Lógica de Primer Orden y Cuantificadores

Pablo F. Castro

Programación Avanzada, Universidad Nacional de Río Cuarto, Departamento de Computación

2015

Lógica de Predicados

La lógica proposicional es útil en muchos casos. Sin embargo, no siempre nos permite razonar sobre individuos o elementos, por ejemplo:

$$\frac{\begin{array}{l}\text{Todos los hombres son mortales.}\\ \text{Sócrates es un hombre.}\end{array}}{\text{Sócrates es mortal.}}$$

En lógica proposicional este razonamiento no puede ser expresado correctamente.

La lógica proposicional no nos permite expresar en detalle la estructura de los predicados, cuando estos involucran personas, objetos, etc. y relaciones entre ellos.

Lógica de Primer Orden o de Predicados

La lógica de primer orden ofrece un lenguaje más expresivo que la lógica proposicional:

- Predicados. ($\leq$, $=$, $\ldots$)
- Funciones. ($+$,$*$, etc)
- Constantes. (Sócrates, 0, etc)
- Variables. ($x, y, z, \ldots$)
- Conectivos. ($\vee$, $\wedge$, $\neg$, $\Rightarrow$)
- Cuantificadores. ($\forall$, $\exists$)

Por ejemplo, el razonamiento anterior puede ser expresado:

$$\frac{\begin{array}{l}\forall x : H(x) \Rightarrow M(x) \\ H(s)\end{array}}{M(s)}$$

En donde, tenemos los siguientes predicados, $H(x)$: x es un hombre, $M(x)$:x es mortal. s es la constante Sócrates.

Expresiones

Los símbolos funcionales y las constantes nos permiten introducir diferentes clases de expresiones. Por ejemplo, si queremos escribir expresiones aritméticas, tenemos las constantes usuales $(0, 1, 2, 3, \dots)$, y las funciones $+, -, *, \dots$. Con estos símbolos podemos construir las siguientes expresiones:

$$1 + 1, 0, x + y, x * 10, \text{etc}$$

Todas las expresiones denotan un valor del dominio de discurso. (Por ejemplo, $1 + 1$ denota el valor 2). En el caso de contener alguna variable, el valor final depende del valor actual de la variable.

Notación

En vez de utilizar la notación $f(x)$ para denotar la aplicación de la función f al elemento x, escribiremos $f.x$.

Fórmulas

Las fórmulas son definidas de la siguiente forma:

- Si E_1 y E_2 son expresiones, entonces $E_1 = E_2$ es una fórmula.
- Si φ y ψ son fórmulas, entonces $\varphi \wedge \psi$, $\neg\psi$, $\varphi \rightarrow \psi$ son fórmulas.
- Si x es una variable y R, T son fórmulas, entonces $\langle \forall x : R : T \rangle$ es una fórmula.
- Si x es una variable y R, T son fórmulas, entonces $\langle \exists x : R : T \rangle$ es una fórmula.

Los últimos dos items introducen los cuantificadores, los cuales pueden ser leídos informalmente de la siguiente forma:

$\langle \forall x :$	$R :$	$T \rangle$
Para todo x	que cumple con R	T es verdadero

La misma interpretación se puede realizar con el cuantificador existencial.

Cuantificación Universal y Existencial

Por ejemplo:

$$\langle \forall k : 0 \leq k \leq N : a[k] = 0 \rangle$$

Significa que se cumple:

$$a[0] = 0 \wedge a[1] = 0 \wedge \cdots \wedge a[N] = 0$$

En cambio,

$$\langle \exists k : 0 \leq k \leq N : a[k] = 0 \rangle$$

significa que se cumple:

$$a[0] = 0 \vee \cdots \vee a[N] = 0$$

Cuando el rango es **finito** el cuantificador universal se comporta como una conjunción y el cuantificador como una disyunción.

Variables Libres y Ligadas

El conjunto de **variables libres** de una expresión o fórmula puede definirse inductivamente, de la siguiente forma:

- La variable i esta libre en la expresión i.
- Si la variable i esta libre en la expresión E, entonces esta libre en la expresión $f.(\ldots, E, \ldots)$.
- Si la variable i esta libre en E_1 o E_2, entonces i está libre en la fórmula $E_1 = E_2$.
- Si la variable i está libre en las fórmulas F_1 o F_2, entonces está libre en $F_1 \wedge F_2$, $F_1 \vee F_2$, $\neg F_1$ y $F_1 \Rightarrow F_2$.
- Si $i \neq x$ y i está libre en la fórmula F, entonces i está libre en las fórmulas: $\langle \forall x : R : F \rangle$, $\langle \forall x : F : R \rangle$, $\langle \exists x : F : R \rangle$, $\langle \exists x : R : F \rangle$.

