Resumen C3

Ignacio Méndez

Definición:

Decimos que R es un **orden parcial** si R cumple ser:

1. **Refleja:** $\forall a \in A. (a,a) \in R$.
2. **Antisimétrica:** $\forall a, b \in A. \big((a,b) \in R \wedge (b,a) \in R\big) \rightarrow a = b$.
3. **Transitiva:** $\forall a, b, c \in A. \big((a,b) \in R \wedge (b,c) \in R\big) \rightarrow (a,c) \in R$.

Definición:

Un orden parcial sobre A lo denotaremos como $(\boldsymbol{A}, \preccurlyeq)$.

Definición:

Sea A un conjunto y $(A, \preccurlyeq)$ un orden parcial.

Decimos que un orden parcial $(A, \preccurlyeq)$ es un **orden total** si $\preccurlyeq$ cumple ser:

1. **Conexo:** $\forall a, b \in A. (a,b) \in R \vee (b,a) \in R$.

Definiciones:

- Un **alfabeto** Σ es un conjunto finito de elementos.
- Un elemento $a \in \Sigma$ lo llamaremos una **letra** o **símbolo**.
- Una **palabra** w sobre Σ es una secuencia finita de letras de Σ.
- El largo $|w|$ de una palabra w sobre Σ es el número de letras.
- Denotaremos ϵ como la **palabra vacía** de largo 0.
- Denotaremos por Σ^* como el **conjunto de todas las palabras** sobre Σ.
- Dado dos palabras $u, v \in \Sigma^*$:

  $$u \cdot v \equiv u \text{ **concatenado** con } v$$

  $u \cdot v$ corresponde a la secuencia u **seguido** de la secuencia v.

- Sea Σ un alfabeto. Se definen las siguientes relaciones entre palabras en Σ^*:
  - $\boldsymbol{u} \leq_{\boldsymbol{p}} \boldsymbol{v}$ si, y solo si, $\exists w \in \Sigma^*. u \cdot w = v$.
  - $\boldsymbol{u} \leq_{\boldsymbol{s}} \boldsymbol{v}$ si, y solo si, $\exists w \in \Sigma^*. w \cdot u = v$.
  - $\boldsymbol{u} \leq_{\boldsymbol{i}} \boldsymbol{v}$ si, y solo si, $\exists w_1, w_2 \in \Sigma^*. w_1 \cdot u \cdot w_2 = v$.

No está en temario

Definición:

Sea $(A, \preccurlyeq)$ un orden parcial y $S \subseteq A$ distinto de $\emptyset$.

- $c \in A$ es una **cota superior** de S ssi $\boxed{\forall y \in S. y \preccurlyeq c}$, es decir, es mayor o igual a todos los elementos de S.
- $\hat{x} \in S$ es un **maximal** ssi $\boxed{\forall y \in S.\ \hat{x} \preccurlyeq y \to \hat{x} = y}$, es decir, ningún elemento es mayor que el.
- $x^{\uparrow} \in S$ es un **máximo** ssi $\boxed{\forall y \in S. y \preccurlyeq x^{\uparrow}}$, es decir, es mayor o igual a cualquier elemento de S.
- $c \in A$ es una **cota inferior** de S ssi $\boxed{\forall y \in S. c \preccurlyeq y}$, es decir, es menor o igual a todos los elementos de S.
- $\breve{x} \in S$ es un **minimal** ssi $\boxed{\forall y \in S.\ y \preccurlyeq \breve{x} \to \breve{x} = y}$, es decir, ningún elemento es menor que el.
- $x^{\downarrow} \in S$ es un **mínimo** ssi $\boxed{\forall y \in S. x^{\downarrow} \preccurlyeq y}$, es decir, es menor o igual a cualquier elemento de S.

Decimos que $c^* \in A$ es un **ínfimo** de S si:

1. c^* es una cota inferior de S.
2. Para toda cota inferior c de S se cumple que $c \preccurlyeq c^*$.
3. Es decir, es la mayor de las cotas inferiores.

