Lógica

Programación Avanzada
UNRC
Pablo Castro

Lógica Proposicional

El lenguaje de la lógica proposicional consta de:

- Letras proposicionales: $p, q, s, t, \ldots$

Representan proposiciones que pueden ser verdaderas o falsas

- Formulas, definidas inductivamente:

1. Las letras proposicionales son formulas
2. Si A y B son formulas, entonces:

$A \wedge B$ $A \vee B$ $\neg A$ $A \Rightarrow B$ $A \equiv B$ son formulas.

Semántica

Para evaluar una fórmula se le pueden asignar valores de verdad a las variables

p	$\vee$	q
T	T	T
T	T	F
F	T	T
F	F	F

Cada operador lógico se corresponde con una tabla de verdad

Terminología

- Una formula es **satisfacible** si hay alguna asignación de valores de verdad a sus variables que la hacen verdadera,

- Una formula se dice **valida**, si todas las asignaciones de verdad hacen la formula verdadera

- Una formula se dice **contradictoria**, si todas las asignaciones de verdad la hacen falsa

Ejercicio, dar un ejemplo de cada clase de formula.

La Equivalencia

La equivalencia lógica es una de las operaciones más importantes:

A	$\equiv$	B
T	T	T
T	F	F
F	F	T
F	T	F

Intuitivamente, A y B toman el mismo valor

Cálculo Proposicional

El cálculo proposicional nos permite demostrar teoremas de la lógica.

- **Axiomas**: Formulas que asumimos como teoremas.
- **Reglas**: Permiten obtener nuevos teoremas de teoremas ya demostrados

Una **demostración** es una secuencia de formulas $A_0, A_1, A_2, \ldots, A_n$ en donde A_n es el teorema demostrado y cada A_i es una axioma o se obtiene por la aplicación de un regla

Reglas de Deducción

$$\frac{A \equiv B, B \equiv C}{A \equiv C}$$

Transitividad de la equivalencia

$$\frac{P \equiv Q}{E[r := P] \equiv E[r := Q]}$$

Reemplazo de equivalentes por equivalentes (Leibniz)

$$\frac{P}{P[r := Q]}$$

Sustitución

En donde A,B,C,E,P,Q son fórmulas, y r una variable proposicional

Axiomas

Equivalencia:

$A \equiv (B \equiv C) \equiv (A \equiv B) \equiv C$ (*Asociatividad*)

$(A \equiv B) \equiv (B \equiv A)$ (*Simetría*)

$A \equiv True \equiv A$ (*Neutro*)

Negación:

$\neg(A \equiv B) \equiv (\neg A \equiv B)$

False $\equiv \neg$True (*Definición de False*)

$\neg\neg A \equiv A$ (*Doble Negación*)

Axiomas

Disyunción:

$$A \vee (B \vee C) \equiv (A \vee B) \vee C$$

$$A \vee B \equiv B \vee A$$

$$A \vee A \equiv A$$

$$A \vee (B \equiv C) \equiv (A \vee B) \equiv (A \vee C)$$

$$A \vee \neg A$$

Conjunción:

$$A \wedge B \equiv A \equiv B \equiv B \vee A \ (\textit{Regla Dorada})$$

$$A \wedge (B \wedge C) \equiv (A \wedge B) \wedge C \ (\textit{Asociatividad})$$

$$A \wedge B \equiv B \wedge A \ (\textit{Conmutatividad})$$

$$A \wedge A \equiv A$$

$$A \wedge \textit{True} \equiv A$$

Implicación:

$$A \Rightarrow B \equiv A \vee B \equiv B$$

Demostraciones

En general demostraremos: $E \equiv E'$

$$
\begin{aligned}
& E \\
& \equiv [\text{justificación de } E \equiv E_1] \\
& E_1 \\
& \vdots \\
& E_n \\
& \equiv [\text{justificación de } E_n \equiv E'] \\
& E'
\end{aligned}
$$

Ejemplo

Demostremos: $P \Rightarrow Q \equiv \neg P \vee Q$

$$
\begin{array}{ll}
 & p \Rightarrow q \\
\equiv & \text{[Definición de } \Rightarrow\text{]} \\
 & p \vee q \equiv q \\
\equiv & [p \vee \mathit{False} \equiv p] \\
 & p \vee q \equiv q \vee \mathit{False} \\
\equiv & \text{[propiedad de } \equiv\text{]} \\
 & (p \equiv \mathit{False}) \vee q \\
\equiv & [p \equiv \mathit{False} \equiv \neg p] \\
 & \neg p \vee q
\end{array}
$$

Resolución de Acertijos

En la isla de los caballeros y los mentirosos hay dos clases de personas:

Los **mentirosos**, siempre dicen mentiras.