El conjunto de variables libres de una expresión o fórmula T es denotada por $FV.T$.

Variables Libres y Ligadas

Las **variables ligadas** en una expresión son aquellas que no están libres. Algunos ejemplos:

- i aparece libre en $i + 4$, es decir: $FV.(i + 4) = \{i\}$.
- i aparece ligada en $\langle \forall i : 1 \leq i \leq N : T.i \rangle$. N es constante.
- x aparece libre en $\langle \exists i, j : 1 \leq i \leq j : i + x = 0 \rangle$

Cuáles variables aparecen libres y cuáles ligadas en las siguientes expresiones?

- $\langle \forall i : \mathit{true} : \langle \exists j : \mathit{false} : i + j = 0 \rangle \rangle$
- $\langle \forall i : N = i : \langle \exists j : \mathit{false} : N + j = 0 \rangle \rangle$
- $\langle \forall i : \mathit{true} : \langle \exists i : \mathit{true} : i + i = 0 \rangle \rangle$

Estas fórmulas son verdaderas o falsas?

Axiomas de los Cuantificadores Existencial y Universal

Utilizaremos el siguiente conjunto de axiomas del cuantificador universal:

- $\langle \forall x :: T.x \rangle \equiv \langle \forall x : true : T.x \rangle$ **[Rango True]**
- $\langle \forall x : R.x : T.x \rangle \equiv \langle \forall x :: R.x \Rightarrow T.x \rangle$ **[Intercambio entre rango y término]**
- $\langle \forall x :: T.x \rangle \wedge \langle \forall x :: R.x \rangle \equiv \langle \forall x :: T.x \wedge R.x \rangle$ **[Regla del término]**
- $X \vee \langle \forall x :: T.x \rangle \equiv \langle \forall x :: X \vee T.x \rangle$ **[Dist. de $\vee$ con $\forall$]**, siempre que x no ocurra en X.
- $\langle \forall x : x = E : T.x \rangle \equiv T.E$ **[Rango Unitario]**
- $\langle \forall x :: \forall y :: F.x.y \rangle\rangle \equiv \langle \forall y :: \langle \forall x :: F.x.y \rangle\rangle$ **[Intercambio]**
- $\langle \forall x, y :: F.x.y \rangle \equiv \langle \forall x :: \langle \forall y :: F.x.y \rangle\rangle$ **[Anidamiento]**

Algunos Teoremas... Probemos el teorema de partición de rango:

$$\langle \forall x : R.x : F.x \rangle \wedge \langle \forall x : S.x : F.x \rangle \equiv \langle \forall x : R.x \vee S.x : F.x \rangle$$

$$\begin{aligned}
&\langle \forall x : R.x : F.x \rangle \wedge \langle \forall x : S.x : F.x \rangle \\
&\equiv \text{[Intercambio, caracterización } \Rightarrow] \\
&\langle \forall x :: \neg R.x \vee F.x \rangle \wedge \langle \forall x :: \neg S.x \vee F.x \rangle \\
&\equiv \text{[Dist. } \forall, \wedge] \\
&\langle \forall x :: (\neg R.x \vee F.x) \wedge (\neg S.x \vee F.x) \rangle \\
&\equiv \text{[Dist. } \vee, \wedge] \\
&\langle \forall x :: (\neg R.x \wedge \neg S.x) \vee F.x \rangle \\
&\equiv \text{[de Morgan]} \\
&\langle \forall x :: \neg (R.x \vee S.x) \vee F.x \rangle \rangle \\
&\equiv [?] \\
&\langle \forall x : R.x \vee S.x : F.x \rangle
\end{aligned}$$

Qué regla usamos en el último paso?

Instanciación

$$\langle \forall x :: F.x \rangle \Rightarrow F.Y$$

Usando la defininción de $\Rightarrow$, tenemos que probar:

$$\langle \forall x :: F.x \rangle \equiv \langle \forall x :: F.x \rangle \wedge F.Y$$

$\langle \forall x :: F.x \rangle$

$\equiv$ [Rango True]

$\langle \forall x : true : F.x \rangle$

$\equiv$ [absorbente del $\vee$]

$\langle \forall x : true \vee x = Y : F.x \rangle$

$\equiv$ [partición del Rango]

$\langle \forall x : true : F.x \rangle \wedge \langle \forall x : x = Y : F.x \rangle$

$\equiv$ [Rango Unit.]

