Logica Computacional: Definiciones

Giuliano Scaglioni

2016

1 Cardinales

1.1 Coordinable

Sean A y B conjuntos, decimos que A es coordinable con B ($A \sim B$) si existe una función $f : A \to B$ biyectiva.

1.2 Sección Inicial (I_n)

Al conjunto $I_n = \{1, 2, 3, ..., n\}$ se lo denomina sección inicial $\forall n \in \mathbb{N}$

1.3 Finito

A conjunto. Decimos que A es finitio si $A = \emptyset$ o existe $n \in \mathbb{N} | A \sim I_n$

1.4 Cardinal

- $Card(\emptyset) = 0$
- $Card(I_n) = n$
- $Card(\mathbb{N}) = \aleph_0$
- $Card([0, 1]) = c$

Notación: $card(A) = \#A = |A|$

1.5 Comparación de cardinales

Sea A conjunto

- $\#A \leq \#B$ si existe $f : A \to B$ inyectiva.
- $\#A \geq \#B$ si existe $f : A \to B$ sobreyectiva.
- $\#A = \#B$ si existe $f : A \to B$ biyectiva.
- $\#A < \#B$ si $\#A \leq \#B$ y $\#A \neq \#B$.
- $\#A > \#B$ si $\#A \geq \#B$ y $\#A \neq \#B$.

1.6 Numerable

A es numerable si A es finito o $A \sim \mathbb{N}$

2 Lenguajes

2.1 Alfabeto

Sea A conjunto, $A \neq \emptyset$, A es un alfabeto.

2.2 Expresión

Una expresión es una secuencia finita de elementos de A o una cadena vacia que representamos con λ

2.3 long(E)

Sea $E = a_0 a_1 ... a_n$ una expresión sobre A, se define $long(E) = n + 1$ y $long(\lambda) = 0$

2.4 A*

$A^* = \bigcup_{n\in\mathbb{N}} A^n$, donde A^n es el conjunto de todas las expresiones sobre A de longitud n, y $A^0 = \lambda$. A^* es el conjunto de todas las expresiones posibles sobre A.

2.5 Lenguaje

A alfabeto, un lenguaje sobre A es un subconjunto $\Sigma \neq \emptyset$ de A^*, $(\Sigma \subset A^*)$

2.6 Concatenación

A alfabeto, $E, F \in A^* | E_0 = a_0...a_n, F = b_0...b_s$ se define $EF = a_0...a_n b_0...b_s$

3 Lógica Proposicional: Sintaxis

3.1 Fórmula

Se denomina fórmula de la lógica proposicional a una expresión sobre A (el alfabeto de la lógica proposicional) que cumple:

- $P_i \in Form = F$
- $\alpha \in F \implies \neg\alpha \in F$
- $\alpha, \beta \in F \implies (\alpha * \beta) \in F, \qquad * \in \{\wedge, \vee, \rightarrow\}$

3.2 Cadena de formación

Una cadena de formación es una sucesión finita $X_1, ..., X_n$ de elementos de A^* que verifica la siguiente propiedad:
Sea $1 \leq i \leq n$

- $X_i \in Var$ ó
- $(\exists\, 1 \leq j < i \leq n | X_i = \neg X_j)$ ó
- $(\exists\, 1 \leq j, k < i \leq n | X_i = (X_j \wedge X_k))$ ó
- $(\exists\, 1 \leq j, k < i \leq n | X_i = (X_j \vee X_k))$ ó
- $(\exists\, 1 \leq j, k < i \leq n | X_i = (X_j \rightarrow X_k))$

3.3 Eslabón

Se denomina eslabón a un elemento de una cadena de formación.

3.4 Subcadena

Sea $X_1, ..., X_n$ una cadena de formación.
Decimos que $X_{i_1}, ..., X_{i_k}$ es una subcadena de la anterior si:

- $X_{i_1}, ..., X_{i_k}$ es una cadena de formación
- $1 \leq X_{i_1} < ... < X_{i_k} = n$

3.5 Cadena de formación minimal

Una cadena de formación es minimal si la unica subcadena que tiene es ella misma.

3.6 Complejidad

Sea E una expresión, se define complejidad de E ($C(E)$) a la cantidad de apariciones de los conectivos $\neg, \wedge, \vee, \to$

3.7 Complejidad binaria

Sea E una expresión, se define complejidad binaria de E ($Cb(E)$) a la cantidad de apariciones de los conectivos $\wedge, \vee, \to$

3.8 Peso

Sea E una expresión, se define peso de E ($C(E)$) a la cantidad de paréntesis que abren menos la cantidad de paréntesis que cierran.