Decimos que $c^* \in A$ es un **supremo** de S si:

1. c^* es una cota superior de S.
2. Para toda cota inferior c de S se cumple que $c^* \preccurlyeq c$.
3. Es decir, es la menor de las cotas superiores.

Definición:

Sea A un conjunto y $R \subseteq A \times A$ una relación.

Una relación $R^r \subseteq A \times A$ es la **clausura refleja** de R si:

1. $R \subseteq R^r$.
2. R^r es refleja.
3. Para toda otra relación refleja R' con $R \subseteq R'$ se cumple $R^r \subseteq R'$.

→ R^r es la **menor relación refleja** que contiene a R.

Una relación $R^t \subseteq A \times A$ es la **clausura transitiva** de R si:

1. $R \subseteq R^t$.
2. R^t es transitiva.
3. Para toda otra relación transitiva R' con $R \subseteq R'$ se cumple $R^t \subseteq R'$.

→ R^r es la **menor relación transitiva** que contiene a R.

Definición:

Sea A un conjunto y $R \subseteq A \times A$ una relación binaria.

Decimos que R es una **relación de equivalencia** si R cumple ser:

1. **Refleja**: $\forall a \in A. (a, a) \in R$.
2. **Simétrica**: $\forall a, b \in A. (a, b) \in R \rightarrow (b, a) \in R$.
3. **Transitiva**: $\forall a, b, c \in A. \big((a, b) \in R \land (b, c) \in R\big) \rightarrow (a, c) \in R$.

Definición:

Sea A un conjunto y $\mathcal{S} \subseteq 2^A$ (un conjunto de subconjuntos de A).

Decimos que $\mathcal{S}$ es una **partición** de A si:

1. Todos los elementos de $\mathcal{S}$ son distintos de vacío.
$$\forall X \in \mathcal{S}. X \neq \emptyset$$
2. La unión de todos los elementos de $\mathcal{S}$ es igual a A.
$$\bigcup \mathcal{S} = A$$
3. Todos los elementos de $\mathcal{S}$ son disjuntos de a pares.
$$\forall X, Y \in \mathcal{S}. X \neq Y \rightarrow X \cap Y = \emptyset$$

Definición:

Sea A un conjunto y $\sim \subseteq A \times A$ es una relación de equivalencia.

Sea $x \in A$. Se define la **clase de equivalencia de x** según $\sim$ como:

$$[x]_{\sim} = \{y \in A \mid x \sim y\}$$

$[x]_{\sim}$ son todos los elementos de A que son "equivalentes" a x.

Propiedades:

1. $\forall x \in A.\ x \in [x]_{\sim}$.
2. $x \sim y$ si, y solo si, $[x]_{\sim} = [y]_{\sim}$.
3. Si $x \nsim y$, entonces $[x]_{\sim} \cap [y]_{\sim} = \emptyset$.

El **conjunto cociente** $A/\sim$ de A con respecto a $\sim$ se define:

$$A/\sim\, = \{\, [x]_{\sim} \mid x \in A\}$$

El conjunto cociente $A/\sim$ es una partición de A.

Definición:

Sea A y B conjuntos no vacíos

Una relación $f \subseteq A \times B$ es una **función** si para todo elemento $a \in A$ existe un único elemento $b \in B$ tal que $(a, b) \in f$.

