Lògica en la Informàtica

Definició de la Lògica de Primer Ordre (LPO)

José Miguel Rivero   Robert Nieuwenhuis

Dept. Ciències de la Computació
Facultat de Informàtica
Universitat Politècnica de Catalunya (UPC)

Tardor 2022

Definició de la Lògica de Primer Ordre

Col·lecció d'apunts bàsics de lògica: ☞ `p4.pdf`

Recordem:

Què és una lògica?

- sintaxi: - què és una fórmula F ?

$+$

- semàntica: -a què és una interpretació I ?

-b quan una I SATISFÀ una F ? $I \models F$?

Intuïtivament:

"Interpretació" $\equiv$ "situació de la vida real a modelar"

Una F "representa" aquelles I on se satisfà, es compleix.

☞ Apunts: `p4.pdf`

Recordem:

Usem I per a denotar interpretacions i F, G per a fórmules.

En qualsevol lògica:

- I **és model** de F si I satisfà a F (es denota $I \models F$)
- F és **satisfactible** si F té algun model
- F és **insatisfactible** si F no té models
- F és **tautologia** si tota I és model de F
- G és **conseqüència lògica** de F si tot model de F satisfà G (es denota $F \models G$)
- F i G són **lògicament equivalents** si F i G tenen el mateixos models (es denota $F \equiv G$)

  Nota: Per definició tenim que $F \equiv G$ ssi $F \models G$ i $G \models F$.

Definició de la Lògica de Primer Ordre

☞ Apunts: `p4.pdf`

LPO: molt més poder expressiu que la LProp.
podem modelar moltes més coses de la vida real:
matemàtiques, verificació de programari, protocols, ...

LPO: deducció més costosa (en complexitat, decidibilitat)
que la LProp

☞ Apunts: `p4.pdf`

LPO: Sintaxi:

$$\left.\begin{array}{l}\left.\begin{array}{ll}\text{símbols de variable:} & X \\ \text{símbols de funció:} & F\end{array}\right\}\ \text{termes} \\ \begin{array}{ll}\text{símbols de predicat:} & P\end{array}\ \_\_\_\_\_\_\_\_\end{array}\right\}\ \text{atoms}$$

Fórmules: àtoms combinats amb connectives $\wedge$ $\vee$ $\neg$ i amb quantificadors $\forall$ $\exists$
(compte amb la notació "text" que també es fa servir aquí: "per a tot" és A, "existeix" és E, etc.)

LPO: Semàntica:

Una I consta de tres parts:

D_I: "el domini" de I (un conjunt no buit)

f_I: per cada símbol de funció f d'aritat n,

una funció $f_I : \overbrace{D_I \times \cdots \times D_I}^{n \text{ args}} \to D_I$ "la interpretació de f en I"

p_I: per cada símbol de predicat p d'aritat n,

una funció $p_I : \overbrace{D_I \times \cdots \times D_I}^{n \text{ args}} \to \{0, 1\}$ "la interpretació de p en I"

Intuïtivament, és com si hi hagués dos TIPUS: els Booleans i "els altres" (els elements de D_I).

F: prenen arguments de D_I i retornen D_I.

P: prenen arguments de D_I i retornen un Booleà.

PER AIXÒ NO TÉ SENTIT NIAR SÍMBOLS DE PREDICAT.

Definició de la Lògica de Primer Ordre

Noció d'avaluació d'una F en una I: ☞ Veure p4.pdf

- Satisfacció
  - Assignació a variables
  - Avaluació de termes
  - Avaluació de fórmules
  - Noció de satisfacció
- Fórmules tancades
  - Aparicions lliures i lligades de variables
  - Fórmules tancades
  - Avaluació de fórmules tancades
  - Satisfacció de fórmules tancades

Exemple:

$\mathcal{F}$ és:
- f d'aritat 2
- g d'aritat 1
- h d'aritat 1
- a d'aritat 0
- b d'aritat 0

$\mathcal{P}$ és:
- p d'aritat 2
- q d'aritat 1
- r d'aritat 0

Exemples de termes: $a \quad b \quad g(a) \quad f(x,a)$
$f(f(a,b),x) \qquad f(g(a),g(g(f(a,x)))) \quad \ldots$

de fet, si només tinc un símbol unari ja puc fabricar infinits termes:
$x \quad h(x) \quad h(h(x)) \quad h(h(h(x))) \quad \ldots$

Exemples d'àtoms: $r \quad q(a) \quad q(f(a,b)) \quad q(h(h(x))) \quad p(a,h(x)) \quad \ldots$

Exemple de fórmula F: $\forall x\, \exists y\, (p(x,h(y)) \vee q(f(x,y)))$

Exemple d'I:

$D_I = \{o, \$\}$

f_I: $D_I \times D_I \rightarrow D_I$

defineixo aquesta funció donant tots els casos:

$f_I(\$, \$) = \$$

$f_I(\$, o) = o$

$f_I(o, \$) = \$$

$f_I(o, o) = \$$

g_I: $D_I \rightarrow D_I$

$g_I(\$) = o$

$g_I(o) = \$$

h_I: $D_I \rightarrow D_I$

$h_I(\$) = \$$

$h_I(o) = o$

$a_I = o$

$b_I = \$$

Exemple d'I (cont.):

$D_I = \{o, \$\}$

p_I: $D_I \times D_I \rightarrow \{0, 1\}$
defineixo aquesta funció donant tots els casos:
$p_I(\$, \$) = 1$
$p_I(\$, o) = 0$
$p_I(o, \$) = 0$
$p_I(o, o) = 1$

q_I: $D_I \rightarrow \{0, 1\}$
defineixo aquesta funció donant tots els casos:
$q_I(\$) = 1$
$q_I(o) = 0$

$r_I = 1$

Tenim $I \models F$?

$$\forall x\, \exists y\, (p(x, h(y)) \vee q(f(x, y)))$$

$$\begin{aligned} p_I(\$, \$) &= 1 \\ p_I(\$, o) &= 0 \\ p_I(o, \$) &= 0 \\ p_I(o, o) &= 1 \end{aligned}$$

$$\begin{aligned} h_I(\$) &= \$ \\ h_I(o) &= o \end{aligned}$$

com p_I s'interpreta com a igualtat, i la h_I és la funció identitat (que "no fa res"), tenim que $\forall x\, \exists y\, p(x, h(y))$ es compleix: per a tota x del domini hi ha una y que és igual:

si $x = \$$ triem que la y sigui també \$

si $x = o$ triem que la y sigui també o

ni tan sols cal mirar la part $q(f(x, y))$.

Tenim que $I \models F$.

Un altre exemple d'interpretació:

$D_I = \mathbb{N}$ (els nombres naturals)

f_I d'aritat 2	la suma de naturals:	$f_I(n, m) = n + m$
g_I d'aritat 1	la funció "successor":	$g_I(n) = n + 1$
h_I d'aritat 1	la funció "doble":	$h_I(n) = 2n$
a_I d'aritat 0	7	
b_I d'aritat 0	23	
p_I d'aritat 2	l'ordre estricte de naturals:	$p_I(n, m) = (n > m)$
q_I d'aritat 1	ens diu si és parell:	$q_I(n) = (n \bmod 2 = 0)$
r_I d'aritat 0	0	

Ara tenim $I \models F$?

$$\forall x\, \exists y\, (p(x, h(y)) \vee q(f(x, y)))$$

per a tota x existeix una y tal que $x > 2y$ o $x + y$ és parell ?
Això és cert, perquè per a tota x podem triar la y que sigui la mateixa x i llavors $x + y = x + x$ que és parell.
(no necessitem la primera meitat de l'or)

Exercicis

5. (dificultat 1) Sigui F la fórmula

$$\exists x\, \exists y\, \exists z\, (p(x,y) \wedge p(z,y) \wedge p(x,z) \wedge \neg p(z,x)).$$

Quines de les següents interpretacions són models de F ?

a) $D_I = \mathbb{N}$ i $p_I(m,n) = 1$ si i només si $m \leq n$.

b) $D_I = \mathbb{N}$ i $p_I(m,n) = 1$ si i només si $n = m + 1$.

c) $D_I = \mathcal{P}(\mathbb{N})$ (això denota parts de $\mathbb{N}$, és a dir, el conjunt de tots els subconjunts de $\mathbb{N}$), i $p_I(A,B) = 1$ si i només si $A \subseteq B$.

En format "text":

```
Ex Ey Ez ( p(x, y) & p(z, y) & p(x, z) & -p(z, x) )
```

Exercicis

5. (dificultat 1) Sigui F la fórmula

$$\exists x \, \exists y \, \exists z \, (p(x,y) \land p(z,y) \land p(x,z) \land \neg p(z,x)).$$

a) $D_I = \mathbb{N}$ i $p_I(m,n) = 1$ si i només si $m \leq n$.

$$\exists x \, \exists y \, \exists z \, (\underbrace{p(x,y)}_{\substack{x \leq y \\ 1 \quad 3}} \land \underbrace{p(z,y)}_{\substack{z \leq y \\ 2 \quad 3}} \land \underbrace{p(x,z)}_{\substack{x \leq z \\ 1 \quad 2}} \land \underbrace{\neg p(z,x)}_{\substack{z > x \\ 2 \quad 1}}) \quad \text{s'avalua com}$$

Sí, $I \models F$.

Exercicis

5. (dificultat 1) Sigui F la fórmula

$$\exists x\,\exists y\,\exists z\,(p(x,y)\land p(z,y)\land p(x,z)\land\neg p(z,x)).$$

b) $D_I=\mathbb{N}$ i $p_I(m,n)=1$ si i només si $n=m+1$.

$$\exists x\,\exists y\,\exists z\,(p(x,y)\land p(z,y)\land p(x,z)\land\neg p(z,x)) \quad \text{s'avalua com}$$

$$\underbrace{\underbrace{y=x{+}1 \quad y=z{+}1}_{x\,=\,z} \quad \overbrace{z=x{+}1}^{}_{\;} \quad x\neq z{+}1}_{}$$

$$\underbrace{x=z \qquad\qquad z=x{+}1}_{\text{NO}}$$

NO, I no és model de F.