3.9 Subfórmula

Sea $\alpha \in F$, definimos subfórmulas de α ($s(\alpha)$) de forma inductiva.

CB) Si $C(\alpha) = 0 \implies \alpha = P_j \in Var$
$s(\alpha) = \{\alpha\}$

HI) Si $C(\alpha) \leq n \implies$ conocemos $s(\alpha)$

TI) Si $C(\alpha) = n + 1$

- $\alpha = \neg\beta$, defino $s(\alpha) = \alpha \cup s(\beta)$
- $\alpha = (\beta_1 * \beta_2)$, defino $s(\alpha) = \alpha \cup s(\beta_1) \cup s(\beta_2)$ $* \in \{\to, \wedge, \vee\}$

4 Lógica Proposicional: Semántica

4.1 Valuación

Una función $v : Form \to \{0, 1\}$ se llama valuación si:

- $v(\neg\alpha) = 1 - v(\alpha)$
- $v(\alpha \wedge \beta) = min\{v(\alpha),\ v(\beta)\}$
- $v(\alpha \vee \beta) = max\{v(\alpha),\ v(\beta)\}$
- $v(\alpha \to \beta) = max\{1 - v(\alpha),\ v(\beta)\}$

4.2 Tautología

Sea $\alpha \in F$, decimos que α es una tautología si $v(\alpha) = 1 \quad \forall v$ valuación.

4.3 Contradicción

Sea $\alpha \in F$, decimos que α es una contradicción si $v(\alpha) = 0 \quad \forall v$ valuación.

4.4 Contingencia

Sea $\alpha \in F$, decimos que α es una contingencia si no es tautología ni contradicción, es decir: $\exists\ v\ val.\ |\ v(\alpha) = 1$ y $\exists\ w\ val.\ |\ w(\alpha) = 0$

4.5 Equivalente

Sea $\alpha, \beta \in F$. Decimos que α y β son equivalentes si $v(\alpha) = v(\beta)$, $\forall v$ valuación
Notación: $\alpha \equiv \beta$

4.6 Función booleana

Es una función $f : \{0,1\}^k \to \{0,1\}$ con $n \in \mathbb{N}_{>0}$

4.7 Adecuado

Sea C un conjunto de conectivos, C es adecuado si $\forall \beta \in F,\ \exists \alpha \in F_C \mid \alpha \equiv \beta$

4.8 Satisface

Sea $\alpha \in F$, V val., decimos que V satisface α si $V(\alpha) = 1$.

4.9 Satisfacible

Sea $\alpha \in F$ es satisfacible si no es una contradiccion. Sea $\Gamma \subset F$ es satisfacible si $\exists\ v\ val. \mid v(\alpha) = 1,\ \forall \alpha \in \Gamma$

4.10 Insatisfacible

Decimos que Γ es insatisfacible si $\forall v\ val,\ \exists \alpha \in \Gamma\ |v(\alpha) = 0$

4.11 Consecuencia

Sea $\Gamma \subset F,\ \alpha \in F$. α es consecuencia de Γ si cumple:

- $v(\Gamma) = 1 \implies v(\alpha) = 1 \quad \forall v\ val.$

Notación: $C(\Gamma)$

4.12 Finitamente satisfacible (f.s.)

Sea $\Gamma \subset F$. Γ es finitamente satisfacible si todo subconjunto finito de Γ es satisfacible.

4.13 Literal

Un literal es una formula que es una variable o una variable negada.

5 Teoría Axiomática

5.1 Axiomas

Axioma 1 $(\alpha \to (\beta \to \alpha))$

Axioma 2 $(\alpha \to (\beta \to \gamma)) \to ((\alpha \to \beta) \to (\alpha \to \gamma))$

Axioma 3 $((\neg\alpha \to \neg\beta) \to ((\neg\alpha \to \beta) \to \alpha))$

$\alpha, \beta, \gamma \in F$

5.2 Prueba

Una prueba es una sucesión finita de fórmulas $\alpha_1, ..., \alpha_n = \alpha$ tal que α_i es un axioma o existe $1 \leq j, k \leq i \mid \alpha_k = (\alpha_j \to \alpha_i)$

5.3 Modus Ponens

Datos: $\alpha_j, (\alpha_j \to \alpha_i)$ obtenemos α_i

5.4 Teorema

$\alpha \in F \mid \alpha$ es demostrable.