1. $\forall a \in A. \exists b \in B. (a, b) \in f.$
2. $\forall a \in A.\ \forall b_1, b_2 \in B.\ \big((a, b_1) \in f \wedge (a, b_2) \in f\big) \rightarrow b_1 = b_2.$

Si $f \subseteq A \times B$ es una **función**, entonces escribiremos:

- $f: A \rightarrow B,$ para decir que f es una función de A a B.
- $f(a) = b,$ para decir que $(a, b) \in f$.
    - *"b es la **imagen** de a en f"*
    - *"a es una **preimagen** de b en f"*

Una relación $f \subseteq A \times B$ es una **función parcial** si para todo elemento $a \in A$, si existe un elemento $b \in B$ tal que $(a, b) \in f$, entonces b es único.

$$\forall a \in A.\ \forall b_1, b_2 \in B.\ \big((a, b_1) \in f \wedge (a, b_2) \in f\big) \rightarrow b_1 = b_2$$

Si $f \subseteq A \times B$ es una **función parcial**, entonces escribiremos:

- $f: A \rightharpoonup B,$ para decir que f es una función parcial de A a B.
- $f(a) = b,$ para decir que $(a, b) \in f$.

Se define el **dominio** e **imagen** de $f: A \rightharpoonup B$ como:

- $dom(f) = \pi_1(f) = \{a \in A \mid \exists b \in B.\ (a, b) \in f\}$
- $img(f) = \pi_2(f) = \{b \in B \mid \exists a \in A.\ (a, b) \in f\}$

Sea $f: A \rightharpoonup B$, entonces f es una función ssi $dom(f) = A$.

Definiciones:

Sea A y B conjuntos no vacíos.

Una función $f: A \rightarrow B$ se dice:

1. **Inyectiva** si no existen dos elementos en A con la misma imagen.

$$\forall a_1, a_2 \in A. f(a_1) = f(a_1) \rightarrow \; a_1 = a_2$$

2. **Sobreyectiva** si todo elemento en B tiene una preimagen.

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

3. **Biyectiva** si es inyectiva y sobreyectiva **a la vez**.

Notación:

- Inyectiva ≡ **1-a-1**.
- Sobreyectiva ≡ función **sobre** o **onto**.
- Biyectiva ≡ **epiyectiva**.

Principio del Palomar.

"Si N **palomas** se distribuyen en M **palomares** y tengo mas palomas que palomares ($N > M$), entonces al menos habrá un palomar con mas de una paloma"

Si $f: A \rightarrow B$ y. $|B| < |A|$, entonces f **NO** puede ser **inyectiva**, esto es:

$$\exists a_1, a_2 \in A. \quad a_1 \neq a_2 \;\wedge f(a_1) = f(a_2)$$

Definición:

Sea A y B dos conjuntos, serán **equinumerosos** entre sí si existe una biyección $f: A \rightarrow B$.
Si A es **equinumeroso** con B lo anotaremos como $|A| = |B|$.

La relación $|\cdot| = |\cdot|$ es una **relación de equivalencia**, esto es:

1. Refleja.
2. Simétrica.
3. Transitiva.

Para un conjunto A, denotaremos por $|A|$ su **clase de equivalencia**
según la relación $|\cdot| = |\cdot|$.

Definición:

A es **numerable** si tiene la misma cardinalidad que un subconjunto de $\mathbb{N}$.

$$\exists S \subseteq \mathbb{N}.\ |A| = |S|$$

A es **numerable** si, y solo si, existe una secuencia (finita o infinita) en A:

$$a_0, a_1, a_2, a_3, \ldots$$

1. $a_i \neq a_j$ para todo $i \neq j$.
2. Para todo $a \in A$, existe un $i \in \mathbb{N}$ tal que $a = a_i$.

A es numerable si, y solo si, todos sus elementos se pueden poner en una lista.

Teorema:

$\mathbb{Q}$ y $\mathbb{N} \times \mathbb{N}$ son conjuntos **numerables**, $\mathbb{R}$ no lo es.

Teorema de Cantor:

NO existe una **biyección** entre A y el conjunto potencia 2^A.

Definición:

Un **problema de decisión** está compuesto por:

1. Un conjunto de **inputs** (llamados instancias).
   a. Números, grafos, palabras, funciones, etc.
2. Una **pregunta** sobre los inputs que se responde con **SI** o **NO**.

Sea I un conjunto de inputs (instancias).