$\langle \forall x :: F.x \rangle \wedge F.Y$

Axiomas del Cuantificador Existencial

Tenemos el siguiente axioma, el cual define el cuantificador existencial utilizando el cuantificador universal.

$$\langle \exists x : R : T \rangle \equiv \neg \langle \forall x : R : \neg T \rangle$$

A partir de este axioma podemos demostrar las siguientes propiedades:

- $\langle \exists x : R : T \rangle \equiv \langle \exists :: R \wedge T \rangle$ **[Intercambio]**
- $\langle \exists x :: T \rangle \vee \langle \exists x :: S \rangle \equiv \langle \exists x : R : T \vee S \rangle$ **[Regla del Término]**
- $X \wedge \langle \exists x :: T \rangle \equiv \langle \exists x :: T \wedge X \rangle$ **[Dist.∃,∧]** Siempre que x no sea libre en X.
- $\langle \exists x : R : T \rangle \vee \langle \exists x : S : T \rangle \equiv \langle \exists x : R \vee S : T \rangle$ **[Partición de Rango]**

Ejemplo de Prueba

Demostremos: $\langle \exists x : R : F \rangle \equiv \langle \exists x :: R \wedge F \rangle$

$$\begin{array}{l}
\langle \exists x : R : F \rangle \\
\equiv [\text{Def.}\exists] \\
\neg \langle \forall x : R : \neg F \rangle \\
\equiv [\text{Intercambio entre rango y término en } \forall] \\
\neg \langle \forall x :: R \Rightarrow \neg F \rangle \\
\equiv [\text{Prop.}\Rightarrow] \\
\neg \langle \forall x :: \neg R \vee \neg F \rangle \\
\equiv [\text{de Morgan}] \\
\neg \langle \forall x :: \neg (R \wedge F) \rangle \\
\equiv [?] \\
\langle \exists x :: R \wedge F \rangle
\end{array}$$

Ejercicio: Demostrar las otras propiedades de $\exists$

Más Propiedades Importantes de los Cuantificadores

- $\langle \forall x : R : P \equiv Q \rangle \equiv \langle \forall x : R : P \rangle \equiv \langle \forall x : R : Q \rangle$
- $\langle \forall x : R : P \wedge Q \rangle \Rightarrow \langle \forall x : R : P \rangle$ **[Fortalecimiento]**
- $\langle \forall x : R \vee S : T \rangle \Rightarrow \langle \forall x : R : T \rangle$ **[Fortalecimiento por Rango]**
- $\langle \forall x : R : P \Rightarrow Q \rangle \Rightarrow (\langle \forall x : R : P \rangle \Rightarrow \langle \forall x : R : Q \rangle)$ **[Monotonía]**

Tenemos similares propiedades para el existe:

- $\langle \exists x : R : P \rangle \Rightarrow \langle \exists x : R : P \vee Q \rangle$ **[Debilitamiento]**
- $\langle \exists x : R : P \rangle \Rightarrow \langle \exists x : R \vee S : Q \rangle$ **[Debilitamiento por Rango]**
- $\langle \exists x : R : P \Rightarrow Q \rangle \Rightarrow (\langle \exists x : R : P \rangle \Rightarrow \langle \exists x : R : Q \rangle)$ **[Monotonía]**
- $\langle \exists x : R : \langle \forall y : S : T \rangle \rangle \equiv \langle \forall y : S : \langle \exists x : R : T \rangle \rangle$ **[Intercambio]**, x no aparece libre en S e y no aparece libre en R.

Ejercicio:Demostrar estas propiedades.