5.5 α se deduce a partir de Γ

$\Gamma \subset F$, $\alpha \in F$. Decimos que α es demostrable a partir de Γ si existe una prueba de α a partir de Γ $\alpha_1, ..., \alpha_n$ tal que:

- α_i es un axioma ó
- α_i se obtiene a partir de m.p. de dos anteriores ó
- $\alpha_i \in \Gamma$, con $1 \leq i \leq n$

Notación: $\Gamma \vdash \alpha$ (si $\emptyset \vdash \alpha \implies \alpha$ es un teorema)

5.6 Consistente

Γ es consistente si $\nexists \varphi \in F \mid \Gamma \vdash \alpha$ y $\Gamma \vdash \neg\alpha$

5.7 Maximal Consistente (m.c.)

Γ es maximal consistente si $\forall \varphi \in F$, $\varphi \in \Gamma$ ó $\Gamma \cup \{\varphi\}$ no es consistente.

5.8 Sistema Axiomático Consistente

Un sistema axiomático es consistente si $\nexists \varphi \in F \mid \vdash_s \varphi$ y $\vdash_s \neg\varphi$

6 Lenguajes de 1º Orden: Sintaxis

6.1 Alfabeto

Conjunto $\mathcal{C}$ de simbolos de constantes $\mathcal{C} = \{c_0, c_1 ...\}$

Conjunto $\mathcal{F}$ de funciones $\mathcal{F} = \{f_0^{k_0}, f_1^{k_1} ...\}$

Conjunto $\mathcal{P} \neq \emptyset$ de predicados $\mathcal{P} = \{P_0^{k_0}, P_1^{k_1} ...\}$

Común para todos los lenguajes de 1º orden:

Variables $var = \{X_0, X_1 ...\}$

Conectivos $\{\wedge, \vee, \rightarrow, \neg, \forall\}$

Paréntesis $\{(,)\}$

6.2 Término

1. Toda variable es un término
2. Toda constante es un término
3. Si $f^k \in \mathcal{F}$ es un simbolo de función y $t_1, ..., t_k$ son términos $\implies f^k(t_1, ..., t_k)$ es un término
4. t es un término si se construye aplicando 1, 2 y 3 finitas veces.

Notación: $term(L)$

6.3 Fórmula

1. Si $P^k \in \mathcal{P}$ es un símbolo de predicado y $t_1, ..., t_k$ son términos $\implies$ $P^k(t_1, ..., t_k)$ es una fórmula.
2. Si α es una fórmula $\implies$ $\neg\alpha$ es una fórmula.
3. Si α, β son formulas $\implies$ $(\alpha \wedge \beta), (\alpha \vee \beta)$ y $(\alpha \to \beta)$ son fórmulas.
4. Si α es una fórmula y X es una variable $\implies$ $\forall X \alpha$ es una fórmula.
5. α es una fórmula si se construye aplicando 1, 2, 3 y 4 finitas veces.

Convención: escribimos $\exists X \alpha$ en lugar de $\neg\forall X \neg\alpha$

6.4 Término cerrado

Un término es cerrado si no tiene variables.

6.5 Variable ligada

Una aparición de una variable esta ligada si esta al alcance de un cuantificador. Si todas sus apariciones son ligadas entonces es una variable ligada.

6.6 Variable libre

Una aparición de una variable esta libre si no esta ligada. Si todas las apariciones son libres la variable esta libre.

6.7 Enunciado o sentencia

Un enunciado o sentencia es una formula con todas sus variables ligadas.

7 Lenguajes de 1º Orden: Semántica

7.1 Interpretación

$\mathcal{I}$ de un lenguaje de primer $\mathcal{L}$ orden consta de:

1. Un conjunto no vacío $U_{\mathcal{I}}$ llamado universo o dominio.
2. Las siguientes interpretaciones para los simbolos de $\mathcal{L}$:
   (a) Si $c \in \mathcal{C} \implies c$ se interpreta como un elemento $c_{\mathcal{I}} \in U_{\mathcal{I}}$ fijo.
   (b) Si $f^k \in \mathcal{F} \implies f^k$ se interpreta como una función $f^k_{\mathcal{I}} : U^k_{\mathcal{I}} \to U_{\mathcal{I}}$
   (c) Si $P^k \in \mathcal{P} \implies P^k$ se interpreta como un predicado $P^k_{\mathcal{I}} \subset \mathcal{U}_{\mathcal{I}}$