Un **problema de decisión** es una función:

$$P: I \rightarrow \{0,1\}$$

Ejemplo:

Sea $PRIMO: \mathbb{N} \to \{0,1\}$ tal que para todo $n \in \mathbb{N}$:

$PRIMO(n) = 1$ si, y sólo si, n es un número primo.

- Una solución `Program` es una **solución para el problema de decisión** P si para todo input $X \in I$ se cumple:

$$P(X) = 1 \text{ si, y sólo si, al ejecutar } \texttt{Program} \text{ con } X \text{ retorna } 1$$

Simplificación

Todo input lo podemos representar con **palabras** de ceros y unos.

Definición:

Un problema de decisión P es una función: $P: \{0,1\}^* \to \{0,1\}$. Se define $\mathcal{P}$ como el conjunto de todos los problemas de decisión:

$$\mathcal{P} = \{\, P: \{0,1\}^* \to \{0,1\} \,\}$$

Teorema:

Los conjuntos $\mathcal{P}$ y $2^{\{0,1\}^*}$ son **equinumerosos**. NO es numerable.

Definición:

Se define el conjunto $\mathcal{O}(g)$ de todas las funciones $f: \mathbb{N} \to \mathbb{R}$ tal que **existe** $c \in \mathbb{R}$ y $n_0 \in \mathbb{N}$ tal que **para todo** $n \geq n_0$:

$$f(n) \leq c \cdot g(n)$$

En notación lógica:

$$\mathcal{O}(g) = \{\, f: \mathbb{N} \to \mathbb{R} \mid \exists c \in \mathbb{R}. \exists n_0 \in \mathbb{N}. \forall n \geq n_0. f(n) \leq c \cdot g(n) \,\}$$

Si $f \in \mathcal{O}(g)$, entonces f **crece mas lento o igual** que g.

Notación:

- f es $\mathcal{O}(g)$ ("f es O-grande de g")
- f es de **orden** g
- $f = \mathcal{O}(g)$ (solo es notación)

Teorema:

1. Sea $f(x) = a_k x^k + \cdots + a_1 x + a_0$ un polinomio sobre $\mathbb{N}$, entonces:
$$f \in \mathcal{O}(x^k)$$
2. $x^{k+1} \notin \mathcal{O}(x^k)$ para todo $k \in \mathbb{N}$.
3. Para todo $a, b > 1$, se tiene que $\log_a(n) \in \mathcal{O}(\log_b(n))$.
4. Para todo $a < b$, se tiene que $a^n \in \mathcal{O}(b^n)$ y $b^n \notin \mathcal{O}(a^n)$.
5. Para todo $a \in \mathbb{N}$, se tiene que $a^n \in \mathcal{O}(n!)$ y $n! \notin \mathcal{O}(a^n)$.
6. $n! \in \mathcal{O}(2^{n \cdot \log n})$.

Notación	Nombre
$\mathcal{O}(1)$	Constante
$\mathcal{O}(\log n)$	Logarítmico
$\mathcal{O}(n)$	Lineal
$\mathcal{O}(n \log n)$	$n \log n$
$\mathcal{O}(n^2)$	Cuadrático
$\mathcal{O}(n^3)$	Cúbico
$\mathcal{O}(n^m)$	Polinomial
$\mathcal{O}(k^n)$	Exponencial
$\mathcal{O}(n!)$	Factorial

Teorema:

- Si $f_1 \in \mathcal{O}(g_1)$ y $f_2 \in \mathcal{O}(g_2)$, entonces $f_1 + f_2 \in \mathcal{O}(\max\{g_1, g_2\})$.
- Si $f_1 \in \mathcal{O}(g_1)$ y $f_2 \in \mathcal{O}(g_2)$, entonces $f_1 \cdot f_2 \in \mathcal{O}(g_1 \cdot g_2)$.