Los **caballeros**, siempre dicen verdades.

Las letras A,B,C,… representan habitantes, en donde:

A: es verdadero ssi A es caballero

Formalización

A dice S se formaliza como:

$$A \equiv S$$

Ejemplos:

A dice “yo soy un caballero” se formaliza: $A \equiv A$

A dice “yo soy un mentiroso” se formaliza: $A \equiv \neg A$

A dice “yo soy del mismo tipo que B” se formaliza:

$$A \equiv (A \equiv B)$$

Ejemplo

Supongamos que A dice “Hay oro en la isla ssi yo soy un caballero”

$$
\begin{aligned}
& A \equiv A \equiv G \\
\equiv \quad & \text{[Asociatividad de } \equiv\text{]} \\
& (A \equiv A) \equiv G \\
\equiv \quad & \text{[Reflexividad de } \equiv\text{]} \\
& \mathit{True} \equiv G \\
\equiv \quad & \text{[identidad } \equiv\text{]} \\
& G
\end{aligned}
$$

Lógica de Primer Orden

La lógica de primer orden introduce cuantificadores y la posibilidad de referirse a individuos o elementos.

Todos los hombres son mortales

Sócrates es hombre

Luego, Sócrates es mortal

Este razonamiento no puede ser expresado en proposicional

Lenguaje de Primer Orden

El lenguaje de primer orden es más expresivo que el proposicional:

- Variables: $x, y, z, \ldots$
- Predicados: $=, \leq, \ldots$
- Funciones: $+, *, \ldots$
- Constantes: $0, \pi, \ldots$
- Conectivos: $\vee, \wedge, \neg, \ldots$
- Cuantificadores: $\forall, \exists$

Fórmulas

Podemos definir las formulas inductivamente:

- Si E_1 y E_2 son expresiones, entonces $E_1 = E_2$ es una fórmula.
- Si φ y ψ son fórmulas, entonces $\varphi \wedge \psi$, $\neg\psi$, $\varphi \to \psi$ 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.

Intuitivamente:

$\langle \forall x :$ $R :$ $T \rangle$

Para todo x que cumple con R T es verdadero

Parecido para el cuantificador existencial

Cuantificadores sobre Conjuntos Finitos

Cuando los cuantificadores son sobre conjuntos finitos se pueden escribir como conjunciones o disyunciones:

Por ejemplo:

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

Significa:

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

y:

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

Significa:

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

Variables Libres y Ligadas

Una variable se dice **ligada** si esta dentro del alcance de un cuantificador

$$\langle \exists i, j : 1 \leq i \leq j : i + x = 0 \rangle$$

x aparece libre

Una variable se dice **libre** si no está ligada

$$\langle \forall i : true : \langle \exists j : false : i + j = 0 \rangle \rangle$$

i, j son variables ligadas

Axiomas Cuantificadores

Utilizaremos los siguientes axiomas:

- $\langle \forall x :: T.x \rangle \equiv \langle \forall x : true : T.x \rangle$ **[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]**

Teoremas

Demostremos un teorema:

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

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

$\equiv$ [Intercambio, caracterización $\Rightarrow$]

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

$\equiv$ [Dist. $\forall$, $\wedge$]

$\langle \forall x :: (\neg R.x \vee F.x) \wedge (\neg S.x \vee F.x) \rangle$

$\equiv$ [Dist. $\vee$,$\wedge$]

$\langle \forall x :: (\neg R.x \wedge \neg S.x) \vee F.x \rangle$

$\equiv$ [de Morgan]

$\langle \forall x :: \neg(R.x \vee S.x) \vee F.x \rangle \rangle$

$\equiv$ [?]

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

Qué regla usamos en el último paso

Demostración de Teoremas

Demostremos una propiedad mas: $\langle \forall x :: F.x \rangle \Rightarrow F.Y$

Por la definición de la implicación debemos demostrar:

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

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

$\equiv$ [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.]