7.2 Valuación

Fijada un interpretación $\mathcal{I}$ una valuación para $\mathcal{I}$ es una función $v : var \to U_{\mathcal{I}}$.
Para interpretar términos extendemos v a $\bar{v} : term \to U_{\mathcal{I}}$ y sea t término:

1. Si $t \in var \implies \bar{v}(t) = v(t)$
2. Si $t \in \mathcal{C} \implies \bar{v}(t) = c_{\mathcal{I}}$
3. Si $t = f^k(t_1, ..., t_k), f^k \in \mathcal{F} \implies \bar{v}(t) = f^k_{\mathcal{I}}(\bar{v}(t_1), ..., \bar{v}(t_k))$

7.3 $V_{x_i=a}$

Sea v una valuación para $\mathcal{I}$, y sea $a \in U_{\mathcal{I}}$, definimos la valuación

$$V_{x_i=a} : var \to U_{\mathcal{I}} / V_{x_i=a}(y) = \begin{cases} v(y) & y \neq x_i \\ a & y = x_i \end{cases}$$

7.4 Interpretación de fórmulas

Sea $\mathcal{I}$ de $\mathcal{L}$ de primer orden y v una valuación para esa $\mathcal{I}$. Decimos que $\alpha \in Form(\mathcal{L})$ es verdadera en $\mathcal{I}$ bajo la valuación v si:

1. $V_{\mathcal{I},v}(\mathcal{P}^k(t_1, ..., t_k))$
2. $v_{\mathcal{I},v}(\neg\alpha) = 1 - v_{\mathcal{I},v}(\alpha)$
3. $v_{\mathcal{I},v}(\alpha_1 \wedge \alpha_2) = min\{v_{\mathcal{I},v}(\beta_1), v_{\mathcal{I},v}(\beta_2)\}$
4. $v_{\mathcal{I},v}(\alpha_1 \vee \alpha_2) = max\{v_{\mathcal{I},v}(\beta_1), v_{\mathcal{I},v}(\beta_2)\}$
5. $v_{\mathcal{I},v}(\alpha_1 \to \alpha_2) = max\{1 - v_{\mathcal{I},v}(\beta_1), v_{\mathcal{I},v}(\beta_2)\}$
6. $v_{\mathcal{I},v}(\forall x_i \alpha) = 1 \leftrightarrow v_{\mathcal{I},v_{x_i=a}}(\alpha), \quad \forall a \in U_{\mathcal{I}}$
7. $v_{\mathcal{I},v}(\exists x_i \alpha) = 1 \leftrightarrow v_{\mathcal{I},v_{x_i=a}}(\alpha), \quad$ para algún $a \in U_{\mathcal{I}}$

7.5 Satisfacible

Sea $\mathcal{L}$ de primer orden y $\alpha \in F$. α es satisfacible si exíste una $\mathcal{I}$ de $\mathcal{L}$ y una $v\ val.$ $v : var \to U_{\mathcal{I}} \mid v_{\mathcal{I},v}(\alpha) = 1$

7.6 Verdadera o válida en I

α es verdadera o válida en $\mathcal{I}$ si $v_{\mathcal{I},v}(\alpha) = 1 \forall v\ val.$

7.7 Universalmente válida

α es universalmente válida si $v_{\mathcal{I},v}(\alpha) = 1 \forall \mathcal{I}, \forall v$

7.8 Consecuencia semántica

$\Gamma \subset F, \alpha \in F, \alpha$ es consecuencia semántica de Γ si $v_{\mathcal{I},v}(\Gamma) = 1 \implies v_{\mathcal{I},v}(\alpha) = 1$
Notación: $\Gamma \models \alpha$

7.9 Lenguaje con igualdad

Es un lenguaje de primer orden que tiene un predicado binario que siempre se interpreta con la igualdad.

7.10 Expresa

$\mathcal{L}$ de primer orden. $\mathcal{I}, \alpha$ fórmula con una única variable libre $\alpha(x)$. $A = \{t \in U_{\mathcal{I}} \mid v_{\mathcal{I},v_{x=t}}(\alpha(x)) = 1\}$ Decimos que α expresa A.

7.11 Expresable

Decimos que A conjunto es expresable en $\mathcal{I}$ si $\exists \alpha(x) \in F$ que lo exprese.

