}\right\} \Rightarrow A=1,\ B=2,\ C=-1,\ D=-2 \text{ de donde } a_n = (n+2)\cdot 2^n - (n+2) = (n+2)(2^n-1)$$

Extendemos las condiciones iniciales para una sucesión arbitraria: $a_0 = a,\ a_1 = 2a_0 + 1 + 2^1 = 2a+3,\ a_2 = 2a_1 + 2 + 2^2 = 4a+12,\ a_3 = 2a_2 + 3 + 2^3 = 8a+35$
Solución general de la no homogénea:

$$\left.\begin{aligned} a &= B+D \\ 2a+3 &= 2A+2B+C+D \\ 4a+12 &= 8A+4B+2C+D \\ 8a+35 &= 24A+8B+3C+D \end{aligned}\right\} \Rightarrow A=1,\ B=a+2,\ C=-1,\ D=-2 \text{ de donde } s_n = (n+a+2)\cdot 2^n - (n+2)$$

2. Álgebras de Boole

2.1. Álgebras de Boole

Definición 2.1 (Álgebra de Boole). Un álgebra de Boole es una seis-upla $(A, \vee, \wedge, \overline{\square}, 0, 1)$ donde A es un conjunto no vacío, $\vee$ y $\wedge$ son operaciones binarias, $\overline{\square}$ es una operación monaria y 0 y 1 son elementos de A. Además $\forall a, b, c \in A$ se cumple:

A1 **Asociatividad** $a \vee (b \vee c) = (a \vee b) \vee c$, $a \wedge (b \wedge c) = (a \wedge b) \wedge c$
A2 **Conmutatividad** $a \vee b = b \vee a$, $a \wedge b = b \wedge a$
A3 **Distributividad** $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$, $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$
A4 **Complementación** $a \vee \overline{x} = 1$, $a \wedge \overline{x} = 0$
A5 **Identidad** $a \vee 0 = a$, $a \wedge 1 = a$

La siguiente definición es equivalente a la anterior:

Definición 2.2 (Huntington). Un álgebra de Boole es una seis-upla $(A, \vee, \wedge, \overline{\square}, 0, 1)$ donde A es un conjunto no vacío, $\vee$ y $\wedge$ son operaciones binarias, $\overline{\square}$ es una operación monaria y 0 y 1 son elementos de A. Además $\forall a, b, c \in A$ se cumple:

A1 **Conmutatividad** $a \vee b = b \vee a$, $a \wedge b = b \wedge a$
A2 **Distributividad** $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$, $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$
A3 **Complementación** $a \vee \overline{a} = 1$, $a \wedge \overline{a} = 0$
A4 **Identidad** $a \vee 0 = a$, $a \wedge 1 = a$

Nota. Los álgebras de Boole cumplen el **principio de dualidad**, pues si tomamos un axioma y cambiamos $\vee$ por $\wedge$, 0 por 1 y el 1 por 0, obtenemos otro axioma. Además, si un teorema es cierto para un álgebra de Boole, también lo es para su dual.

Observación. Los símbolos para operaciones de un álgebra de Boole también se suelen notar de distintas formas:

- $\vee$: $+$, OR.
- $\wedge$: $\cdot$, $\times$, AND.
- $\overline{\square}$: $\square^*$, $\neg\square$, $\square'$, NOT $\square$.
- 0: F (Falso), F (False).
- 1: V (Verdadero), T (True).

Propiedades 2.1. Supongamos que $(B, \vee, \wedge, \overline{\square}, 0, 1)$ es un álgebra de Boole y $x, y, z \in B$. Entonces:

1. **Idempotencia:** $x \vee x = x$; $x \wedge x = x$.
2. **Dominación:** $x \vee 1 = 1$; $x \wedge 0 = 0$.
3. **Absorción:** $x \vee (x \wedge y) = x$; $x \wedge (x \vee y) = x$.
4. **Propiedad cancelativa:** $\left.x \vee y = x \vee z,\ x \wedge y = x \wedge z\right\} \Rightarrow y = z$
5. **Doble complementación:** $\overline{\overline{x}} = x$.
6. $x \vee (\overline{x} \wedge y) = x \vee y$; $x \wedge (\overline{x} \vee y) = x \wedge y$.
7. **Leyes de De Morgan:** $\overline{x \vee y} = \overline{x} \wedge \overline{y}$; $\overline{x \wedge y} = \overline{x} \vee \overline{y}$.
8. Son equivalentes: $x \vee y = y$, $x \wedge y = x$, $\overline{x} \vee y = 1$, $x \wedge \overline{y} = 0$.

Proposición 2.1. Sean $(B_1, \vee_1, \wedge_1, \overline{\square}, 0, 1)$ y $(B_2, \vee_2, \wedge_2, \overline{\square}, 0, 1)$ dos álgebras de Boole. Entonces el conjunto $B_1 \times B_2$ con las operaciones $(x, y) \vee (x', y') = (x \vee_1 x', y \vee_2 y')$ tiene estructura de álgebra de Boole para $x, x' \in B_1,\ y, y' \in B_2$.

Nota. Esta proposición es fácilmente extensible por inducción a $B_1 \times B_2 \times \cdots \times B_n$ siendo B_n conjuntos con estructuras de álgebras de Boole.