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

Demostración

Cuantificador Existencial

El cuantificador existencial se puede definir a partir del cuantificador universal.

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

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.$\exists$,$\wedge$]** 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 Demostración

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

$\langle \exists x : R : F \rangle$

$\equiv$ [Def.$\exists$]

$\neg\langle \forall x : R : \neg F \rangle$

$\equiv$ [Intercambio entre rango y término en $\forall$]

$\neg\langle \forall x :: R \Rightarrow \neg F \rangle$

$\equiv$ [Prop.$\Rightarrow$]

$\neg\langle \forall x :: \neg R \vee \neg F \rangle$

$\equiv$ [de Morgan]

$\neg\langle \forall x :: \neg(R \wedge F) \rangle$

$\equiv$ [?]

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

Propiedades Importantes

Para el cuantificador universal:

- $\langle \forall x : R : P \equiv Q \rangle \equiv \langle \forall x : R : P \rangle \equiv \langle \forall x : R : Q \rangle$
- $\langle \forall x : R : P \wedge Q \rangle \Rightarrow \langle \forall x : R : P \rangle$ **[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]**

Para el cuantificador existencial:

- $\langle \exists x : R : P \rangle \Rightarrow \langle \exists x : R : P \vee Q \rangle$ **[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.

Cuantificadores en General

Para cualquier operación $\oplus$ asociativa y conmutativa, podemos definir cuantificadores:

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

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

$\langle Min\ i : R.i : T.i \rangle$ — Minimo

$\langle Max\ i : R.i : T.i \rangle$ — Maximo

Ejemplos de Expresiones Cuantificadas

$$\langle \Sigma\ i : 1 \leq i \leq n : 2^i \rangle = 2^1 + 2^2 + 2^3 + \cdots + 2^n$$

$$\langle \Pi\ i : 1 \leq i \leq n : i \rangle = 1 * 2 * \cdots * n$$

$$\langle \Sigma\ i : 1 \leq i \leq n : 2^n \rangle = 2^n + 2^n + 2^n + \cdots + 2^n$$

n veces

$$\langle \Sigma\ i : 1 \leq i \leq n : 1 \rangle = 1 + 1 + 1 + \cdots + 1$$

Cuenta la cantidad de números pares entre 1 y n

$$\langle \Sigma\ i : 1 \leq i \leq n \wedge i\ mod\ 2 = 0 : 1 \rangle = 1 + 1 + 1 + \cdots + 1$$

Propiedades Cuantificadores

Los cuantificadores tienen ciertas propiedades generales:

- $\langle \oplus i : \mathit{false} : T \rangle = e$ **[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

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 $f : \mathbb{Z} \to \mathbb{Z}$.

Cuantificador de Conteo

Un cuantificador interesante es el de conteo:

$$\langle N\ i : R.i : T.i \rangle = \langle \Sigma\ i : R.i \wedge T.i : 1 \rangle$$

Cantidad de elementos del rango que cumplen T

Por ejemplo:

$$\langle N\ i : 1 \leq i \leq n : esPar.i \rangle$$

Cantidad de pares en el intervalo [1,n]

Cuantificadores en Haskell

Podemos utilizar listas por comprensión para escribir los cuantificadores en Haskell.

Tenemos que tener en cuenta que en ese caso estamos considerando una forma de **computar** la solución

Dado el cuantificador: $\langle \oplus i : R \,.\, i : T \,.\, i \rangle$ (con rango finito) lo podemos escribir en Haskell como:

```
f [ T i | i <- xs, R i]
```

En donde:

`xs` es el universo de cuantificación.

`f :: [a] -> a` es el operador llevado a listas

Ejemplos de Cuantificadores en Haskell

Logica	Haskell
$\langle \forall i : 0 \leq i \leq \#xs : xs\,.\,i = 0 \rangle$	`and [xs!!i==0|i<-[0..lenght xs-1]]`
$\langle \sum i : 0 \leq i < n \wedge i \mid n : i \rangle$	`sum [i|i<-[0..n-1],n `mod` i==0]`
$\langle \forall i, j : 0 \leq i < j \leq \#xs : xs\,.\,i \neq xs\,.\,j \rangle$	`and [xs!!i/=xs!!j|i<-[0..length xs-1],j<-[i+1..length xs-1]]`