7.12 Distinguible

$\mathcal{L}$ de primer orden, $\mathcal{I}$ interpretación con universo $U_{\mathcal{I}}$, $a \in U_{\mathcal{I}}$, se dice que a es distinguible si $\{a\}$ es expresable.

7.13 Isomorfismo

$\mathcal{L}$ de primer orden, $\mathcal{I}_1, \mathcal{I}_2$ interpretaciones con universos U_1 y U_2.
Una función $F : U_1 \to U_2$ es isomorfismo si

1. F es biyectiva
2. Sea $c \in \mathcal{C}$ y $c_{\mathcal{I}_1}, c_{\mathcal{I}_2}$ sus respectivas interpretaciones $\implies F(c_{\mathcal{I}_1}) = c_{\mathcal{I}_2}$
3. $f_k \in \mathcal{F} \implies F(f^k_{\mathcal{I}_1}(t_1, ..., t_k)) = f^k_{\mathcal{I}_2}(F(t_1), ..., F(t_k))$
4. $P \in \mathcal{P} \implies (a_1, ..., a_k) \in P^k_{\mathcal{I}_1} \leftrightarrow (F(a_1), ..., F(a_k)) \in P^k_{\mathcal{I}_2}$

8 Lenguaje S

8.1 Recursión Primitiva Tipo I (ERI)

Sea $f : \mathbb{N} \to \mathbb{N}$, decimos que f se obtiene por un ERI a partir de $g : \mathbb{N}^2 \to \mathbb{N}$ si: $f(0) = k$ y $f(n+1) = g(n, f(n))$

8.2 Recursion Primitiva Tipo II (ERII)

Sean $f : \mathbb{N}^{n+1} \to \mathbb{N},\ g : \mathbb{N}^{n+2} \to \mathbb{N}$ y $h : \mathbb{N}^n \to \mathbb{N}$ funciones.
Decimos que f se obtiene por un ERII a partir de g y h si:
$f(x_1, ..., x_n, 0) = h(x_1, ..., x_n)$
$f(x_1, ..., x_n, t + 1) = g(x_1, ..., x_n, t, f(x_1, ..., x_n, t))$

8.3 Funciones iniciales

- $cero : \mathbb{N} \to \mathbb{N}/cero(n) = 0$
- $suc : \mathbb{N} \to \mathbb{N}/suc(n) = n + 1$
- $\Pi^k_i : \mathbb{N}^k \to \mathbb{N}/\Pi^k_i(x_1, ..., x_n) = x_i$

8.4 Clase PRC

Una clase C de funciones totales es PRC si

1. Las funciones iniciales estan en C
2. Si f se obtiene a partir de funciones que estan en C mediante composición o recursion primitiva $\implies$ $f \in C$

8.5 Funcion RP

Una función es RP si se puede obtener a partir de las funciones iniciales aplicando un número finito de composiciones y/o recursiones primitivas.

8.6 Funciones de Gödel

Sea $k \in \mathbb{N} \geq 1$, para cada k se define la función

$$[\cdot, ..., \cdot] : \mathbb{N}^{k+1} \to \mathbb{N}/[(a_0, ..., a_k)] = P_0^{a_0} \cdot ... \cdot P_k^{a_k}$$

Con $P_j < P_{j+1}$ primos consecutivos

8.7 Indicadores de Gödel

$$|\cdot| : \mathbb{N} \to \mathbb{N} / |n| = \begin{cases} long(n) & n > 1 \\ 0 & n = 0 \\ 1 & n = 1 \end{cases}$$

$$\cdot[\cdot] : \mathbb{N}^2 \to \mathbb{N} / x[i] = \begin{cases} V_{P_i} & x \neq 0 \\ 0 & x = 0 \end{cases}$$

Nota: Sea $n > 0, n = P_0^{a_0} \cdot ... \cdot P_k^{a_k}$, $long(n) = k + 1$

8.8 Halt

$$Halt : \mathbb{N}^2 \to \mathbb{N} / Halt(x, y) = \begin{cases} 1 & \text{si el programa de código } y \\ & \text{termina ante la entrada } x \\ 0 & \text{sino} \end{cases}$$

8.9 Programas Universales

Para cada $n > 0$ se define

$$\Phi^n(x_1, ..., x_n, e) = \Psi_P^n(x_1, ..., x_n) = \begin{cases} y & \text{si } y \text{ es la salida del programa} \\ & P \text{ ante la entrada } (x_1, ..., x_n) \\ \uparrow & \text{sino} \end{cases}$$

Donde P es el programa de código e