Definición:

Se define el conjunto $\Omega(g)$ de todas las funciones $f: \mathbb{N} \to \mathbb{R}$ tal que **existe** $c \in \mathbb{R}$ y $n_0 \in \mathbb{N}$, tal que **para todo** $n \geq n_0$:
$$f(n) \geq c \cdot g(n)$$

En notación lógica:

$$\Omega(g) = \{\, f: \mathbb{N} \to \mathbb{R} \mid \exists c \in \mathbb{R}.\, \exists n_0 \in \mathbb{N}.\, \forall n \geq n_0.\, f(n) \geq c \cdot g(n) \,\}$$

Si $f \in \Omega(g)$, entonces f **crece mas rápido o igual** que g.

Definición:

Se define el conjunto $\Theta(g)$ de todas las funciones $f: \mathbb{N} \to \mathbb{R}$ tal que **existen** $c_1, c_2 \in \mathbb{R}$ y $n_0 \in \mathbb{N}$, tal que **para todo** $n \geq n_0$:

$$c_1 \cdot g(n) \leq f(n) \leq c_2 \cdot g(n)$$

En notación lógica:

$$\Theta(g) = \{\, f: \mathbb{N} \to \mathbb{R} \mid \exists c_1, c_2 \in \mathbb{R}. \exists n_0 \in \mathbb{N}. \forall n \geq n_0.\ \ c_1 \cdot g(n) \leq f(n) \leq c_2 \cdot g(n) \,\}$$

$f \in \Theta(g)$ si, y solo si, $f \in \Omega(g)$ y $f \in \mathcal{O}(g)$

Teorema:

1. Sea $f(n) = a_k n^k + \cdots + a_1 n + a_0$ un polinomio sobre $\mathbb{N}$, entonces:
$$f \in \Theta(n^k)$$
2. $n^{k+1} \notin \Theta(n^k)$ para todo $k \in \mathbb{N}$.
3. Para todo $a, b > 1$, se tiene que $\log_a(n) \in \Theta(\log_b(n))$.
4. Si $f_1 \in \Theta(g)$ y $f_2 \in \Theta(g)$, entonces $f_1 + f_2 \in \Theta(g)$.
5. Si $f_1 \in \Theta(g_1)$ y $f_2 \in \Theta(g_2)$, entonces $f_1 \cdot f_2 \in \Theta(g_1 \cdot g_2)$.

Definición:

Un **algoritmo** es una secuencia finita de instrucciones precisas para realizar una computación o resolver un problema.

Para un **algoritmo** A sobre un conjunto de inputs I se define la función:

$$tiempo_A: I \to \mathbb{N}$$

Tal que para todo input $i \in I$:

$$tiempo_A(i) = número\ de\ \boldsymbol{pasos\ realizados}\ por\ A\ con\ input\ i$$

Un algoritmo A es el "más eficiente" si para todo algoritmo B que calcula lo mismo que A se tiene que $tiempo_A(i) \leq tiempo_B(i)$ para todo $i \in I$.

Definición:

Para un conjunto de inputs I se define su función tamaño:

$$|\cdot|: I \rightarrow \mathbb{N}$$

Tal que para todo input $i \in I$:

$|i| =$ Es el tamaño de i según su "**representación**".

En general, $|i|$ será un valor que "representa" el tamaño de i y que nos será útil en nuestro análisis/modelación.

En general:

La definición más absoluta y general del tamaño $|i|$:

$|i| =$ número de bits de una **codificación** "razonable" de i

Siempre vamos a depender de la codificación del *input*.

Definición:

Para un algoritmo A y su conjunto de *inputs* i se definen funciones:

$$peor \cdot caso_A: \mathbb{N} \rightarrow \mathbb{N} \quad \text{y} \quad mejor \cdot caso_A: \mathbb{N} \rightarrow \mathbb{N}$$

- Función de complejidad en el **peor caso** de A:

$$peor \cdot caso_A(n) = \max_{i \in I}\{tiempo_A(i) \mid |i| = n\}$$

- Función de complejidad en el **mejor caso** de A:

$$mejor \cdot caso_A(n) = \min_{i \in I}\{tiempo_A(i) \mid |i| = n\}$$