Exercicis

5. (dificultat 1) Sigui F la fórmula

$$\exists x\, \exists y\, \exists z\, (p(x,y) \wedge p(z,y) \wedge p(x,z) \wedge \neg p(z,x)).$$

c) $D_I = \mathcal{P}(\mathbb{N})$ i $p_I(A,B) = 1$ si i només si $A \subseteq B$.

$$\exists x\, \exists y\, \exists z\, (\underset{\substack{x \subseteq y \\ \{1\}\ \{1,2,3\}}}{p(x,y)} \wedge \underset{\substack{z \subseteq y \\ \{1,2\}\ \{1,2,3\}}}{p(z,y)} \wedge \underset{\substack{x \subseteq z \\ \{1\}\ \{1,2\}}}{p(x,z)} \wedge \underset{\substack{z \not\subseteq x \\ \{1,2\}\ \{1\}}}{\neg\, p(z,x)}) \quad \text{s'avalua}$$

Sí, $I \models F$.

Exercicis

6. (dificultat 2) Expressa amb tres fórmules les propietats de reflexivitat, simetria i transitivitat d'un predicat binari p i demostra que cap de les tres fórmules és conseqüència lògica de (la conjunció de) les altres dues.

Una interpretació p_I d'una predicat binari p, és una funció $p_I : D_I \times D_I \rightarrow \{0,1\}$. Ens adonem que en realitat p_I és el mateix que una relació binària sobre D_I:

p_I ens diu quines parelles d'elements de D_I donen 1 (estan en la relació).

Exercicis

6. (dificultat 2) Expressa amb tres fórmules les propietats de reflexivitat, simetria i transitivitat d'un predicat binari p i demostra que cap de les tres fórmules és conseqüència lògica de (la conjunció de) les altres dues.

Recordem:

p és **reflexiu**		$p(e,e)$	per a tot e de S.
	FR: $\forall x\, p(x,x)$		
p és **simètric**	si $p(e,e')$	implica $p(e',e)$	per a tot e,e' de S.
	FS: $\forall x\, \forall y\, (p(x,y) \rightarrow p(y,x))$		
p és **transitiu**	si $p(e,e')$ i $p(e',e'')$	implica $p(e,e'')$	per a tot e,e',e'' de S.
	FT: $\forall x\, \forall y\, \forall z\, (p(x,y) \land p(y,z) \rightarrow p(x,z))$		

Exercici 6 (cont.)

1r cas: FR no és conseqüència lògica de $FS \land FT$.

Sigui I la interpretació on $D_I = \{*\}$ i $p_I(*,*) = 0$.
Llavors tenim que I no és model de FR.
Però I sí que és model de FS:

$$\forall x\,\forall y\,(p(x,y) \to p(y,x)) \;\equiv\; \forall x\,\forall y\,(\neg p(x,y) \lor p(y,x))$$

i I també és model de FT:

$$\forall x\,\forall y\,\forall z\,(p(x,y) \land p(y,z) \to p(x,z)) \;\equiv\; \forall x\,\forall y\,\forall z\,(\neg p(x,y) \lor \neg p(y,z) \lor p(x,z))$$

Per tant, tenim que FR no és conseqüència lògica de $FS \land FT$.

Exercici 6 (cont.)

2n cas: FS no és conseqüència lògica de $FR \wedge FT$.

Sigui I la interpretació on $D_I = \{a, b\}$

$p_I(a, a) = 1$ (per reflexivitat)
$p_I(a, b) = 1$ per a incomplir la simetria, juntament amb la línia següent
$p_I(b, a) = 0$ per a incomplir la simetria, juntament amb la línia anterior
$p_I(b, b) = 1$ (per reflexivitat).

Tenim que I no és model de FS, però sí de FR i de FT.

Per tant, tenim que FS no és conseqüència lògica de $FR \wedge FT$.

Exercici 6 (cont.)

3r cas: FT no és conseqüència lògica de $FR \wedge FS$.

Sigui I la interpretació on $D_I = \{a, b, c\}$

	FR	$\neg FT$	FS
$p_I(a,a) =$	1		
$p_I(a,b) =$		1	
$p_I(a,c) =$		0	
$p_I(b,a) =$			1
$p_I(b,b) =$	1		
$p_I(b,c) =$		1	
$p_I(c,a) =$			0
$p_I(c,b) =$			1
$p_I(c,c) =$	1		

Tenim que I no és model de FT, però sí de FR i de FS.

Per tant, tenim que FT no és conseqüència lògica de $FR \wedge FS$.

Exercicis del capítol `p4.pdf` per al proper dia:

☞ 7, 8, 9, 10, 11, 12, 16, 21 en endavant.