Ejemplo 2.1. Sea $\mathbb{B} = \{0, 1\}$. Este conjunto tiene estructura de álgebra de Boole con las operaciones $\vee$ y $\wedge$ de la forma $(B, \vee, \wedge, \overline{\square}, 0, 1)$:

$\vee$	0	1
0	0	1
1	1	1

$\wedge$	0	1
0	0	0
1	0	1

mientras que $\overline{0} = 1$ y $\overline{1} = 0$. Luego por la proposición anterior, sabemos que $(\mathbb{B} \times \mathbb{B}, \vee, \wedge)$ es también un álgebra de Boole. De hecho, $\mathbb{B}^n\ \forall n \in \mathbb{N}$ son álgebras de Boole.

Teorema 2.1 (Orden). Sea $(B, \vee, \wedge)$ un álgebra de Boole. Definimos la **relación de orden en** B como: $x \leq y \iff x \vee y = y$. Además, dados $x, y \in B$ se tiene que $sup\{x, y\} = x \vee y$ e $inf\{x, y\} = x \wedge y$. Además, $max(B) = 1$ y $min(B) = 0$.

Este teorema por tanto nos dice que, al ser éste equivalente a la propiedad 2.1.8, todo álgebra de Boole es un conjunto ordenado $(B, \leq)$. Sin embargo, para que un conjunto ordenado $(X, \leq)$ sea un álgebra de Boole, deben cumplirse las siguientes comdiciones:

- Existen $max(X)$ y $min(X)$ que notaremos como 1 y 0 respectivamente.
- Dados $x, y \in X$, $sup\{x, y\} = x \vee y$ e $inf\{x, y\} = x \wedge y$.
- Para cualquier $x \in X$, $\exists y \in X \implies x \vee y = 1$ y $x \wedge y = 0$.

Una forma muy útil de representar un conjunto ordenado es a través de su **diagrama de Hasse**.

Ejemplo 2.2. Diagrama de Hasse de las álgebras de Boole $\mathbb{B}$, $\mathbb{B}^2$, $\mathbb{B}^3$:

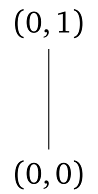

Diagrama Hasse $\mathbb{B}$

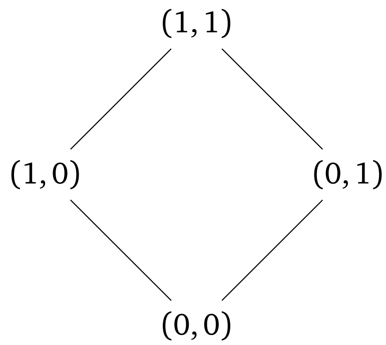

Diagrama Hasse $\mathbb{B}^2$

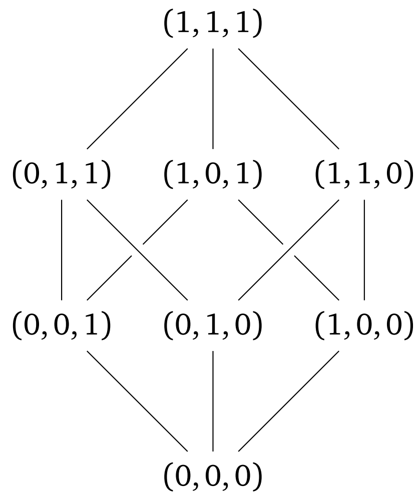

Diagrama Hasse $\mathbb{B}^3$

Propiedades 2.2. Sea $(B, \vee, \wedge, \overline{\square}, 0, 1)$ un álgebra de Boole. Entonces $\forall x, y, z \in A$:

- $0 \leq x \leq 1$.
- Isotonía: Si $x \leq y$, entonces $x \vee z \leq y$ y $x \wedge z \leq y \wedge z$.
- $x \leq y \iff \overline{y} \leq \overline{x} \iff x \leq \overline{y} = 0$.
- $x \wedge y \leq z \iff x \leq \overline{y} \vee z$.

2.2. Átomos de un Álgebra

Definición 2.3 (Maximal y minimal). Sea X un conjunto con una relación de orden $\leq$, y sea $m \in X$. Se dice que m es un **elemento maximal de** X, si y sólo si, no existe $x \in X$ con $x \neq m$ tal que $m \leq x$. De manera análoga, m es un **elemento minimal de** X, si y sólo si, no existe $x \in X$ con $m \neq x$ tal que $x \leq m$.

Definición 2.4 (Átomo). Sea B un álgebra de Boole y $a \in B$. Se dice que a es un **átomo** si a es un elemento minimal de $B \backslash \{0\}$. Es decir, $\forall a \in B \backslash \{0\}$ $(x \leq a \implies x = a)$.

Teorema 2.2. Sea B un álgebra de Boole finita y $x \in X \backslash \{0\}$. Entonces x se expresa de forma única como supremo de átomos.

Lema 2.1. Sea B un álgebra de Boole finita y $x \in X \backslash \{0\}$. Entonces existe $a \in B$ átomo tal que $a \leq x$.

Nota. Denotamos por A_x al conjunto de elementos de A menores o iguales que x.

Parte II.
Ejercicios