Ejemplos

Volvamos al ejemplo:

$$\frac{\text{Todos los hombres son mortales.} \quad \text{Sócrates es un hombre.}}{\text{Sócrates es mortal.}}$$

Podemos definir: $M.x$:x es un mortal. $H.x$:x es un hombre. s:Sócrates.

$$
\begin{array}{l}
(\langle \forall x : H.x : M.x \rangle \wedge H.s) \Rightarrow M.s \\
\equiv \text{[Intercambio]} \\
(\langle \forall x :: H.x \Rightarrow M.x \rangle \wedge H.s) \Rightarrow M.s \\
\equiv \text{[Instanciación]} \\
(\langle \forall x :: H.x \Rightarrow M.x \rangle \wedge (H.s \Rightarrow M.s) \wedge H.s) \Rightarrow M.s \\
\equiv \text{[Modus Ponens]} \\
(\langle \forall x :: H.x \Rightarrow M.x \rangle \wedge H.s \wedge M.s) \Rightarrow M.s \\
\equiv \text{[fortalecimiento]} \\
True
\end{array}
$$

Expresiones Cuantificadas

En general podemos utilizar cuantificadores en expresiones, por ejemplo:

$$\sum_{1 \leq i \leq N} i$$

o bien:

$$\prod_{1 \leq i \leq N} i$$

En general, para cualquier operador $\oplus$ es cual es asociativo y conmutativo, podemos considerar la expresión:

$$\langle \oplus i : R.i : T.i \rangle$$

Ejemplos:

$$\langle \sum i : R.i : T.i \rangle$$

o bien:

$$\langle \prod i : R.i : T.i \rangle$$

Expresiones Cuantificadas

Algunos ejemplos de expresiones cuantificadas:

- $\langle \sum i : 1 \leq i \leq n : 2^i \rangle$
- $\langle \prod i : 1 \leq i \leq n : i \rangle$
- $\langle \uparrow i : 0 \leq i \leq n : i + 1 \rangle$
- $\langle \downarrow i : 0 \leq i \leq n : i + 1 \rangle$

La definición de variable libre y variable ligada es exáctamente la misma que para los cuantificadores lógicos.

Axiomas de las Expresiones Cuantificadas

- $\langle \oplus i : \mathit{false} : T \rangle = e$ **[Rango Vacío]** (e es el neutro de $\oplus$)
- $\langle \oplus i : i = N : T \rangle = T[i := N]$ **Rango Unitario**
- $\langle \oplus i : R \vee S : T \rangle = \langle \oplus i : R : T \rangle \oplus \langle \oplus i : S : T \rangle$ **[Partición de Rango]** Siempre que $\oplus$ sea idempotente o $R \wedge S \equiv \mathit{false}$.
- $\langle \oplus i : R : T_0 \oplus T_1 \rangle = \langle \oplus i : R : T_0 \rangle \oplus \langle \oplus i : R : T_1 \rangle$ **[Regla del Término]**
- $\langle \oplus i, j : R.i \wedge S.i.j : T.i.j \rangle \equiv \langle \oplus i : R.i : \langle \oplus j : S.i.j : T.i.j \rangle \rangle$ **[Anidamiento]**
- $\langle \oplus i : R : T \rangle \equiv \langle \oplus k : R[i := k] : T[i := k] \rangle$ **[Cambio de Variables]**, donde k no aparece libre en T o R.
- $\langle \oplus i : R.i : C \rangle = C$ **[Término Constante]**, donde el rango no es vacío y $\oplus$ es idempotente.

En el caso de que $\otimes$ es distributivo con respecto a $\oplus$ y el rango no es vacío, entonces:

- $\langle \oplus i : R : k \otimes T \rangle \equiv k \otimes \langle \oplus i : R : T \rangle$

Cambio de Variables con Funciones Biyectivas

Dada una función biyectiva: $f : A \to A$ en donde A es el dominio del cuantificador $\oplus$, entonces:

$$\langle \oplus i : R.i : T.i \rangle = \langle \oplus j : R.f.j : T.f.j \rangle$$

Por ejemplo, consideremos:

$$\langle \sum i : 1 \leq i \leq n+1 : i \rangle$$

es lo mismo que:

$$\langle \sum j : 1 \leq j+1 \leq n+1 : j+1 \rangle$$

en donde: $f.j = j+1$ y $f : \mathbb{Z} \to \mathbb{Z}$.

El Operador de Conteo

Un operador interesante es el siguiente:

$\langle N i : R.i : T.i \rangle \equiv \langle \sum i : R.i \wedge T.i : 1 \rangle$

Este operador nos permite *contar* todos los elementos en el rango R que cumplen con T. Por ejemplo,

$$\langle N i : i \in S : par.i \rangle$$

Cuenta la cantidad de pares en S (S tiene que ser finito).

Ejercicio: Definir el predicado par.i